Chapter 3 :- Continuous Predicates as a Topology

It is possible to define a topology on the space of processes P (or one of the product spaces P^{Λ}) in which the closed sets are identified with the continuous predicates. This can be done for each of the types of continuity we have met so far. In any particular case we will have:

3.1 $X \in \mathbb{C}$ (the class of closed sets)
$\Leftrightarrow R(A) \equiv$ "$A \in X$" is a continuous predicate.

That these are the closed sets of a well-defined topology follows because (a) both "true" and "false" are always continuous and so both $\emptyset$ and the whole of P (or P^{Λ}) are closed and (b) the class of continuous predicates is closed under arbitrary conjunctions and finite disjunctions (and so the closed sets are closed under arbitrary intersections and finite unions). (These results for general restriction operators follow in much the same ways as 2.18(xii)&(xiii) and 2.46(viii)&(ix).)

From here on we will consider only topologies of P (which correspond with predicates of a single variable). This is simply for the sake of clarity, and it is possible to extend many of the results obtained to the general space P^{Λ}.

We will first examine the topology arising from a metric defined relative to an arbitrary normal class of restriction operators. We will then show that this is the same topology which arises from definition 3.1 (for the same class of operators). Later we will see the implications of these results for the special cases of weak continuity (2.12) and strong continuity (2.44).

Suppose that $\{\lceil n \mid n \in N\}$ is a normal class of restriction operators (2.49). Define a metric on P as follows:

3.2 $d(A,A) = 0$
$A \neq B \Rightarrow d(A,B) = \frac{1}{n}$, where n is minimal w.r.t. $A\lceil n \neq B\lceil n$.

(That such an n exists when $A \neq B$ is easily shown from 2.49 .)

This is a well-defined metric, for (i) clearly $d(A,B) = d(B,A)$ for all A and B, (ii) $d(A,B) \geqslant 0$ and $d(A,B) = 0 \Rightarrow A=B$,

(iii) for all A,B&C if $A \upharpoonright n \neq C \upharpoonright n$ then clearly either $A \upharpoonright n \neq B \upharpoonright n$ or $B \upharpoonright n \neq C \upharpoonright n$ so that $d(A,C) \leqslant \max(d(A,B), d(B,C))$.

This strong type of metric (with "max" instead of the usual triangle inequality $d(A,C) \leqslant d(A,B) + d(B,C)$) has several interesting properties. Recall the following definitions (which are valid in an arbitrary metric space (P,d)).

3.3(i) An <u>open ball</u> is a set of the form $\{B \mid d(A,B) < a\}$ (denoted by $\mathbf{B}_A^a$) for any $a > 0$ and $A \in P$.

(ii) An <u>open set</u> is any union of open balls.

(iii) A <u>closed set</u> is any set whose complement is open.

(iv) (P,d) is said to have <u>dimension zero</u> if for every $A \in P$ and $\delta > 0$ there is some set $\mathbf{B}$ which contains A, is both open and closed (<u>clopen</u>) and has the property that $C \in \mathbf{B} \Rightarrow d(A,C) < \delta$.

3.4 <u>Theorem</u>

Suppose that (P,d) is a metric space which satisfies the condition $d(A,C) \leqslant \max(d,(A,B), d(B,C))$ for all $A,B,C \in P$. Then each of the following holds of (P,d).

(i) If $\mathbf{B}_A^a$ and $\mathbf{B}_C^c$ are two open balls such that $a \leqslant c$, then either they are disjoint or $\mathbf{B}_A^a \subseteq \mathbf{B}_C^c$.

(ii) $\{\bigcup \mathbf{C} \mid \mathbf{C}$ is a finite set of open balls$\}$ is a basis for the metric topology which is closed under finite intersection.

(iii) The open balls are closed sets.

(iv) (P,d) has dimension zero.

<u>proof</u>

(i) Suppose $\mathbf{B}_A^a \cap \mathbf{B}_C^c \neq \emptyset$, then $\exists D \in \mathbf{B}_A^a \cap \mathbf{B}_C^c$.
We then have that $d(A,D) \leqslant a$ and $d(C,D) \leqslant c$, so $d(A,C) \leqslant \max(a,c)$.
Hence $A \in \mathbf{B}_C^c$.
Now suppose that $D \in \mathbf{B}_A^a$, then $d(C,D) \leqslant \max(d(C,A), d(A,D))$
$\leqslant \max(c,a) = c$.
Thus $D \in \mathbf{B}_C^c$, and so $\mathbf{B}_A^a \subseteq \mathbf{B}_C^c$ as desired.

(ii) This is trivially a basis (as the set of open balls is one). It is closed under finite intersections since by (i) the intersection of two open balls is either an open ball or $\emptyset$ (which is the union of the empty set of balls).

(iii) Part (i) shows that all the distinct a-balls (for any fixed a) are disjoint. This together with the fact that

$C \in B^a_C$ gives us that for any $A \in P$ we have $B^a_A \cap U = \emptyset$, where U is the open set $\bigcup_{C \notin B_A} B^a_C$. Clearly also $B^a_A \cup U = P$, so we have $\overline{U} = B^a_A$ and so B^a_A is the complement of an open set as desired.

(iv) By part (iii) it is sufficient to take a sufficiently small open ball about a point $A \in P$, since these are now known to be clopen.

Recall the definition of a Cauchy sequence over a metric space:

3.5 If (P,d) is a metric space and $\langle A_i \mid i \in N \rangle$ is a sequence of points in P then $\langle A_i \mid i \in N \rangle$ is said to be a Cauchy sequence if $\forall \delta > 0.\ \exists n \in N.\ \forall r,s \geqslant n.\ d(A_r, A_s) < \delta$.

Note that under the conditions of 3.4 a sequence is a Cauchy sequence if it satisfies the weaker condition
$\forall \delta > 0.\ \exists n.\ \forall r \geqslant n.\ d(A_r, A_n) < \delta$.

A metric space is said to be complete if each Cauchy sequence converges to some limit, that is

$$\exists A.\ \forall \delta > 0.\ \exists n.\ \forall r \geqslant n.\ d(A, A_r) < \delta.$$

3.6 Theorem

The metric space defined relative to any normal class of restriction operators is complete.

proof

Suppose that $\langle A_i \mid i \in N \rangle$ is a Cauchy sequence relative to such a class of operators. Define functions r,n,j from Σ^* to N as follows:

$r(w)$ = minimal r s.t. $\forall B.\ w \in B \Leftrightarrow w \in B \restriction r$
(such an r exists by 2.49)

$n(w) = \max\{r(v) \mid v \leqslant w\}$

$j(w)$ = minimal j s.t. $i \geqslant j \Rightarrow d(A_i, A_j) < \frac{1}{n(w)}$
(such a j exists by definition of Cauchy seq.)

Now define $A = \langle w \mid w \in A_{j(w)} \rangle$. Claim that A is the limit of the Cauchy sequence.

A is an element of P for certainly $\langle\rangle \in A_{j(\langle\rangle)}$ and also

$v < w \in A \Rightarrow v \in A_{j(w)}$ (as $A_{j(w)} \in P$)
$\Rightarrow v \in A_{j(w)} \restriction r(v)$
$\Rightarrow v \in A_{j(v)} \restriction r(v)$ (as $d(A_{j(v)}, A_{j(w)}) < \frac{1}{r(v)}$
$\Rightarrow A_{j(v)} \restriction r(v) = A_{j(w)} \restriction r(v)$)
$\Rightarrow v \in A_{j(v)}$

Suppose that $\langle A_i \mid i \in N \rangle$ did not converge to the given A. Then there is some $\delta > 0$ s.t. $\forall m.\ \exists n.n \geq m \ \&\ d(A_n, A) > \delta$. By the definition of the metric, since $\langle A_i \rangle$ is a Cauchy sequence, for each $n \in N$ there is some m s.t. $k \geq m \Rightarrow A_k \lceil n = A_m \lceil n$. Thus there are some n&m s.t. $k \geq m \Rightarrow A_m \lceil n = A_k \lceil n \neq A \lceil n$ (choose $n > \frac{1}{\delta}$ and m as in the last sentence relative to it).

There would thus either be some $w \in \Sigma^*$ which was an element of $A \lceil n - A_k \lceil n$ for every $k \geq m$ or some $w \in \Sigma^*$ which was an element of $A_k \lceil n - A \lceil n$ for every $k \geq m$.

Suppose first that the first of these two possibilities could arise. Since $\lceil n$ is a continuous function by assumption we have $A \lceil n = \bigcup \{B \lceil n \mid B \subseteq A \ \&\ B \text{ is finite}\}$. Hence there is some finite $B \subseteq A$ such that $w \in B \lceil n$.

Suppose that $B = \{v_1, \ldots, v_s\}$; let $r = \max\{m, j(v) \mid v \in B\}$.

Since each $v_i \in A$, we have $v_i \in A_r$ (as $r \geq j(v_i)$).
Hence $B \subseteq A_r$, which implies that $w \in A_r \lceil n$, which contradicts the fact that $r \geq m$. Thus the first possibility cannot arise.

The second possibility can similarly be excluded by rev-continuity of $\lceil n$ and the fact that $A \lceil n = \bigcap \{B \lceil n \mid B \supseteq A \ \&\ B \text{ ecf}\}$ where an ecf (effectively cofinite) element of P is one which can be written in the form $\{v \mid \neg \exists u \in C.v \geq u\}$ for some finite subset C of Σ^*.

This completes our proof that $\langle A_i \mid i \in N \rangle$ does in fact converge to A as desired.

A metric space is said to be compact if every infinite sequence contains a convergent subsequence.

3.7 Theorem
The metric space defined relative to a normal class of restriction operators is compact if and only if there are only finitely many possible values for $B \lceil n$ for every $n \in N$.

proof
Suppose that there were infinitely many possible values for some n. Then we could pick an infinite sequence $\langle A_i \mid i \in N \rangle$ such that $i \neq j \Rightarrow A_i \lceil n \neq A_j \lceil n$. It is easy to see that this sequence can contain no convergent subsequence as any such subsequence would be a Cauchy sequence in which no two points were within $\frac{1}{n}$ of one another.

Suppose then that there are only finitely many values possible for each restriction operator and that $\langle A_i \mid i \in N \rangle$ is an infinite sequence of processes.

Claim that it is possible to find integers $n_{i,j}$ $(i,j \in N)$ satisfying the following conditions:

(i) $n_{i,j} < n_{i,j+1}$

(ii) $A_{n_{i,j}} \restriction i = A_{n_{i,o}} \restriction i$

(iii) $\forall j.\forall i.\exists k.k \geqslant j \;\&\; n_{i+1,j} = n_{i,k}$

We will construct these by recursion on i.

Set $n_{o,i} = i$ - these satisfy (ii) as $\restriction o$ is a one-valued function (2.49)

Suppose that we have constructed the $n_{i,j}$. By assumption there are only finitely many values taken by the $A_{n_{ij}} \restriction i+1$. Therefore there is at least one value (B say) which occurs infinitely often.

Let $n_{i+1,j}$ = jth $n_{i,k}$ s.t. $A_{n_{i,k}} \restriction i+1 = B$.

It is easily seen that these $n_{i+1,j}$ satisfy all that is required of them.

Note that this proof requires the use of the Axiom of Choice in the choosing of value B.

Having constructed the $n_{i,j}$ set $m_i = n_{i,i}$. These satisfy $m_i < m_{i+1}$ (by (i)&(iii) above) and $i,j \geqslant k \Rightarrow A_{m_i} \restriction k = A_{m_j} \restriction k$ (by (ii)).

Thus $i,j \geqslant k \Rightarrow d(A_{m_i}, A_{m_j}) < \frac{1}{k}$ so that the $\langle A_{m_i} \mid i \in N \rangle$ are a Cauchy subsequence of $\langle A_i \mid i \in N \rangle$. By 3.6 this subsequence has a limit and so $\langle A_i \mid i \in N \rangle$ has a convergent subsequence as desired.

Note that this result gives us that (P,d) can only be compact when Σ is countable, for every element of P can in some sense be identified with the sequence of its restrictions $(A \restriction n)$ and the cardinal of these sequences is at most **c** (continuum) if each $\restriction n$ has a finite range. (This also follows more conventionally from the fact that every compact metric space is separable.)

The following result shows that all restriction operators giving rise to compact metric spaces give rise to the same topology.

3.8 Theorem

Over any space of processes all normal classes of restriction operators inducing compact metric spaces induce the same topology. In the case where Σ is countable the restriction operators inducing strong continuity induce a compact metric space (and hence the only possible such topology).

proof

We know that there can be no such metric when Σ is uncountable (by the remarks above) so it is sufficient to consider only the case of countable Σ. That the class of operators described in 2.54 give rise to a compact metric space is an immediate consequence of 3.7, since plainly there is only a finite number of possible values which can be taken by each one.

Suppose that $\{\restriction n \mid n \in N\}$ and $\{\restriction' n \mid n \in N\}$ are two classes of restriction operators giving rise to compact metric spaces, and that their associated metrics are d and e respectively. To show that the topologies are the same it is sufficient, by symmetry, to show that every d-closed set is also e-closed. We will use the fact that a set is closed in a metric space if and only if it contains all its accumulation points (i.e. the points which are the limits of convergent sequences contained entirely within the set).

Suppose that X is a d-closed set. To show that it is e-closed we must show that every e-convergent sequence has its limit in X. Suppose that $\langle A_i \mid i \in N \rangle$ is an e-convergent sequence with limit A. By compactness of the metric space (P,d) there is a d-convergent subsequence, say $\langle A'_i \mid i \in N \rangle$, with a limit A', say. Being a subsequence of $\langle A_i \mid i \in N \rangle$ this must be e-convergent with limit A. It is sufficient to show that A = A', for A' is in X since it is the limit of a d-convergent sequence in X. Suppose $w \in \Sigma^*$; since both classes of operators are normal there exist integers r & s s.t. for all $C \in P$ $w \in C \Leftrightarrow w \in C\restriction r$ and $w \in C \Leftrightarrow w \in C\restriction' s$. Let $m = \max(r,s)$; it is easily shown that $w \in C \Leftrightarrow w \in C\restriction m \Leftrightarrow w \in C\restriction' m$. By construction there exists some $n \in N$ s.t. $d(A'_n, A') < \frac{1}{m}$ and $e(A'_n, A) < \frac{1}{m}$. This tells us that $A'_n\restriction m = A'\restriction m$ and $A'_n\restriction' m = A\restriction' m$.

We thus have $w \in A' \Leftrightarrow w \in A'\lceil m$

$\Leftrightarrow w \in A'_n\lceil m$

$\Leftrightarrow w \in A'_n$

$\Leftrightarrow w \in A'_n\lceil' m$

$\Leftrightarrow w \in A\lceil' m$

$\Leftrightarrow w \in A$

Since this holds for all w we thus must have $A = A'$ as desired.

Observe that the above proof shows that each d-closed set is e-closed simply by assuming that (P,d) is compact. This shows directly that the topology induced by a compact metric space of the type we are studying is weaker than that induced by any other (i.e. has less closed sets). We will shortly see that this is very much the same result as 2.50.

The opposite role to the compact topology is played in a much less interesting way by the classical discrete topology in which all subsets are open and closed. An example of a normal class of operators giving rise to this topology is the following.

$A\lceil *o = \underline{\text{abort}} \qquad (A \in P)$

$A\lceil *n = A \qquad (n > o)$

Note that the metric which this class induces is the usual discrete metric.

We are now in a position to establish the fundamental connection between the metric spaces described above and the corresponding topologies of continuous predicates which were described in 3.1. We show that the metric topology and the continuous predicate topology are the same. By doing this we are able to use results obtained about the topological properties of spaces of processes to classify the continuous predicates. We are also enabled to prove certain results on the satisfiability of predicates, a topic which is often in practical situations one of the most difficult to deal with.

3.9 Theorem

Suppose that $\{\lceil n \mid n \in N\}$ is a normal class of restriction operators. Let d be the metric defined on P relative to this class (3.2). Then a predicate R is continuous relative to this class if and only if $\{B \mid R(B)\}$ is a closed set in the metric space (P,d). In other words the topology induced by the metric d is the same as that introduced in 3.1.

proof

We use the result that a set is closed if and only if it contains all its accumulation points (i.e. points which are the limits of convergent sequences contained wholly within the set).

Suppose first that R is a continuous predicate and that $\langle A_i \mid i \in N\rangle$ is a convergent sequence contained in the set $\{B \mid R(B)\}$ (with limit A, say). Then for each $n \in N$ there must be some i s.t. $d(A,A_i) < \frac{1}{n}$, so that $A\lceil n = A_i\lceil n$ and $R(A_i)$. R(A) then follows by definition of continuity (2.13).

Thus $\{B \mid R(B)\}$ contains all its accumulation points, and so is a closed set.

Secondly suppose that $\{B \mid R(B)\}$ is a closed set and that $a \in P$ is such that $\forall n.\exists B_n.(A\lceil n = B_n\lceil n)$ & $R(B_n)$.
These B_n clearly form a Cauchy sequence converging to A (as $m \leqslant n \Rightarrow B_n\lceil m = A\lceil m$). Hence R(A) holds as $\{B \mid R(B)\}$ is closed and so contains its accumulation points.

Thus R is continuous by 2.13.

We can thus now start to apply results of topology to our predicates. The first two results we obtain concern the satisfiability of predicates.

3.10 Theorem

If $\langle R_n \mid n \in N\rangle$ is a sequence of continuous predicates (relative to some normal class of operators) such that $R_{n+1} \Rightarrow R_n$ and if $\langle A_n \mid n \in N\rangle$ is a sequence of processes such that $A_{n+1}\lceil n = A_n\lceil n$ and $R_n(A_n)$ holds for each n, then there is some $A \in P$ s.t.

(i) $A\lceil n = A_n\lceil n$ for all n

(ii) $R_n(A)$ holds for each n.

proof

Denote by $\mathfrak{R}^a$ the subset $\{\bigcup\{B_A^a \mid A \in \mathbf{C}\} \mid \mathbf{C} \subseteq P\}$ of $\mathfrak{B}$.

Note that $a \geqslant b \Rightarrow \mathfrak{R}^a \subseteq \mathfrak{R}^b$, for if $\mathbf{E} \in \mathfrak{R}^b$ then

$$\mathbf{E} = \bigcup\{B_A^a \mid A \in \mathbf{E}\} .$$

(The containment of the L.H.S. within the R.H.S. is obvious, the reverse one following from 3.4(i).)

To show that $\mathfrak{B}$ is closed under finite intersections and unions it will thus be sufficient to show that each $\mathfrak{R}^a$ is. (This is because in any finite intersection of elements of $\mathfrak{B}$ there will be some minimal "a".)

The union case is easy: clearly $\bigcup\{B_A^a \mid A \in C\} \cup \bigcup\{B_A^a \mid A \in D\}$ $= \bigcup\{B_A^a \mid A \in (C \cup D)\}$.

In the intersection case we have

$$\bigcup\{B_A^a \mid A \in C\} \cap \bigcup\{B_A^a \mid A \in D\} = \bigcup\{B_A^a \cap B_B^a \mid A \in C \ \& \ C \in D\}$$

which is an expression of the correct form since each of the $B_A^a \cap B_B^a$ is either empty or B_A^a (by 3.4 (i)).

$\mathfrak{B}$ certainly now contains the basis of 3.4 (ii) for it contains each ball B_A^a individually and is closed under finite unions. Each element of $\mathfrak{B}$ is open by construction (union of open sets). These two facts together tell us that $\mathfrak{B}$ is a basis. Each element is closed since it is the complement of the union of those balls os the same radius which are disjoint from it (an open set). Thus every element is clopen.

If the space is compact then there are only finitely many balls of any given radius (as in 3.7) and so each element of $\mathfrak{B}$ is a finite union, and so is contained in the original basis. Hence in this case the two bases are the same.

If the space is not compact then by 3.7 there is some n such that $\lceil n$ takes infinitely many values. Without loss of generality we can assume that n is minimal with respect to this property. There can only be finitely many values taken by all $\lceil m$ such that $m < n$, in particular n-1 ($n > 0$ as $\lceil o$ is one-valued). Pick elements $A_1, A_2, \ldots$ of P with distinct images under $\lceil n$. Since there are only finitely many values of $\lceil n-1$ we can pick an infinite number of the A_is which take the same value under $\lceil n-1$ ($A_1', A_2', \ldots$ say).

Let $\mathbf{C} = \{A'_{2i} \mid i \in N\}$; by construction $\bigcup\{B^{\frac{1}{4}}_A \mid A \in \mathbf{C}\}$ (= X) is an element of $\mathfrak{B}$. We need to show that X cannot be expressed as a finite union of balls. Suppose that $X = B_1 \cup B_2 \cup .. \cup B_k$ where each B_i is a ball. The radius of each of the B_i must be $\leqslant \frac{1}{n}$, since (i) all the A'_i (and hence every point of X) takes the same value under $\lceil n-1$ (ii) thus the "centre" of such a ball would also have to take this value and so (iii) each A'_{2i+1} is also in the ball (which contradicts the fact that $A_1 \notin X$). However this implies that each A'_{2i} is contained in a different B_j, since it is easily seen that no ball of radius $\leqslant \frac{1}{n}$ can contain two points whose distance is $\frac{1}{n}$ (in a metric satisfying the conditions of 3.4). This clearly makes impossible our supposition that there are only a finite number of balls in the union.

The next result completely classifies the space of clopen sets in the compact case, showing that in this case the clopen sets correspond exactly to $\mathfrak{B}$ (and hence to the original basis).

3.13 Theorem

In cases where (P,d) is compact a subset X of P is clopen if and only if it is in $\mathfrak{B}$ (and so can be expressed as a finite union of balls).

proof

Suppose that (P,d) is compact and that X is a clopen set. Since X is an open set it can be expressed as a countable union of balls (countable since when (P,d) is compact there are only countably many balls). We can assume that this expression is infinite, for otherwise the result is immediate. Since there are only a finite number of balls of any given radius we can assume that the balls are expressed in order of descending radius: $B_1, B_2, \ldots$.
If $\bar{X}$ were expressible as a finite union of balls then so would be X (this being because then $X = \bigcup\{B^a_A \mid A \in X\}$, where a is any number smaller then the smallest radius occurring amongst the expression for $\bar{X}$, but this union is only finite because for any a there are only finitely many a-balls). Since $\bar{X}$ is open it can also be expressed as a countable infinite union of balls of descending radius: $B'_1, B'_2, \ldots$.

We can assume that all of the balls B_i and B_i' are disjoint. Let $Z_i = (B_1 \cup B_1' \cup B_2 \cup \ldots \cup B_i \cup B_i')$. By construction Z_i is open and so $\overline{Z}_i$ is closed. Also $\overline{Z}_i$ is non-empty ($B_{i+1} \subseteq \overline{Z}_i$) and $\overline{Z}_{i+1} \subseteq \overline{Z}_i$ for every i. The $\overline{Z}_i$ are thus a non-empty descending sequence of closed sets in a compact metric space. Hence there is some point in their intersection, A*, say. This however contradicts the fact that $\bigcup_{i=0}^{\infty} Z_i = P$ ($= \mathbf{X} \cup \overline{\mathbf{X}}$), so we must conclude that this case, where **X** is not expressible as a finite union of balls, cannot arise. This completes the proof of our result.

3.14 Corollary

When Σ is countable a predicate R and its negation $\neg R$ are both strongly continuous if and only if R can be expressed finitely in terms of propositions of the form "$w \in A$" ($w \in \Sigma^*$), "$\neg$" and "$\vee$".

proof

That each predicate R expressed in these terms has both R and $\neg R$ strongly continuous is easily proved by induction, because each of the sets $\{A \mid w \in A\}$ is clopen ($w \in \Sigma^*$) and the space of clopen sets is closed under complementation and finite unions.

That every R with both R and $\neg R$ strongly continuous can be written in this form follows because the set $\{A \mid R(A)\}$ is clopen, and so can be written as a finite union of balls in the metric space induced by the restriction operators given in 2.54. (Every ball can be written finitely in terms of "$\neg$" and "$\wedge$" and "$w \in A$", which is translatable into the desired form.)

Note that it is a corollary to 3.8 that all normal classes of restriction operators which give compact metric spaces have the same class of continuous predicates, and so the above theorem is equally valid for each of them.

It is possible to give a general classification of all clopen sets and hence of all "doubly continuous" predicates for general classes of restriction operators. Before we do this we need a normal form result for closed and for open sets.

3.15 Lemma

If d is the metric defined relative to some normal class of restriction operators then a set X is open in (P,d) if and only if it can be written in the form $\bigcup_{i=1}^{\infty} C_i$, where $C_n \in \mathfrak{R}^{\frac{1}{n}}$, (as defined in the proof of 3.12), $C_i \cap C_j = \emptyset$ if $i \neq j$ and for any $a > \frac{1}{n}$ & $A \in P$ we have $B_A^a \not\subseteq \bigcup_{i=n}^{\infty} C_i$. This expression for X in terms of the C_i is unique for each open set X.

Under the same conditions a set X is closed in (P,d) if and only if it can be written in the form $\bigcap_{i=1}^{\infty} C_i$, where $C_n \in \mathfrak{R}^{\frac{1}{n}}$, $C_{n+1} \subseteq C_n$ and for all $a \geqslant \frac{1}{n}$ & $A \in P$ we have $B_A^a \cap X = \emptyset \Rightarrow C_n \cap X = \emptyset$. This expression is unique for each closed set X.

This result is a fairly easy consequence of 3.12.

It follows that the following four conditions are equivalent for any set X.

(a) X is clopen.
(b) X can be written in each of the forms given above.
(c) X and $\overline{X}$ can be written in the first (open) form above.
(d) X and $\overline{X}$ can be written in the second form above.

In particular a set X is clopen if and only if there are some C_i and C_i' such that $X = \bigcap_{i=1}^{\infty} C_i$ and $\overline{X} = \bigcap_{i=1}^{\infty} C_i'$, both sequences satisfying the conditions of the second half of 3.15. Consider the sets $D_i = C_i \cap C_i'$. By construction these are closed sets satisfying the conditions $D_{n+1} \subseteq D_n$ and $\bigcap_{i=1}^{\infty} D_i = \emptyset$. This can arise in two essentially different ways: either $D_i = \emptyset$ for some $i \in N$ or not. In the first case we have that $C_j = C_i$ for all $i < j$ (since $C_j \subseteq C_i$ & $C_j \cup \overline{C}_j = P$) which tells us that $X = C_i$. Thus $X \in \mathfrak{B}$. It is also true that if $X \in \mathfrak{B}$ then $D_i = \emptyset$ for some i (any i s.t. $\frac{1}{i} < a$, where a is such that $X = \bigcup \{B_A^a \mid A \in C\}$). Thus the first case arises exactly when X lies in the class of clopen sets which we have already identified, namely $\mathfrak{B}$. The other case (which cannot arise when the metric space is compact) is harder to describe exactly.

The following result gives an exact but not very elegant list of all the clopen sets (including the first case). For an example of what one of the second case sets looks like see 3.17.

This characterisation of clopen sets is unfortunately rather too abstract to yield a very useful tool in identifying the "doubly continuous" predicates in a given system. It should be said though that apart from the "finite" ones which are easily identified (i.e. ones which correspond to some element of $\mathfrak{B}$) these predicates are rarely of much practical use. The following is an example of a doubly continuous predicate which is not finite (in the sense defined above), in the system defined by weak continuity (2.6 et seq.) with alphabet containing N, the natural numbers. The derivation of the corresponding set from 3.16 requires one application of rule (ii).

3.17 Example

Let A_n (for $n \in N$) be the process $n \to (n \to ..(n \to \underline{skip}))..)$ (n "n"s). Then the predicate $R(A) \equiv \exists n.A=A_n$ is doubly continuous but not finite with respect to weak continuity.

The basic principle at work here is that one can tell in a finite time (after one step) exactly how long one has to wait to know whether or not the predicate holds. It is generally true that all doubly continuous predicates result from the compounding of this principle.

Note that neither the above R nor its negation $\neg R$ is strongly continuous. This is because we can find convergent sequences of processes satisfying the predicate ($\langle A_n | n \in N \rangle$ as a sequence has limit abort) and not satisfying it ($\langle A_o \sqcap A_{n+1} | n \in N \rangle$ which has limit A_o) whose limits act oppositely. However this does not extend to a general principle, for if we were to substitute abort into the definition of A_n in place of skip the resulting R would still be doubly weakly continuous but now R would be strongly continuous (though of course not $\neg R$).

There are several results about continuous predicates which follow from the zero-dimensionality of our metric spaces.

3.18 Theorem (Sharpened normality property)

If R and S are two inconsistent predicates, continuous relative to some normal class of restriction operators, then there is a doubly continuous predicate T such that $R \Rightarrow T$ and $S \Rightarrow \neg T$.

3.16 Theorem

In the metric space (P,d) defined relative to some normal class of restriction operators the space $\mathfrak{H}$ of clopen sets satisfies the following:

(i) $\mathfrak{B} \subseteq \mathfrak{H}$.

(ii) If for any $n \in N$ we have a family $\mathfrak{N}$ of clopen sets satisfying $X,Y \in \mathfrak{N}$, $X \neq Y$, $A \in X$ & $B \in Y \Rightarrow A\restriction n \neq B\restriction n$ then $\bigcup\mathfrak{N} \in \mathfrak{H}$.

$\mathfrak{H}$ is the smallest collection of sets satisfying the above.

proof

We will first show that $\mathfrak{H}$ satisfies condition (ii) above (we already know that it satisfies condition (i)). Let $\mathfrak{N}$ be a family of clopen sets satisfying the hypotheses in condition (ii) above for some $n \in N$, and let $X = \bigcup\mathfrak{N}$. That X is open follows from the fact that it is a union of open sets. X is closed since the tail of any convergent sequence contained in X must be contained in one of the elements of $\mathfrak{N}$, and so its limit is contained in that element.

Secondly we will show that every clopen set can be derived from (i) & (ii) above. Define $\mathfrak{G}$ to be the family of clopen sets which can be so derived, and suppose that X is clopen. Observe first that for any n and any such X at least one element of $\{X \cap \{A \mid A\restriction n = B\restriction n\} \mid B \in P\}$ is clopen and not in $\mathfrak{G}$. (Every element of this set is clopen by construction, and if each were in $\mathfrak{G}$ then so would be X as it is the union of a family of elements of $\mathfrak{G}$ satisfying (ii) for n.) Set $X_o = X$, and for any n choose X_{n+1} to be one of the $X_n \cap \{A \mid A\restriction n+1 = B\restriction n+1\}$ which is of the offending form. Each of the X_i is nonempty (since $\emptyset \in \mathfrak{G}$) so we can pick a sequence $\langle A_i \mid i \in N\rangle$ s.t. $A_i \in X_i$. By construction this sequence is Cauchy, and hence convergent to some $A^* \in P$. Certainly $A^* \in X$, since each $A_i \in X$ and X is closed, but also for each n we must have $X_n \neq \{A' \mid A'\restriction n = A_n\restriction n\}$ (for this set is in $\mathfrak{G}$). We can therefore pick a second sequence $\langle A'_n \mid n \in N\rangle$ such that $A'_n\restriction n = A_n\restriction n$ and such that $A'_n \notin X_n$. This means that $\langle A'_n \mid n \in N\rangle$ also converges to A^*, and also that $A'_n \in \overline{X}$ (it is easy to see that $X_n = X \cap \{A' \mid A'\restriction n = A_n\restriction n\}$). Hence $A^* \in \overline{X}$, as $\overline{X}$ is closed, which is a contradiction. We may thus conclude that our assumption that such an X exists is false.

proof

It is sufficient (by the correspondence theorem 3.9) to show that in the corresponding metric space every two disjoint closed sets can be separated by a clopen set. We will show that this is true in any metric space which satisfies the conditions of 3.4.

Suppose that (P,d) is such a space, and that X and Y are a pair of disjoint closed subsets of P. It is clear that given any point of X there is some $n \in N$ such that the (clopen) ball of radius 2^{-n} about it is disjoint from Y, for otherwise we could find a convergent sequence of points in Y converging to a point in X.

For each $A \in X$ define $B(A)$ to be the $B_A^{2^{-n}}$ of least n such that it is disjoint from Y. It is not hard to see that by 6.4(i) $B(A) \cap B(A') \neq \emptyset \Rightarrow B(A) = B(A')$ for all $A,A' \in X$ (if they are not disjoint then one is contained in the other, but if either had strictly smaller radius than the other it would not have maximal possible radius with respect to being disjoint from Y).

Now define $Z = \bigcup_{A \in X} B(A)$. Claim that Z is clopen (it is trivially disjoint from Y and contains the whole of X as $A \in B(A)$ for all $A \in X$).

Z is open by construction, since it is the union of a set of open balls.

If Z were not closed then there would be a sequence of points $A_1, A_2, \ldots$ which converged to a point A^* not in Z. There are essentially two cases to consider: <u>either</u> infinitely many of the A_i lie in one of the $B(A)$ <u>or</u> not (in which case there must be an infinite collection of the balls $B(A)$ $(A \in X)$ containing them).

In the first case it is easy to see that (if $A \in X$ is such that infinitely many A_i are in $B(A)$) there is an infinite subsequence which lies in $B(A)$, which tells us that $A^* \in B(A)$ as $B(A)$ is closed by 6.4(iii). Thus this case cannot arise.

In the second case either arbitrarily small balls appear amongst the $B(A_i')$, where $A_i' \in X$ is such that $A_i \in B(A_i')$, or not. If this is not the case and b is the smallest radius occurring among the $B(A_i')$ then it is clear that the entire sequence $A_1, A_2, \ldots$ is contained in the clopen (by 3.12)

subset $\bigcup_{i=1}^{\infty} B^{a}_{A_i}$ of Z. But this would imply that $A^* \in Z$, so this possibility cannot arise. If arbitrarily small balls do appear among the $B(A'_i)$ then without loss of generality we can assume that the radii of the $B(A'_i)$ are strictly decreasing. (This is because some infinite subsequence of the A_i must then have this property.) For all n we then have that $d(A_n, A'_n) \leqslant 2^{-n}$. This is easily seen to imply that $\langle A'_i \mid i \in N \rangle$ converges to A^*. This however is impossible since then, because X is closed we must have $A^* \in X \subseteq Z$.

It is interesting to see how the topological notions of convergence and continuous functions relate to the ideas we met in the previous two chapters. It is in fact easy to see that a sequence of processes converges in the sense of 2.42 if and only if it converges relative to the corresponding metric (both ideas are equivalent to there being for every $w \in \Sigma^*$ a point in the sequence after which w is either always present or always absent).

It is possible for a function to be continuous in the topological sense (i.e. inverse images of open sets being open) without being continuous in the lattice sense, as a function can be topologically continuous without being monotonic. We can for example divide P into two clopen sets, pick any two points we wish in P and have the function which maps one set to one point and the other to the other topologically continuous. There are though some weaker comparisons possible.

3.19 Theorem

Suppose that (P,d) is a metric space induced by a class of restriction operators giving a compact space. Then a function $f:P \to P$ which is doubly continuous in the lattice sense is topologically continuous. Furthermore every function which is topologically continuous and monotone is also (lattice) doubly continuous.

proof

The first part of this follows from the facts that a function is continuous in (P,d) if and only if it preserves the limits of convergent sequences, that the two types of convergence are the same (see above), and that a doubly continuous function preserves the limits of convergent sequences (2.48).

The second part follows since as (P,d) is compact Σ must be countable. This means that for any $A \in P$ we can find sequences $\langle A_i \mid i \in N\rangle$ and $\langle A'_i \mid i \in N\rangle$ which consist respectively of increasing finite processes and decreasing ecf processes, each of which converges to A. By topological convergence we get that each of $\langle f(A_i) \mid i \in N\rangle$ and $\langle f(A'_i) \mid i \in N\rangle$ is convergent with limit $f(A)$. This combined with monotonicity easily yields the desired result that $f(A) = \bigcup\{f(B) \mid B \subseteq A \ \&\ B \text{ is finite}\} = \bigcap\{f(B) \mid B \supseteq A \ \&\ B \text{ is ecf}\}$.

Note that 2.46(vii) extends the first part of this result to the case of strong continuity over uncountable alphabets, since it tells us that the inverse image of a closed set under a doubly continuous function is closed (in the topology defined as in 3.1 by reference to strong continuity).

The above result can be regarded as an explanation of the connection which we observed between strong continuity of predicates and doubly continuous functions.

Other classes of restriction operators relate less well to lattice continuity. For example in the case of weak continuity (with its usual metric) there are lattice continuous functions which are not topologically continuous, and monotonic topologically continuous functions which are not lattice continuous.

3.20 Examples

(i) The function $f:P \to P$ defined by $f(A) =$ abort if A^o is finite, $f(A) =$ skip if A^o is infinite, is both monotone and topologically continuous but is not lattice continuous whenever Σ is infinite.

(ii) Suppose that $N \subseteq \Sigma$ and that $b \in \Sigma$. The function $f:P \to P$ defined $f(A) = \{\langle\rangle\} \cup \{\langle n\rangle \mid \langle \overset{n}{\overbrace{bb..b}}\rangle \in A\}$ is lattice doubly continuous but not topologically continuous.

The second example works because it maps the convergent sequence $\langle B_i \mid i \in N\rangle$ (where $B_i = \{\langle\rangle, \langle b\rangle, \langle bb\rangle, \ldots, \langle \overset{i}{\overbrace{bb..b}}\rangle\}$) to the non-convergent sequence $\langle \{\langle n\rangle \mid n \leqslant m\} \cup \{\langle\rangle\} \mid m \in N\rangle$.

It is however possible to recast the usual ϵ-δ metric space continuity criterion in a more familiar form:
$\forall B \in P.\ \exists g:N \to N$ s.t. $\forall A.(A \restriction g(n) = B \restriction g(n)) \Rightarrow f(A) \restriction n = f(B) \restriction n$.

The above formula, which holds for a function f if and only if f is continuous in the topological sense, is rather like 2.18(x) (though slightly stronger). That this should be so is of course quite natural, since 2.18(x) plays the same role for weak continuity as 2.46(vii) does for strong continuity.

The next question to ask is how constructive functions behave in our metric spaces. It will be seen immediately that a constructive function has the effect of reducing the distance between two points, and that a non-destructive function is one which guarantees not to reduce the distance between two points. One gets a slightly preferable picture at this point by altering the metric slightly: let d' be the metric defined by setting $d'(A,A) = 0$ and $d'(A,B) = \frac{1}{2^n}$, where n is minimal with respect to $A\restriction n \neq B\restriction n$ (if $A \neq B$). This alteration does not affect our earlier work except in minor computational details, all results still stand in the metric space (P,d'). The advantage gained is that a constructive map now becomes a contraction mapping: for all $A,B \in P$, if f is constructive then $d'(f(A),f(B)) \leqslant \frac{1}{2}d'(A,B)$. It is possible to derive all our basic results about existence of fixed points and recursion induction from this fact alone. This topic and the wider uses of contraction mappings deserve more attention, but we will leave it here.

Following Scott ( ) it is possible to define a topology $\mathfrak{T}$ whose continuous functions correspond exactly to the lattice continuous functions.

3.21 Theorem

Let $\mathfrak{T}$ be the topology generated by the subbasis $\mathfrak{S} = \{\{A \mid A \supseteq B\} \mid B \in P \ \& \ B \text{ finite}\}$. Then a function $f:P \to P$ is continuous in this topology if and only if it is continuous in the usual lattice sense.

The proof of this result is omitted, being very similar to the usual proof over P(N). This topology is very much weaker than any of the ones associated with restriction operators. It is T_0 (i.e. given any pair of distinct points there is an open set containing one and not the other) but not T_1.

Before we summarise the implications of this chapter we will see one more result: an alternative characterization of the topology induced by our compact metric space.

3.22 Theorem

If $A,B \in P$ define the interval $[A,B]$ to be the set $\{C \mid A \subseteq C \subseteq B\}$. The set $\mathfrak{I}$ of intervals is closed under intersection. Let $\mathfrak{U}$ be the weakest topology on P in which all intervals are closed. $\mathfrak{U}$ is the same as the topology induced by strong continuity when Σ is countable (and hence is also the same as the metric topology induced by the operators described in 2.54).

proof

The set $\mathfrak{U}^c$ of closed sets in the topology is the following:

(i) $\mathfrak{I} \subseteq \mathfrak{U}^c$

(ii) $\mathfrak{U}^c$ is closed under taking finite unions.

(iii) $\mathfrak{U}^c$ is closed under taking arbitrary intersections.

(iv) $\mathfrak{U}^c$ is the smallest set satisfying (i)-(iii).

That these are the closed sets of some topology is not hard to prove, and having done this the resulting topology must by construction be the weakest one in which all intervals are closed.

Let $\mathfrak{C}$ be the set of closed sets of the topology induced by strong continuity (3.1). To prove our result it is sufficient to show that $\mathfrak{U}^c = \mathfrak{C}$. That $\mathfrak{U}^c \subseteq \mathfrak{C}$ follows inductively from the fact that the predicate induced by each interval is strongly continuous (2.46(i,ii,viii)) and the fact that $\mathfrak{C}$ is closed under finite unions and arbitrary intersections.

To prove that $\mathfrak{C} \subseteq \mathfrak{U}^c$ it is sufficient to prove that each element of the known basis for $\mathfrak{C}$ is in $\mathfrak{U}^c$ (as the complement of each basis element is also in , so we are showing that each is also open in $\mathfrak{U}$). Since there are only finitely many balls of a given radius and $\mathfrak{U}^c$ is closed under finite intersections it is sufficient to show that all balls B^a_A are in $\mathfrak{U}^c$. It is easily seen that for every ball there is an expression which has the form $Z_o \cap Z_1 \cap \ldots \cap Z_n$, where Z_i is either $\{A \mid w_i \in A\}$ or $\{A \mid w_i \notin A\}$ ($\{w_o, w_1, \ldots\}$ the enumeration of Σ^* in 2.54) and n is minimal with respect to $\frac{1}{n} < a$ (radius of the ball). It

is sufficient therefore to show that each possible Z_i is an interval. To do this we simply observe that

$$\{A \mid w \in A\} = [\{v \mid v \leqslant w\}, \underline{run}] \quad (\underline{run} \text{ is maximal in } P)$$
$$\{A \mid w \notin A\} = [\underline{abort}, \{v \mid w \not\leqslant v\}] \quad (\text{if } w \neq \langle\rangle)$$
$$= [\underline{run}, \underline{abort}] \quad (\text{if } w = \langle\rangle).$$

This completes the proof of 3.22.

This result is pleasing, since it shows that the topology induced by all compact metrics and strong continuity is quite a natural one. It can be used to prove results of closed sets (and hence of strongly continuous predicates) inductively. If a property holds of all the basic intervals ($[\underline{abort}, A]$, $[A, \underline{run}]$) and is preserved by finite union and arbitrary intersection then it holds of all closed sets in $\mathfrak{C}$. In the language of predicates this translates to the following inductive principle: if a property holds of each predicate of the form $R(A) = A \supseteq B$ or $R(A) = A \subseteq B$ $(B \in P)$ and is preserved by finite disjunctions and arbitrary conjunctions then it holds of all strongly continuous predicates. (Both of these principles hold only when Σ is countable.) One application of this is an alternative proof of 2.46(vii), which becomes an immediate consequence of 2.46(v,vi,viii,ix). Several of our other results have alternative proofs using the same principle. If desired this principle can be strengthened: it is in fact only necessary to show that a property holds of all of the basic predicates above with B finite and ecf in the respective cases. This is because every other of the basic predicates can be expressed as a conjunction of ones of this form.

To conclude this chapter we will take stock of our results, paying particular attention to how they affect our understanding of the two main classes of continuous predicates we met in chapter 2.

We have seen that given any normal class of restriction operators on P we can define a corresponding metric space in a natural way, and that the closed sets of this metric space correspond in a natural way to the predicates which are continuous relative to the class of restriction operators. This corresponds to the fact that (as we already

knew) continuous predicates are closed under finite disjunctions and arbitrary conjunctions. We found that our metric spaces were of a very discrete kind, and were complete. Completeness was used to prove a satisfiability result. We found that the metric space was compact only when the predicates continuous with respect to a class of restriction operators were exactly the strongly continuous ones, and Σ was countable. We re-established the fact that a strongly continuous predicate is continuous with respect to all other normal operator classes, and also discovered that strong continuity is in several ways better behaved than other sorts (e.g. 3.11, 3.13, 3.14, 3.19 & 3.21). In investigating how continuous functions in the metric space behave we discovered another way of treating constructive functions.

Below is a summary of the results affecting our knowledge of weakly and strongly continuous predicates.

a) Weakly continuous

(i) 3.10 (which is obvious in this case anyway)

(ii) 3.15 (which can be adapted to give a normal form for weakly continuous predicates)

(iii) 3.16 (which classifies the predicates which are "doubly continuous")

(iv) 3.18 (the application of which is helped by our classification of doubly continuous predicates)

b) Strongly continuous

Each of the above also holds in this case, except that 3.14 plays the role of 3.15. In addition we have:

(i) 3.11

(ii) The explanation of the connection with doubly continuous functions.

(iii) The inductive principles which come from 3.22.

It is possible to prove most of the above without consideration of topology or metric spaces, and indeed it is possible to do much of the topology (e.g. 3.13 & 3.22) without using metric considerations. The use of metric spaces does however often seem to be the most convenient and elegant way to deal with continuous predicates.

Appendix: A summary of some later results.

The results we have so far met in this chapter do not tell us a great deal about the case of strong continuity when Σ is uncountable. Most of the following results are extensions of existing results to this case (or demonstrations that existing results do not then apply). The first theorem is however an additional classification of strong continuity over countable alphabets.

3.23 Theorem

The topology induced by strong continuity is homeomorphic to the usual metric topology of the Cantor set if and only if Σ is countably infinite.

This follows quite easily from theorem 30.3 of Willard( ), since if Σ is infinite every point is the limit of a sequence of points distinct from itself, whereas if Σ is finite the process abort is not.

3.24 Theorem

The topology induced by strong continuity is, when Σ is uncountable, neither first countable, metrizable nor compact.

That it is not first countable follows from the fact that there exists an uncountable set $\{\{\langle\rangle, \langle a\rangle\} | a \in \Sigma\}$ of nearly disjoint processes. If the topology were first countable there would exist a sequence of closed sets C_j such that abort $\notin C_i$, $C_i \subseteq C_{i+1}$, and whenever X is a closed set not containing abort there exists some j s.t. $X \subseteq C_j$. One can then show that one of the C_j must contain infinitely many of the one point closed sets $\{\{\{\langle\rangle, \langle a\rangle\}\} | a \in \Sigma\}$ as subsets; but this implies that this C_j contains a convergent sequence of points converging to abort, contradicting the fact that abort $\notin C_j$.

That it is not metrizable (and hence not the topology induced by any normal class of restriction operators) follows from the fact that every metric space is first countable.

The fact that it is not compact follows from the fact that we can find (under the continuum hypothesis) an infinite set of points with no limit point. This is because under the continuum hypothesis it is clearly sufficient to show that this can be done for any particular alphabet of

cardinal $2^{\aleph_0}$. Now let $\Sigma = \{f \mid f:N \to N\}$, and define $A_i = \{\langle\rangle, \langle f\rangle \mid \exists k.\ f(2k)=i\}$. If the set $\{A_i \mid i \in N\}$ were to contain a limit point it is easy to show that there would have to exist some 1-1 function f such that the sequence $\langle A_{f(i)} \mid i \in N\rangle$ was convergent; but for any such sequence it is easy to see that $\langle f\rangle \in \text{limsup}A_{f(i)}$ but $\langle f\rangle \notin \text{liminf}A_{f(i)}$.

The next few results show that by generalizing the idea of convergent sequences we can find a new class of predicates, the extra continuous ones, which (i) is contained in the class of strongly continuous predicates, coinciding with it when Σ is countable; (ii) gives rise to a more pleasant topology; and (iii) generalizes theorem 2.53.

Let us extend the notion of sequence to include functions from arbitrary non-empty directed sets to P. We will call such a sequence a <u>generalized sequence</u> and a sequence from non-empty directed set D to P a <u>D-sequence</u>. If f is a D-sequence and D* is a subset of D with the property that for each $d \in D$ there exists some $d^* \in D^*$ s.t. $d^* \geqslant d$ we will say that $f\restriction D^*$ is a <u>subsequence</u> of f (it is easy to see that each such D* must be directed). If f is a D-sequence define $\text{limsup}(f) = \bigcap_{d\in D}(\bigcup_{e\geqslant d} f(e))$ and $\text{liminf}(f) = \bigcup_{d\in D}(\bigcap_{e\geqslant d} f(e))$. Say that f converges to A (or $f \to A$) if $\text{limsup}(f) = A = \text{liminf}(f)$. Say that a predicate R is <u>extra-continuous</u> if it satisfies the condition that whenever f is a convergent generalized sequence of points satisfying it then lim(f) satisfies R also. The following is a compilation of some easy results about generalized sequences.

3.24 <u>Theorem</u>

(i) For each generalized sequence f we have $\text{liminf}(f) \subseteq \text{limsup}(f)$.

(ii) All finite generalized sequences converge,

(iii) If f* is a subsequence of f then $\text{liminf}(f) \subseteq \text{liminf}(f^*) \subseteq \text{limsup}(f^*) \subseteq \text{limsup}(f)$.

(iv) There is a topology, $\mathfrak{E}$, in which a set X is closed if and only if there is some extra-continuous predicate R such that $X = \{A \mid R(A)\}$.

The following are four important results which have fairly complicated proofs using the axiom of choice.

3.25 Theorem
The topology $\mathfrak{E}$ has $\{\{A \mid A \subseteq B\}, \{A \mid A \supseteq B\} \mid B \in P\}$ as a sub-basis for its closed sets. Thus the class of extra continuous predicates is contained in the class of strongly continuous ones. This containment is strict if and only if Σ is uncountable.

(An example of a strongly continuous but not extra continuous predicate: $R(A) = \ulcorner A$ is countable$\urcorner$.)

3.26 Theorem
The topology $\mathfrak{E}$ is compact (i.e. if $\mathfrak{F}$ is a family of closed sets such that each finite subset of $\mathfrak{F}$ has non-empty intersection then $\cap\mathfrak{F}$ is non-empty).

3.27 Theorem
The topology $\mathfrak{E}$ is zero-dimensional (i.e. if X is any closed set and $A \notin X$ then there exists a clopen set Z with the property $A \in Z$ and $X \cap Z = \emptyset$).

3.28 Theorem
a) The clopen sets of $\mathfrak{E}$ are precisely those which can be constructed from sets of the form $\{A \mid w \in A\}$ and $\{A \mid w \notin A\}$ by finite intersections and unions.

b) The predicates R such that both R and $\neg R$ are extra continuous are precisely those which can be defined using the constructs "$w \in A$" ($w \in \Sigma^*$), "$\wedge$" and "$\neg$".

Note that 3.28 extends 3.13 and 3.14 to general alphabets.

The following result is a justification of the use of these extra continuous predicates, since it extends theorem 2.53 to the case of uncountable alphabets, and hence provides an alternative set of conditions justifying the use of 2.1 in an inductive proof. Note that the statement of 3.29 is a translation of the statement of 2.53 into topological terms (as well as being a generalization to arbitrary alphabets).

3.29 Theorem
Suppose that X is a non-empty closed set of $\mathfrak{E}$ and that $f:P \to P$ is a monotonic function with a unique fixed point; then if $f(X) \subseteq X$ we must have $fix(f) \in X$.

proof

The proof is not difficult once we have 3.25 and 3.26. Define $f^{\alpha}(\bot)$ and $f^{\alpha}(\top)$ for arbitrary ordinals α in the same way as we did in 2.53. By 3.25 each of the sets $C_{\alpha} = \{A \mid f^{\alpha}(\bot) \subseteq A \subseteq f^{\alpha}(\top)\}$ is closed. Easy consequences of our definition are that $\beta \in \alpha \Rightarrow C_{\beta} \supseteq C_{\alpha}$ and that $C_{\lambda} = \bigcap_{\beta \in \lambda} C_{\beta}$ if λ is a limit ordinal. Claim that each of the closed sets $X \cap C_{\alpha}$ is non-empty. Proof is by transfinite induction.

When $\alpha = o$ we have $C_o \cap X = X$, which is non-empty by assumption.

If $X \cap C_{\alpha}$ is non-empty, then it contains some element A, say. Then $f(A) \in X$, since $f(X) \subseteq X$, and $f(f^{\alpha}(\bot)) \subseteq f(A) \subseteq f(f^{\alpha}(\top))$ since f is monotonic and $f^{\alpha}(\bot) \subseteq A \subseteq f^{\alpha}(\top)$. Thus $f(A) \in X \cap C_{\alpha+1}$, so $X \cap C_{\alpha+1}$ is non-empty.

If λ is a limit ordinal and each $X \cap C_{\alpha}$ $(\alpha \in \lambda)$ is non-empty then $\langle X \cap C_{\alpha} \mid \alpha \in \lambda \rangle$ is a chain of non-empty closed sets. By compactness this chain has a non-empty intersection. But $\bigcap_{\alpha \in \lambda}(X \cap C_{\alpha}) = X \cap \bigcap_{\alpha \in \lambda} C_{\alpha} = X \cap C_{\lambda}$, so $X \cap C_{\lambda}$ is non-empty as claimed. This completes our inductive proof, so we can deduce that $X \cap C_{\alpha}$ is non-empty for all ordinals α.

Since f has a unique fixed point there must exist some ordinal ξ such that $f^{\xi}(\bot) = f^{\xi}(\top) = \mathrm{fix}(f)$. This tells us that $\mathrm{fix}(f) \in X$, as claimed $(C_{\xi} = \{\mathrm{fix}(f)\})$.

It is usual, in spaces defined by convergent sequences, to define compactness by the property that all sequences have convergent subsequences. This result does not translate verbatim to the space $\mathfrak{E}$ (consider the sequence A_i which we defined in 3.24) but there is a corresponding lemma (which can be used to give an alternative proof of 3.29 very much like the proof of 2.53).

3.30 Lemma

If f is any generalized sequence of points in P then there is a point A which is in cl(f), the smallest closed set containing all the points of f, and such that $\mathrm{liminf}(f) \subseteq A$ and $A \subseteq \mathrm{limsup}(f)$.

Since singleton sets are closed in $\mathfrak{E}$ and any ordinary convergent sequence is also a convergent generalized sequence the proof (in 3.24) that the topology is not first countable is still valid for $\mathfrak{E}$ when Σ is uncountable.

Chapter 4 :- A Model for Non-deterministic Processes

We can model the behaviour of non-deterministic machines by observing not only the traces which it is possible for them to execute, but also the sets of symbols which it is possible for them to reject at each stage. The model we use therefore is a subset of $\mathcal{P}(\Sigma^* \times \mathcal{P}(\Sigma))$, i.e. the relations between traces and subsets of Σ (interpreted as refusal sets). As a relation it is possible to regard any process as a function from traces to sets of refusal sets, the image (as a function) of any trace being the set of its (relational) images. It is necessary to impose certain conditions to ensure that a process is realistic. Formally a non-deterministic machine N is a relation which satisfies the following conditions:

4.1 a) The domain of N ($dom(N) = \{w \mid \exists X.\ (w,X) \in N\}$) is non-empty and prefix closed.

b) $X \in N(w)\ \&\ Y \subseteq X \Rightarrow Y \in N(w)$
(where N(w) is the set of images of w under N)

c) $X \in N(w)\ \&\ Y \cap (N \underline{\text{after}}\ w)^0 = \varnothing \Rightarrow X \cup Y \in N(w)$

d) If $D \subseteq N(w)$ is a directed set then $\bigcup D \in N(w)$.

$N \underline{\text{after}}\ w = \{(v,X) \mid (wv,X) \in N\}$

$N^0 = \{a \in \Sigma \mid \langle a \rangle \in dom(N)\}$

A set of sets is said to be <u>directed</u> if $X,Y \in D \Rightarrow \exists Z \in D.\ Z \supseteq X \cup Y$.

The justifications of these conditions are as follows:

a) If a process has executed any trace it must previously have executed every prefix. It must be possible for a process to do at least nothing ($\langle\rangle$).

b) If a process can refuse every element of a set of symbols then it can refuse every element of a subset.

c) If a process can refuse a set X and it is impossible for it to accept any element of Y then it must be able to refuse the whole of $X \cup Y$.

d) If a process can refuse all approximations to a given set then it can refuse the set itself.

Condition d) is almost always (except in the case of an uncountably infinite alphabet) equivalent to the ascending chain condition:

4.2 d)* If $X_1 \subseteq X_2 \subseteq \ldots \subseteq X_i \subseteq \ldots$ is an ascending chain in N(w) then $\bigcup_{i=1}^{\infty} X_i \in N(w)$,

which is easier to justify intuitively, but breaks down in

the uncountable Σ case.

It is possible to consider different versions of these conditions. We could for example re-phrase the definition in terms of acceptance sets (complements of refusal sets). The resulting model is then clearly isomorphic in a simple way to the original.

More fundamentally we could insist that refusal sets be finite. This involves dropping condition (d) and altering (c) slightly. It is fairly easy to show that the two models are isomorphic (by closing up under condition (d)) and that all our definitions of operators are isomorphic except in one case, which we will meet shortly.

I have included infinite refusal sets in this treatment for several reasons. Firstly if we allow infinite alphabets it seems reasonable that we should be able to test a process by offering it an infinite choice (for example the ability to output any integer). This type of behaviour seems to be modelled more naturally by the inclusion of infinite refusal sets. Secondly they give a more natural model to some recent proof rules of C.A.R.Hoare. Thirdly they pose the soundness problem (where the two models may not be isomorphic) explicitly rather than implicitly. This soundness problem (which we will meet in 4.10 et seq) also places a bound on the validity of the above-mentioned proof-rules.

The definitions of the operators are summarized in an appendix to this chapter. The definitions used are motivated in Hoare, Brookes & Roscoe ( ), which also contains much basic material on the model which omitted here.

4.3 Theorem

a) The space M of non-deterministic machines can be partially ordered by reverse inclusion $A \sqsubseteq B$ if $A \supseteq B$. This order can be interpreted $A \sqsubseteq B$ if B is more deterministic than A. Under this order M is a complete partial order in which the maximal elements are the deterministic machines and the minimal element, CHAOS ($= \Sigma^* \times \wp(\Sigma)$) represents the process which is absolutely unpredictable.

b) $N \in M \Rightarrow (\langle\rangle, \varnothing) \in N$

c) A process is <u>deterministic</u> if

$$w \in \mathrm{dom}(N) \Rightarrow N(w) = \{X \mid X \cap (N \text{ } \underline{\text{after}} \text{ } w)^{o} = \varnothing\}$$

d) The non-deterministic <u>or</u> operator is modelled by union.

All the operators defined in the paper with the exceptions of hiding and $\otimes$(intersection) are easy to prove well-defined (map machines to machines) and continuous (preserve directed limits).

The rest of this chapter will consist of an examination of the problems introduced by these operators. The following chapters will show ways of proving correctness properties of individual processes, by adapting and extending the ideas of chapter 2.

Recall the definition of the hiding operator:

4.4 $$N/X = \{(w\lceil(\Sigma - X), Y) \mid (w, Y \cup X) \in N\}$$
$$\{(wy, X) \mid \{w' \in \mathrm{dom}(N) \mid w'\lceil(\Sigma - X) = w\} \text{ is infinite}\}$$

We cannot hope that this definition will give rise to a continuous operator for infinite X because of the following :

4.5 <u>Example</u>

Let $\Sigma = N \cup \{a\}$ $(a \notin N)$

$A_n =$ <u>stop</u> <u>or</u> $(?m:(\{k \mid k > n\}) \rightarrow a \rightarrow$ <u>stop</u> $)$

Then it is easy to verify that $\forall n.A_n \sqsubseteq A_{n+1}$ and that $\bigsqcup_{n=1}^{\infty} A_n =$ <u>stop</u> .

But then $(A_n)/N$ = CHAOS for each n (infinitely many derivations of $\langle\rangle$) and $(\bigsqcup_{n=1}^{\infty} A_n)/N =$ <u>stop</u> .

Thus $\bigsqcup_{n=1}^{\infty}(A_n/N) \neq (\bigsqcup_{n=1}^{\infty} A_n)/N$

(<u>stop</u> is the process $\{(\langle\rangle, X) \mid X \subseteq \Sigma\}$ which corresponds to <u>abort</u> in this model.)

If we were to alter the second clause of the hiding definition to require arbitrarily long derivations of w, which might seem more natural for infinite X, it would still not make this example continuous. Also it is necessary in this case to make a slight amendment to the operator to make it well-defined with respect to 4.1 (d).

By placing stronger conditions upon the types of process we allow, it is possible to make certain types of infinite hiding continuous. The basic ideas are to divide the alphabet into finitely many portions, and to insist that if an infinite part of one of the portions is available then the whole of it must be. The analysis of this topic is long and complicated, and the results technical. I therefore omit this topic for lack of space, and return to the simpler analysis of finite hiding.

4.6 Theorem

If the set X of hidden symbols is finite, then the hiding operator N/X is well-defined and continuous.

proof

Say that a trace w is a derivation (with respect to X) of v if $w\restriction(\Sigma - X) = v$.

We will prove first that N/X is well-defined.

Throughout this proof A will denote the first (normal) clause of the definition 4.4 of N/X and B will denote the second (infinite chatter) clause.

a) That the domain of N/X is non-empty follows as either $\langle\rangle$ has infinitely many derivations, in which case $(\langle\rangle, \varnothing) \in B$, or it has a maximal one, say w. As w is maximal we must have $(N \underline{\text{after}}\ w)^{o} \cap X = \varnothing$, which implies $(w,X) \in N$ (by clause (c) of N) and thus $(w, X \cup \varnothing) \in N \Rightarrow (\langle\rangle, \varnothing) \in N/X$.

To prove that the domain of N/X is prefix-closed we use a similar argument. Suppose that $v^\frown w \in \mathrm{dom}(N/X)$. Then either some prefix of v has an infinite number of derivations (in which case $(v, \varnothing) \in B$) or v has at least one derivation (for then either w has a derivation, or the minimal prefix of w with infinitely many derivations is greater than v). If v has a derivation the argument is the same as for $\langle\rangle$ above.

b) Suppose $(w,Y) \in N/X$ and $Y' \subseteq Y$

If $(w, \varnothing) \in B$ the result is elementary,

$$(w,Y) \in A \Rightarrow \exists v.\ v\restriction(\Sigma - X) = w \ \&\ (v, X \cup Y) \in N$$
$$\Rightarrow v\restriction(\Sigma - X) = w \ \&\ (v, X \cup Y') \in N$$
$$\Rightarrow (w,Y') \in A$$

c) Suppose $(w,Y) \in N/X$ and $Z \cap (N \underline{\text{after}}\ w)^{o} = \varnothing$

If $(w, \varnothing) \in B$ then $(N \underline{\text{after}}\ w)^{o} = \Sigma$, so the result is trivial.

We may thus suppose that $(w, \varnothing) \notin B$

Hence there is some $v \in \mathrm{dom}(N)$ such that

$v\restriction(\Sigma - X) = w \;\&\; (v, Y \cup X) \in N$

Now $(N \underline{\text{after}}\ v)^{o} \cap (\Sigma - X) \subseteq (N/X \text{ after } w)^{o}$

Thus $(\Sigma - X) \cap Z \cap (N \underline{\text{after}}\ v)^{o} = \varnothing$

$\Rightarrow (v, Y \cup X \cup ((\Sigma - X) \cap Z)) = (v, Y \cup X \cup Z) \in N$

$\Rightarrow (w, Y \cup Z) \in N/X$ as desired.

d) In this section we use the fact that (as will be proved in 4.14) in these circumstances (given that we have already proved (b)) directed set closure is equivalent to closure under the limits of arbitrary (possibly longer than ω) chains.

Suppose therefore that C is a chain contained within $(N/X)(w)$. Again if $(w, \varnothing) \in B$ the result is trivial, so we may suppose not, so $(w, Y_\alpha) \in A$ for each $Y_\alpha \in C$ (assume the chain is indexed by $\alpha < \xi$ (some initial ordinal) and that $\alpha < \beta \Rightarrow Y_\alpha \leqslant Y_\beta$).
Now as $(w, \varnothing) \in A - B$ there must be finitely many $v_i \in \mathrm{dom}(N)$ which are derivations of w $(v_1, \ldots, v_k$, say).
For each $\alpha < \xi$ there must be one of the v_i s.t. $(v_i, Y_\alpha \cup X) \in N$.
We can therefore partition ξ into k sets $\Xi_1, \ldots, \Xi_k$ with the property that $\alpha \in \Xi_i \Rightarrow (v_i, Y_\alpha \cup X) \in N$. It is easy to show that there must be at least one Ξ_i with the property $\alpha < \xi \Rightarrow \exists \beta \in \Xi_i . \alpha \leqslant \beta$.

If we now let $Y'_\alpha = Y_\beta$, where β is minimal in Ξ_i w.r.t. $\beta \geqslant \alpha$ then we have that $C' = \langle Y'_\alpha \cup X \mid \alpha < \xi \rangle$ is a chain contained in $N(v_i)$. Therefore $\bigcup C' = (\bigcup C) \cup X \in N(v_i)$, so $\bigcup C \in (N/X)(w)$ as desired.

To show that N/X is a continuous operator it is necessary to show that if D is a directed set of machines then $(\bigsqcup D)/X = \bigsqcup \{N/X \mid N \in D\}$.
It is easy to show that N/X is a monotonic operator, so we have: $N \in D \Rightarrow N \sqsubseteq \bigsqcup D$

$\Rightarrow (N/X) \sqsubseteq (\bigsqcup D)/X$

$\Rightarrow \bigsqcup \{(N/X) \mid N \in D\} \sqsubseteq (\bigsqcup D)/X$

It therefore only remains to show the reverse inclusion.
Because of the reverse nature of the order used, this means showing $(w, Y) \in \bigsqcup \{N/X \mid N \in D\} \Rightarrow (w, Y) \in (\bigsqcup D)/X$.

There are two cases to consider:

a) $\forall N \in D.\ (w, \varnothing) \in B_N$, where B_N is the second clause in the definition of N/X.

b) $\exists N \in D.\ (w, \varnothing) \notin B_N$

In the first case it is clearly sufficient to prove that some prefix of w has infinitely many derivations, for then $(w,X) \in B$ for all $X \subseteq \Sigma$ (where B is the second clause in the definition of $(\bigsqcup D)/X$). There is some prefix v of w which is minimal with respect to there being an infinite derivation set for it in each $N \in D$.

There is therefore some $N_v \in D$ s.t. no proper prefix of v has an infinite derivation set in N_v. Let $D^* = \{N \in D \mid N \sqsupseteq N_v\}$. It is easy to show that $\bigsqcup D^* = \bigsqcup D$ and hence that $(\bigsqcup D^*)/X = (\bigsqcup D)/X$. It is therefore sufficient to show that some prefix of w (namely v) has an infinite derivation in $\bigsqcup D^*$.

As $N \sqsupseteq N_v \not\Rightarrow N \subseteq N_v$ there must be finitely many derivations of every proper prefix of v for every $N \in D^*$.

Claim that the number of <u>k-minimal</u> derivations of v is finite for each $N \in D^*$ and $k \in \mathbb{N}$ (natural numbers), where a k-minimal derivation of v is one which has precisely k proper prefixes which are derivations of v.

(Thus if $X = \{a\}$ we have -

$\langle aab \rangle, \langle ab \rangle, \langle b \rangle$ are all o-minimal derivations of $\langle b \rangle$,

$\langle aba, \langle ba \rangle, \langle aaba \rangle$ are all 1-minimal,

$\langle abaa \rangle, \langle baa \rangle$ are 2-minimal, etc.)

Firstly the number of o-minimal derivations is finite. This is certainly true if $v = \langle\rangle$, for then the only one is $\langle\rangle$. If $v = v'\langle a \rangle$ the number must be finite since each o-minimal s must have the form $s'\langle a \rangle$ for some s' which is a derivation of v'. But v' is known only to have finitely many derivations in $N \sqsupseteq N_v$, which gives us the desired result.

If we suppose the number of k-minimal derivations is finite, then since each k+1-minimal derivation has the form $s\langle b \rangle$, where s is k-minimal and $b \in X$ (and X is finite) the number of k+1-minimal derivations must also be finite.

Hence by induction the number of k-minimal derivations is finite for each k. Also, since v has infinitely many derivations each of which is k-minimal for some k, there must be k-minimal derivations present for each k in every $N \in D^*$.

Claim that there is a k-minimal derivation of v present in $\bigcup D^*$ for each k. Suppose not (for some k) and that $s_1 \ldots s_r$ are the k-minimal derivations present in N_v. If (for any i) $(s_i, \emptyset) \in N'$ for each $N' \in D^*$ then we would have $(s_i, \emptyset) \in \bigcup D^*$, contradicting our assumption. Thus, for each i, there must be some $N_i \in D^*$ s.t. $(s_i, \emptyset) \in N_i$. But then (as D^* is directed) there is some $N^* \in D^*$ s.t. $N^* \sqsupseteq N_i$ for each i. Therefore $\forall i . s_i \notin \mathrm{dom}(N^*)$, but as also $\mathrm{dom}(N^*) \subseteq \mathrm{dom}(N_v)$ there can be no k-minimal derivations of v in N^*. This contradicts the remark on the previous page. Thus the claim that there is some k-minimal derivation of v in $\bigcup D^*$ is proven.

But now since every n-minimal derivation of v is clearly distinct from every m-minimal one (if $n \neq m$) there must be an infinity of derivations of v in $\bigcup D^*$, which was what we wanted to prove.

This completes the proof of case (a).

Case (b) is rather easier.
If $\exists N_w$ D. $(w, \emptyset) \notin B_{N_w}$ set $D^* = \{N \mid N \sqsupseteq N_w\}$, then as before D^* is itself directed and $\bigcup D^* = \bigcup D$. Since $N \in D^* \Rightarrow N \subseteq N_w$ we must have $N \in D^* \Rightarrow (w, \emptyset) \notin B_N$.
Thus the number of derivations of w in each $N \in D^*$ is finite, and clearly the derivations in each $N \in D^*$ are included in those in N_w (as $N \subseteq N_w$).
We must have $(w, Y) \in A_N$ for each $N \in D^*$.
For each $N \in D^*$ there is thus a non-empty set S_N of the traces in dom(N) s.t. $s \in S_N \Leftrightarrow s\lceil(\Sigma - X) = w$ and $(s, Y \cup X) \in N$.
By construction each of these S_N is finite and included in S_{N_w}.
Claim that $\exists s \in S_{N_w} . (s, X \cup Y) \in (\bigcup D^*)$.
If not then for each $s \in S_{N_w}$ we can find a $N_s \in D^*$ s.t. $s \notin S_{N_s}$.
But then as D^* is directed we can find some $N^* \sqsupseteq N_s$ for every s.
But then we would have $S_{N_w} \cap S_{N^*} = \emptyset$, which contradicts the structure of the S_N. Thus $\exists s \in S_{N_w} . (s, X \cup Y) \in (\bigcup D^*)$ as claimed.
But this is the desired result, since then $(w, Y) \in (\bigcup D^*)/X$.

By similar methods one can prove (for finite X & Y)

4.7 $(N/X)/Y = N/(X \cup Y)$.

The following commutativity law is an immediate corollary to 4.7 .

4.8 $(N/X)/Y = (N/Y)/X$

There will be further analysis of the hiding operator in chapters 5 & 6, where we will examine the pipe operator "$\gg$" and the Master/Slave operator $(A \| a::B)$ in some depth (both of which use hiding in their definitions).

We now turn our attention to the intersection operator "$\otimes$". This operator is used critically in the definition of the parallel combinator $(A_X \|_Y B)$. Recall its definition:

4.9 $A \otimes B = \{(w, X \cup Y) \mid (w,X) \in A \ \& \ (w,Y) \in B\}$

The interpretation of this is that $A \otimes B$ will only execute traces possible for both A & B and at any stage it can refuse any set which A and B can co-operate in refusing.

It is this last feature (the refusal sets) which cause us the problems. It is easy to show that the domain of $A \otimes B$ is non-empty and prefix closed, that $A \otimes B(w)$ satisfies left-closure (4.1 (b)) and condition 4.1(c). It seems, however, to be far from easy to prove anything about 4.1(d).

The root of this difficulty lies in the fact that if $\{X \cup Y \mid X \in K_1 \ \& \ Y \in K_2\}$ is a directed set there is no reason why K_1 or K_2 should be directed, so it is difficult to prove the existence of elements on the two sides which combine to give the limit of the directed set. The problem can be stated thus:

4.10 If F_1 and F_2 are two families of subsets of Σ which satisfy:

a) <u>left-closure</u> $X \in F \ \& \ Y \subset X \Rightarrow Y \in F$

b) <u>directed closure</u> $D \subseteq F$ directed $\Rightarrow \bigcup D \in F$

does the family $\{X \cup Y \mid X \in F_1 \wedge Y \in F_2\}$ satisfy these conditions?

The conditions (a) & (b) here are the same as 4.1 (b) & (d) respectively.

This problem does not exist for finite alphabets, for then every directed set contains its limit, so we need to examine

only the various possible cardinalities of infinite alphabets.

We will adopt the following approach in analysing the problem. Firstly we will see that the answer to 4.10 is affirmative if Σ is countable, which means that in this case $\otimes$ is both well-defined and continuous. Secondly we will see an example to show that if we substitute the countable chain condition 4.2 for directed closure the answer to 4.10 (for uncountable alphabets) is negative. Finally we will see how to prove the well-definedness of $\otimes$ for arbitrary alphabets and that it is a non-trivial set-theoretic tool.

4.11 Theorem

If Σ is countably infinite then the answer to 4.10 is yes.

proof

This result can be proved using directed sets explicitly, using a version of Konig's lemma independent of the Axiom of Choice. We here however prove a version involving chains, since this ties in better with what is to follow.

4.11.1 lemma

If Σ is countable then we can substitute the chain condition

$\langle X_i \mid i \in N \rangle$ a sequence in F s.t. $X_i \subseteq X_{i+1} \Rightarrow \bigcup_{i=1} X_i \in F$

for directed closure in 4.10 and the effect of the new pair of conditions is equivalent to that of the old pair.

proof

That the above condition is weaker than directed closure is obvious since every ascending chain is a directed set.

It is therefore sufficient to show that if D is a directed set in a family F which is left-closed and ascending chain closed then $\bigcup D \in F$.

Suppose X is any finite subset of $\bigcup D$. Then it is easy to show by techniques akin to some used in the proof of 4.6 that there is some $Y \in D$ s.t. $X \subseteq Y$. Thus $X \in F$ (by left-closure), so every finite subset of $\bigcup D$ is in F.

As Σ is countable we can enumerate the elements of $\bigcup D$ as $\{a_1, a_2, \ldots, a_i, \ldots\}$ (if $\bigcup D$ is finite then $\bigcup D \in F$ by the above, so the result is trivial).

But then if $X_i = \{a_j \mid j < i\}$ we have that $\langle X_i \rangle$ is an ascending sequence in F (finite subsets of $\bigcup D$) and so $\bigcup_{i=1} X_i = \bigcup D \in F$.

It is thus sufficient to prove that if F_1 and F_2 are two left-closed and ascending chain closed families then so is

$$\{X \cup Y \mid X \in F_1 \ \& \ Y \in F_2\} \ .$$

Suppose that these conditions hold of F_1 and F_2 and that

$$X_1 \cup Y_1, \ X_2 \cup Y_2, \ \ldots, \ X_i \cup Y_i, \ \ldots$$

is an ascending chain with limit Z, say and where $X_i \in F_1$, $Y_i \in F_2$.

If Z is finite then the sequence $X_i \cup Y_i$ is ultimately constant (and equal to Z). In that case the desired result, namely the existence of some $X \in F_1$ and $Y \in F_2$ s.t. $X \cup Y = Z$, is trivial. We may therefore assume that Z is infinite and is enumerated as $\{a_1, \ldots, a_i, \ldots\}$.

Claim that for each $j \in N$ we can find an infinite sequence of natural numbers $\langle n_{j,i} \mid i \in N \rangle$ with the following properties:

a) $i < i' \Rightarrow n_{j,i} < n_{j,i'}$

b) $\langle n_{j+1,i} \rangle_i$ is a subsequence of $\langle n_{j,i} \rangle_i$.

c) If $A_j = \{a_k \mid k < j\}$ then $\forall i . A_j \cap X_{n_{j,i}} = A_j \cap X_{n_{j,1}}$, $\forall i . A_j \cap Y_{n_{j,i}} = A_j \cap Y_{n_{j,1}}$ and $\forall i . A_j \subseteq X_{n_{j,i}} \cup Y_{n_{j,i}}$.

(Note that this is very similar to the construction used in the proof of 2.52.)

We can find such a sequence for j=1 since $A_1 = \emptyset$ so we can put $n_{j,i} = i$.

Suppose that we have constructed such a sequence for j. By construction (since $n_{j,i+1} > n_{j,i}$) the sequence $\langle X_{n_{j,i}} \cup Y_{n_{j,i}} \mid i \in N \rangle$ is ascending with limit Z. Thus $a_j \in \bigcup_{i=1} (X_{n_{j,i}} \cup Y_{n_{j,i}})$, so there is some k such that $i \geq k \Rightarrow a_j \in (X_{n_{j,i}} \cup Y_{n_{j,i}})$.

It is easy to see that <u>either</u> there is an infinite subset of $\{i \mid i \geq k\}$ such that $a_j \in X_{n_{j,i}} \cap Y_{n_{j,i}}$ for each i, <u>or</u> there is an infinite subset such that $a_j \in X_{n_{j,i}} - Y_{n_{j,i}}$ for each i, <u>or</u> there is an infinite subset such that $a_j \in Y_{n_{j,i}} - X_{n_{j,i}}$ for each i. We now define $n_{j+1,i}$ to be the ith $n_{j,s}$ such that s lies in the first of these infinite sets to exist (that is, if $a_j \in X_{n_{j,i}} \cap Y_{n_{j,i}}$ set exists, choose it, etc.).

It is now easy to show that the new sequence $n_{j+1,i}$ satisfies all that is required of it.

Now choose $m_i = n_{i,i}$. By conditions (a) & (b) above we have that $m_i < m_{i+1}$ for each i.

Now let $W_i = X_{m_i} \cap A_i$ and $V_i = Y_{m_i} \cap A_i$. The following must hold of these W_i an V_i.

a) $W_i \in F_1$ & $V_i \in F_2$ (by left-closure)

b) $W_i \cup V_i = A_i$

c) $W_i \subseteq W_{i+1}$ & $V_i \subseteq V_{i+1}$ (as every $n_{i+1,j}$ is a $n_{i,j}$)

But since F_1 and F_2 are ascending chain closed they must contain $\bigcup_{i=1}^{\infty} W_i$ and $\bigcup_{i=1}^{\infty} V_i$ respectively, and

$$(\bigcup_{i=1}^{\infty} W_i) \cup (\bigcup_{i=1}^{\infty} V_i) = \bigcup_{i=1}^{\infty}(W_i \cup V_i) = \bigcup_{i=1}^{\infty} A_i = Z \quad .$$

Hence Z lies in $\{X \cup Y \mid X \in F_1 \ \& \ Y \in F_2\}$ as desired.

4.12 Theorem

The ascending chain condition 4.2 is insufficient to make $\otimes$ well defined if Σ is uncountable.

proof

First observe that for an uncountable alphabet 4.2 is a strictly weaker condition than directed closure.
An example to show this is the countable subsets of the real numbers. This family is closed under 4.2 (and is left closed) but is not directed closed since the family itself is directed but does not contain its union.

Our aim will be to show there exists an uncountable alphabet which is somehow isomorphic to the set of proofs of membership of families which are left closed and satisfy 4.2.

4.12.1 If $\langle X_i \rangle$ is any sequence of sets define

$$\text{liminf}(X_i) = \bigcup_{j=1}^{\infty}(\bigcap_{i=j}^{\infty}(X_i))$$

(Note the similarity between this and 2.42.)

Claim that if $\langle X_i \rangle$ is any sequence of sets in a chain-closed family (for the rest of this section we will use the term chain closed to mean left closed and satisfying 4.2) then $\text{liminf}(X_i)$ is also contained in the family.

Let $Y_i = \bigcap_{j=i}^{\infty}(X_j)$.

Clearly each Y_i is contained in the family (F say) by left closure (it is greater than X_i).

Also the Y_i are an increasing sequence (being intersections of decreasing sets).

Therefore $\text{liminf}(X_i) = \bigcup_{i=1}^{\infty} Y_i \in F$ as desired.

4.12.2 lemma

If G is any family of sets which is closed under the taking of liminfs then the family $\{X \mid \exists Y \in G.Y \supseteq X\}$ is chain closed.

proof

Let $F = \{X \mid \exists Y \in G.Y \supseteq X\}$.

That F is left closed is trivial since $X \in F \Rightarrow \exists Y \in G.X \subseteq Y$ so $X' \subset X \Rightarrow X' \subset Y$. Thus $X' \in F$ as desired.

Suppose that $\langle X_i \rangle$ is any ascending chain contained in F. Then for each X_i we can choose a $Y_i \in G$ such that $X_i \subseteq Y_i$. But then

$$\begin{aligned} j > i &\Rightarrow X_i \subseteq X_j \subseteq Y_j \\ &\Rightarrow X_i \subseteq \bigcap_{j=1}^{\infty} Y_j \\ &\Rightarrow \bigcup_{i=1}^{\infty} X_i \subseteq \bigcup_{i=1}^{\infty}\left(\bigcap_{j=1}^{\infty} Y_j\right) = \operatorname{liminf}(Y_j) \in G \end{aligned}$$

Hence $\bigcup_{i=1}^{\infty} X_i \in F$ as desired.

This result (in a way which will become clear shortly) helps us to bound the number of elements we must include in any chain closed family, given that we wish it to contain an arbitrary collection of sets.

4.12.3 Define a finite path ω-branching tree $t \in T_N$ as follows:

a) t is a directed tree with a single base node.

b) Every non-leaf node of t is unlabelled and has edges labelled 1,2,3,... leading out of it to subtrees $t_1, t_2, \ldots \in T_N$ which are all distinct.

c) Every leaf node of t is labelled by some $n \in N$.

d) t contains no infinite path.

4.12.4 lemma

a) The relation $t_1 < t_2$ if t_1 is a strict subtree* of t_2 is a partial order on T_N.

b) It is a well-founded partial order, and thus every subset of T_N contains its minimal elements and induction and recursion are both possible.

proof

a) If $t_1 < t_2$ and $t_2 < t_3$ then trivially $t_1 < t_2$. If $t_1 > t_2 > t_3 > \ldots > t_i > \ldots$ were an infinite descending

(* - all descendants of some non-base node of t_2)

chain in T_N then t_1 would contain an infinite path (through the successive base nodes of the t_i) contradicting its membership of T_N. Hence there are no such chains in T_N, so in particular for no element of T_N can we have $t > t$ for this would give rise to the descending chain $t > t > t > \ldots\ldots$. This completes the proof that T_N is partially ordered by $<$.

b) Suppose S is any non-empty subset of T_N which does not contain any elements which are minimal with respect to it. Then for every element t of S there is some $s \in S$ such that $s < t$. It is then easy to show (given AC) that there is an infinite descending chain (starting from any element) contradicting the above.

Hence every subset S of T_N contains some element t such that $t \in S \Rightarrow \neg(s < t)$.

It is then easy to prove the inductive principle:

$(\forall t \in T_N.(\forall s < t.R(s)) \Rightarrow R(t)) \Rightarrow (\forall t \in T_N.R(t))$

for any property R.

Also it is easy to show that if H is any function

$H: \{(t,g) \mid t \in T_N \ \& \ g:\{s \mid s < t\} \to A\} \to A$ (for any set A)

then there is a unique total function $f:T_N \to A$ which satisfies $f(t) = H(t, f\restriction\{s \mid s < t\})$ for all $t \in T_N$.

Define $t \in T_N$ to be a <u>singleton</u> if it has only a single node (we will denote t by $\langle n \rangle$, where the single (leaf) node is labelled "n").

We will sometimes denote <u>infinite</u> elements of T_N by the elements of T_N at the ends of their lowest level edges, thus $\langle t_i \mid i \in N \rangle$ is the tree with t_i at the end of edge i leading out of the base node.

Define functions $f:T_N \times T_N \to \wp(N)$ and $g:T_N \times T_N \to \wp(N)$ as follows:

If t & s are both singletons then $f(s,t) = g(s,t) = \emptyset$.

If t is a singleton $\langle n \rangle$ and s is infinite then $f(t,s) = \{n\}$ and $g(t,s) = \{m \mid m$ labels some leaf of s and $n \neq m\}$.

If s is a singleton $\langle n \rangle$ and t is infinite then $g(t,s) = \{n\}$ and $f(t,s) = \{m \mid m$ labels some leaf of t and $n \neq m\}$.

If both t & s are infinite then each contains a finite or countable number of non-leaf nodes with infinitely many leaves attached. (This is easy to prove using the induction principle outlined on the last page.)

Suppose that these nodes of t are $n_1, n_2, \ldots, n_k, \ldots$
and that these nodes of s are $m_1, m_2, \ldots, m_k, \ldots$

and that the leaf nodes of n_i form the sequence $\langle n_{i,j} \rangle (j \geq 0)$
and that the leaf nodes of m_i form the sequence $\langle m_{i,j} \rangle$.

Define $H_o = L_o = \emptyset$, and define two cyclical functions:

Let $p(r) = r \pmod{n}$ if there is a finite number n of n_js
$= r -$ (the greatest triangular number $\leq r$)
if there are infinitely many n_js

Let $q(r) = r \pmod{m}$ if there are m m_js
$= r -$ (the greatest triangular number $\leq r$)
if there are infinitely many m_js

Now let l_r = least element of $\{n_{p(r),j} \mid j \in N\} - (H_{r-1} \cup L_{r-1})$
and h_r = least element of $\{m_{q(r),j} \mid j \in N\} - (H_{r-1} \cup L_{r-1} \cup \{l_r\})$
and $H_r = H_{r-1} \cup \{h_r\}$ & $L_r = L_{r-1} \cup \{l_r\}$ $(r \geq 1$ in each case).

This is a well-defined recursion since each H_r and L_r is finite, and the sets $\{n_{i,j} \mid j \in N\}$ and $\{m_{i,j} \mid j \in N\}$ are infinite for every i in the correct ranges as all the leaves on the n_i and m_i are by assumption different.

Note that since by construction all the l_i are distinct from all l_j $(i \neq j)$ and from all h_j the two sets $\{l_i \mid i \in N\}$ and $\{h_i \mid i \in N\}$ are disjoint.

Now set $f(t,s) = \{l_j \mid j \in N\}$
and $g(t,s) = \{h_j \mid j \in N\}$.

This completes the definition of f & g.
Note that in the last case, since the functions p & q each take every node index as their value infinitely many times, there are infinitely many $n_{i,j}$ in $f(t,s)$ for each i and infinitely many $m_{i,j}$ in $g(t,s)$ for each i.

By construction also $f(t,s) \cap g(t,s) = \emptyset$ for all $t,s \in T_N$.

Now define $X^*_n = \{(t,s) \mid n \notin f(t,s)\}$
$Y^*_n = \{(t,s) \mid n \notin g(t,s)\}$
For each n we have $X^*_n \cup Y^*_n = T_N \times T_N$, since $(t,s) \in T_N \times T_N$ implies $f(t,s) \cap g(t,s) = \emptyset$ so either $n \notin f(t,s)$ or $n \notin g(t,s)$.

Now define $X_n = X^*_n \cup \{0,1,\ldots,n\}$
$Y_n = Y^*_n \cup \{0,1,\ldots,n\}$

Thus $X_n \cup Y_n = T_N \times T_N \cup \{0,1,2,\ldots,n\}$ and so the $X_n \cup Y_n$ form an ascending chain with limit $T_N \times T_N \cup N$ $(= \Sigma$, say).

Define functions $h,k: T_N \to \wp(\Sigma)$ by recursion.
$h(\langle n \rangle) = Y_n$ $\quad k(\langle n \rangle) = X_n$
$h(\langle t_i \mid i \in N \rangle) = \text{liminf}(h(t_i))$
$k(\langle t_i \mid i \in N \rangle) = \text{liminf}(k(t_i))$
By 4.12.4 this recursion is well-defined.

Consider now the families F_1 and F_2 defined:
$F_1 = \{X \mid \exists t \in T_N . X \subseteq k(t)\}$
$F_2 = \{X \mid \exists t \in T_N . X \subseteq h(t)\}$
These families are both chain closed by a similar argument to 4.12.2 (a little care is required to show that we can get away with our demand that all the first level subtrees of any tree are distinct).

Claim that the limit (Σ) of the above ascending chain cannot be expressed as $X \cup Y$, where $X \in F_1$ and $Y \in F_2$.
It is clearly sufficient to show that Σ cannot be expressed as $k(t) \cup h(s)$ for any $(t,s) \in T_N \times T_N$.
If t & s are both singletons, labelled n & m respectively then $\max(n,m)+1 \notin k(t) \cup h(s)$.

Otherwise claim that $(t,s) \notin k(t) \cup h(s)$.
We will show here that $(t,s) \notin k(t)$, the proof that $(t,s) \notin h(s)$ being practically identical.

If t is a singleton labelled n then $n \in f(t,s)$, and thus $(t,s) \notin X^*_n$. Hence $(t,s) \notin X_n = k(\langle n \rangle)$, as required.

If t is infinite and s is a singleton $\langle n \rangle$ then work by induction on the structure of t.
Claim that every infinite $t' < t$ satisfies $(t,s) \notin k(t')$.

Assume that all infinite t_i in $\langle t_i \mid i \in N \rangle \leqslant t$ satisfy this.
Either $\langle t_i \mid i \in N \rangle$ has infinitely many of the t_i infinite or it does not.
In the first case, by induction, there are infinitely many i such that $(t,s) \notin k(t_i)$. But then $(t,s) \notin \text{liminf}(k(t_i))$. Thus $(t,s) \notin k(\langle t_i \mid i \in N \rangle)$ as desired.
In the second case there must be infinitely many leaf nodes amongst the t_i, only one of which (at most) can be labelled n. For each $\langle m \rangle$ s.t. $m \neq n$ we have

$m \in f(t,s)$ (as $m (\neq n)$ labels a leaf node of t)

$\Rightarrow (t,s) \notin k(\langle m \rangle)$.

Thus again $(t,s) \notin k(t_i)$ for infinitely many i, so that $(t,s) \notin \text{liminf}(k(t_i)) = k(\langle t_i \mid i \in N \rangle)$ as required.

Finally we have the case that both t and s are infinite.
Again we prove by induction on the infinite $t' \leqslant t$ that $(t,s) \notin k(t')$.
Assume that all infinite t_i in $\langle t_i \mid i \in N \rangle \leqslant t$ satisfy this.
If there are infinitely many infinite t_i then $(t,s) \notin k(\langle t_i \rangle_i)$ by the same argument as above. If there are not then infinitely many of the t_i must be leaf nodes. Thus in the definition of f(t,s) and g(t,s) the base node of $\langle t_i \mid i \in N \rangle$ must be one of the n_i. Hence infinitely many of the labels of the t_i are included in f(t,s). Thus, as above, there are infinitely many t_i s.t. $(t,s) \notin k(t_i)$ and so $(t,s) \notin \text{liminf}(k(t_i)) = k(\langle t_i \mid i \in N \rangle)$ as required.
This completes the induction, and so the property holds of t itself.

This completes the proof that if t & s are not both singletons then $(t,s) \notin h(s) \cup k(t)$.

Hence in any case $(s,t) \in T_N \times T_N \Rightarrow k(t) \cup h(s) \neq \Sigma$, which is known to be the limit of an ascending chain in $\{ X \cup Y \mid X \in F_1 \ \& \ Y \in F_2 \}$, and so this family is not chain closed.

To complete the proof of 4.12 all we now have to do is set $N_1 = \{(\langle\rangle, X) \mid X \in F_1\} \cup \{(\langle a \rangle, X) \mid a \in \Sigma, X \subseteq \Sigma\}$
$N_2 = \{(\langle\rangle, X) \mid X \in F_2\} \cup \{(\langle a \rangle, X) \mid a \in \Sigma, X \subseteq \Sigma\}$
and observe that both N_1 and N_2 satisfy 4.1 (a)-(c) and 4.2 but $N_1 \otimes N_2$ does not.

It is possible to extend the notion of ascending chain (and so also the ascending chain condition 4.2) to include chains indexed by larger ordinals than the usual ω.

If η is any ordinal define a η-chain to be a function $\theta: \eta \to \wp(\Sigma)$ which satisfies $\xi \in \pi \Rightarrow \theta(\xi) \subseteq \theta(\pi)$.
We will often use the notation $\langle c_\rho | \rho \in \eta \rangle$ for the η-chain with ρ-component c_ρ.

Clearly the only η-chains to be of interest from the point of view of taking unions are those indexed by limit ordinals (as other ones contain their unions as last members).

We can now extend 4.2 either to insist that a family be closed under the unions of arbitrary length chains or under the unions of all chains of length smaller than some λ.

The following is a technical result in classifying these conditions.

4.13 Lemma

Suppose that Σ is an infinite alphabet with cardinal $|\lambda|$, where λ is an initial ordinal. Then if $C = \langle c_\kappa | \kappa \in \eta \rangle$ is any chain over this Σ there is some subchain $D = \langle d_\kappa | \kappa \in \tau \rangle$ of C such that $\tau \leq \lambda$ is a regular initial ordinal and $\bigcup C = \bigcup D$.

The proof is not difficult but is omitted.

It is fairly easy to see how the methods of 4.12 could be extended to show that no ascending chain condition which expressed a bound on the length of chain could work for general alphabets (in the sense of making the definition of $\otimes$ valid). 4.13 also shows that (using AC) for any fixed alphabet there is maximum length of chain which need be considered.

The next result shows that the arbitrary ascending chain condition is in fact equivalent to directed set closure.

4.14 Lemma

Suppose that Σ is an alphabet of cardinality $|\lambda|$, where λ is an infinite initial ordinal. Suppose further that F is a family of subsets of Σ which is left-closed. Then the following two conditions are equivalent.

(i) F is directed closed.

(ii) F is closed under the limits of η-chains for every regular initial ordinal $\eta \leq \lambda$.

proof

That (i) $\Rightarrow$ (ii) is obvious since every η-chain is a directed set in its own right. In proving the converse note that by 4.13 the second condition is equivalent to closure under the unions of arbitrary length chains.

Suppose then that (ii) holds of F and that $D \subseteq F$ is a directed set. Claim that for each $D' \subseteq D$ (D' not necessarily directed) we have $\bigcup D' \in F$.

Prove this by transfinite induction on $|D'|$ (actually T.I. on the initial ordinal equinumerous with D', so we are using AC here).

If D' is finite then there must be some element of D which contains $\bigcup D'$ since D is directed. Thus $\bigcup D' \in F$ by left-closure.

Suppose then that D' is infinite and that the result holds of all sets with smaller cardinality. Enumerate D' by its initial ordinal (so that $D' = \{X_\kappa | \kappa \in \theta\}$). For each $\alpha \in \theta$ set $D'_\alpha = \{X_\kappa | \kappa \in \alpha\}$. By construction each D'_α has strictly smaller cardinal than D' and so $\bigcup D'_\alpha \in F$ by assumption.

The $\bigcup D'_\alpha$ are an ascending θ-chain (as the D'_α are an ascending sequence of sets) so by 4.13 $\bigcup_{\alpha \in \theta} (\bigcup D'_\alpha) = \bigcup D' \in F$.

Hence by induction $\bigcup D' \in F$ for every $D' \subseteq D$, and in particular $\bigcup D \in F$ as desired, completing the proof of 4.14.

The methods used in proving can be extended to show, using the above, that 4.10 holds for certain uncountable alphabets. These methods become quite involved, and seem to break down at the cardinal $\aleph_\omega$ (which may or may not be less than the cardinal of the real numbers, dependant on the continuum hypothesis).

In order to complete the proof of the truth of 4.10 for general alphabets we appeal to the compactness theorem of propositional calculus. We will in fact see that not only is this implied by propositional compactness but that also compactness is directly provable from 4.10 without recourse to any other powerful set-theoretic tools such as Zorn's lemma (the normal result used to prove compactness).

4.15 Theorem

The truth of 4.10 is both implied by and implies the compactness theorem for propositional calculi with arbitrarily large collections of propositional variables.

proof

Recall the compactness theorem:

If L is a propositional language which consists of the finite formulae formed from a set of propositional variables and the standard connectives then any subset of L which finitely consistent is consistent. A set $K \subseteq L$ is consistent if there is some truth assignment which satisfies every element of K and is finitely consistent if each finite $K' \subseteq K$ is consistent.

We show first that the truth of 4.10 is implied by the above. Suppose that Σ is any alphabet and that F_1 and F_2 are two families of subsets of Σ which satisfy the conditions of 4.10. Let L be the language which contains distinct propositional variables p_α and q_α for each $\alpha \in \Sigma$ and the finite combinations of these by "$\neg$","$\vee$"&"$\wedge$".

Suppose that D is a directed subset of $\{ X \cup Y \mid X \in F_1 \ \& \ Y \in F_2 \}$. Define sets of formulae K_1, K_2 & K_3 as follows:

$$K_1 = \{ p_\alpha \vee q_\alpha \mid \alpha \in \cup D \}$$
$$K_2 = \{ \neg(p_\alpha \wedge p_\beta \wedge \ldots \wedge p_\eta) \mid \{\alpha, \overset{(\text{finite})}{\beta}, \ldots, \eta\} \notin F_1 \}$$
$$K_3 = \{ \neg(q_\alpha \wedge q_\beta \wedge \ldots \wedge q_\eta) \mid \{\alpha, \overset{(\text{finite})}{\beta}, \ldots, \eta\} \notin F_2 \}$$

Claim that $K = K_1 \cup K_2 \cup K_3$ is finitely consistent.

Suppose that $K' \subseteq K$ is finite. Then $K' \cap K_1$ is finite and so is $U = \{ \alpha \mid p_\alpha \vee q_\alpha \in K' \}$. For each $\alpha \in U$ there is some $X \in D$ such that $\alpha \in X$ and so, as D is directed, there is some $X \in D$ such that $U \subseteq X$. This X can be written $Y \cup Z$ for some $Y \in F_1$ and $Z \in F_2$ (by assumption). Define a truth assignment s as follows:

$s(p_\alpha)$ = <u>true</u> if $\alpha \in Y$

$s(p_\alpha)$ = <u>false</u> otherwise

$s(q_\alpha)$ = <u>true</u> if $\alpha \in Z$

$s(q_\alpha)$ = <u>false</u> otherwise .

By construction $s(\varphi)$ = <u>true</u> for each $\varphi \in K' \cap K_1$.

If $\varphi \in K_2$ then φ can be written $\neg(\bigwedge_{\alpha \in W} p_\alpha)$ for some finite $W \notin F_1$. Certainly $W \not\subseteq Y$ (as $Y \in F_1$) so that $W - Y \neq \emptyset$. Hence $s(\varphi)$ = <u>true</u>.

Similarly $\psi \in K_3 \Rightarrow s(\psi)$ = <u>true</u>.

Thus $s(\psi)$ = <u>true</u> for each $\psi \in K' \cap K_1$ or $K' \cap K_2$ or $K' \cap K_3$ and so the whole of K' is satisfied by s.

This completes the proof that K is finitely consistent.

By the assumption of the compactness theorem, therefore, there is some truth assignment s* which simultaneously satisfies the whole of K. Define $Y = \{\alpha \in UD \mid s^*(p_\alpha)\}$ and $Z = \{\alpha \in UD \mid s^*(q_\alpha)\}$.

Clearly $UD = Y \cup Z$ as $\alpha \in UD \Rightarrow s^*(p_\alpha \vee q_\alpha) = \underline{\text{true}}$

$\Rightarrow s^*(p_\alpha) = \underline{\text{true}} \vee s^*(q_\alpha) = \underline{\text{true}}$

$\Rightarrow \alpha \in Y \vee \alpha \in Z$

Also $Y \in F_1$ as the set $\{Y' \mid Y' \subseteq Y \ \& \ Y' \text{ finite}\}$ is directed with limit Y and is contained in F_1 as

$(Y' \subseteq Y) \ \& \ Y'$ finite $\Rightarrow s^*(\varphi) = \underline{\text{true}}$, where $\varphi = \bigwedge_{\alpha \in Y'} p_\alpha$

$\Rightarrow s^*(\psi) = \underline{\text{false}}$, where $\psi = \neg(\bigwedge_{\alpha \in Y'} p_\alpha)$

$\Rightarrow \psi \notin K_2$

$\Rightarrow Y' \in F_1$.

Similarly $Z \in F_2$ which completes the proof of our result.

Secondly we show that the truth of 4.10 can be used to prove the compactness theorem. Suppose that L is a propositional language of finite formulae with variables V. Suppose further that $K \subseteq L$ is finitely consistent. Define two families F_1 and F_2 as follows:

$F_1 = \{X \subseteq L \mid X \cup K \text{ is finitely consistent}\}$

$F_2 = \{X \subseteq L \mid X \text{ is finitely frustratable}\}$

where $X \subseteq L$ is finitely frustratable (f.f.) if for every finite $X' \subseteq X$ there is a truth assignment which maps each $\psi \in X'$ to $\underline{\text{false}}$.

Each of these families satisfies the conditions of 4.10: left-closure is trivial and directed set closure follows from the fact that every finite subset of the union of a directed set is contained in some element of the set.

Claim that the whole of L can be expressed as $Y \cup Z$ for some $Y \in F_1$ and $Z \in F_2$. By the assumption of the truth of 4.10 it will be sufficient to show that each finite subset of L can be so expressed (as these finite sets are a directed set with union L).

Claim that each finite subset of L is a subset of some set of the form $Y \cup Z$, such that $Y \in F_1$, $Z \in F_2$ and $Z \subseteq \{\psi \mid \neg\psi \in Y\}$.

Proof is by induction on the size of the subset.
The result is trivial for the empty set $\emptyset$.
Suppose that it holds of all smaller sets than $X = X^* \cup \{\psi\}$ ($\psi \notin X^*$). By assumption there are $Y^* \in F_1$ and $Z^* \in F_2$ which satisfy our requirements for X^*.
Either $K \cup Y^* \cup \{\psi\}$ is finitely consistent or $K \cup Y^* \cup \{\psi\}$ is. This is because if not there would be finite subsets U & V of $K \cup Y^*$ such that $U \cup \{\psi\}$ and $V \cup \{\neg\psi\}$ are both inconsistent. But then it is easy to see that $U \cup V$ would be an inconsistent finite subset of $K \cup Y^*$, something which by assumption does not exist.

In the first case, let $Y = Y^* \cup \{\psi\}$ and $Z = Z^*$, in the second case let $Y = Y^* \cup \{\neg\psi\}$ and $Z = Z^* \cup \{\psi\}$. It is easy to see that in either case Y and Z satisfy all that is required of them for X.

Hence the result holds for all finite $X \subseteq L$. Thus as stated there must be some $Y \in F_1$ and $Z \in F_2$ such that $Y \cup Z = L$.

For each $\psi \in L$ either $\psi \in Y$ or $\neg\psi \in Y$. This is because the set $\{\psi, \neg\psi\}$ is not f.f. and so is not contained in Z.
Hence in particular this is true of the atomic propositional variables. Define a truth assignment s^* by $s^*(q)$ = <u>true</u> if $q \in Y$ and $s^*(q)$ = <u>false</u> if $\neg q \in Y$ (there can be no ambiguity as $\{q, \neg q\}$ is not consistent).

Claim that every statement in K is satisfied by s^*. This is true as for each $\psi \in K$ the set $\{\psi, \delta q \mid q \text{ occurs in } \psi\}$ is consistent, where $\delta q = q$ if $q \in Y$, $\delta q = \neg q$ otherwise.

Thus K is consistent as desired, completing the proof of 4.15.

This result means that our result is equivalent to several other results such as the so-called "ultrafilter lemma" (which can itself be easily proved from the truth of 4.10).

The consistency of this model under the $\otimes$ operator (and hence under the ($\|_X$) operator) has the implication that the parallel operator does not introduce any new non-determinism into a system in the following sense:

4.16 <u>Corollary</u>
If $(P \|_X Q) \xrightarrow{s} R$, where $R^\circ = Z$, then there exist P* & Q* such that $P \xrightarrow{s'} P^*$ and $Q \xrightarrow{s''} Q^*$ and $Z \cap (X \cup Y) = (X \cap P^\circ) \cup (Y \cap Q^\circ)$.
($s' = s \restriction X$, $s'' = s \restriction Y$).

The continuity of $\otimes$ follows immediately from its well-definedness in the following manner.

4.17 Theorem

The $\otimes$ operator is continuous.

proof

The continuity of $\otimes$ in both arguments follows from its continuity in its two arguments seperately, and that in one argument follows from that in the other by commutativity. It will thus suffice to show that if D is a directed set of processes then for each N M we have $(\bigsqcup D) \otimes N = \bigsqcup_{Q \in D} (Q \otimes N)$.

That $(\bigsqcup D) \otimes N \sqsupseteq \bigsqcup_{Q \in D} (Q \otimes N)$ follows easily from monotonicity, so it is sufficient to show that $(s,X) \in \bigsqcup_{Q \in D} (Q \otimes N) \Rightarrow (s,X) \in (\bigsqcup D) \otimes N$.

Suppose that $(s,X) \in \bigsqcup_{Q \in D} (Q \otimes N)$. By left-closure $(s,X^*) \in \bigsqcup_{Q \in D} (Q \otimes N)$ for each finite $X^* \subseteq X$. For each $Q \in D$ therefore there is a non-empty set $\Theta(Q) = \{Y \in Q(s) \mid \exists Z \in N(s). Z \cup Y = X^*\}$. Of necessity $\Theta(Q)$ is finite as it is a subset of the finite set $\wp(X^*)$, and we also have $Q' \sqsupseteq Q \Rightarrow \Theta(Q') \subseteq \Theta(Q)$. As a downwards-directed set of finite non-empty sets the $\Theta(Q)$ have a non-empty intersection.

There is therefore some $Y \in \bigcap_{Q \in D} Q(s)$ such that $\exists Z \in N(s). Y \cup Z = X^*$. But $\bigcap_{Q \in D} Q(s) = (\bigsqcup D)(s)$, which tells us that $X^* \in (\bigsqcup D) \otimes N(s)$. Since $(\bigsqcup D) \otimes N(s)$ contains each finite subset of X, and as $(\bigsqcup D) \otimes N$ is a well-defined process by 4.15 we have the desired result that $X \in (\bigsqcup D) \otimes N(s)$.

Appendix to Chapter 4 :- Definitions of Operators

Suppose that A, B, A_x ($x \in T$) are all elements of M, the space of non-deterministic processes, $a \in \Sigma^-$, $X, Y \subseteq \Sigma$, and T is a set of unnamed elements of Σ^-.

(i) $\quad CHAOS = \{(w,X) \mid w \in \Sigma^* \ \& \ X \subseteq \Sigma\}$

(ii) $\quad \underline{abort} = \{(\langle\rangle, X) \mid X \subseteq \Sigma\}$

(iii) $\quad \underline{skip} = \{(\langle\rangle, X), (\langle\surd\rangle, Y) \mid X \subseteq \Sigma^- \ \& \ Y \subseteq \Sigma\}$

(iv) $\quad a \rightarrow A = \{(\langle\rangle, X) \mid a \notin X\} \cup \{(\langle a\rangle w, X) \mid (w,X) \in A\}$

(v) $\quad x{:}T \rightarrow A_x = \{(\langle\rangle, X) \mid X \cap T = \emptyset\} \cup \{(\langle x\rangle w, X) \mid (w,X) \in A_x \ \& \ x \in T\}$

(vi) $\quad a.x{:}T \rightarrow A_x = \{(\langle\rangle, X) \mid X \cap a.T = \emptyset\} \cup \{(\langle a.x\rangle w, X) \mid x \in T \ \& \ (w,X) \ A_x\}$

(vii) $\quad a.T = \{(a.w, X \cup a.Y) \mid (w,Y) \in A \ \& \ X \cap a.\Sigma^- = \emptyset\}$

(viii) $\quad A \ \underline{or} \ B = A \cup B$

(ix) $\quad A \,\Box\, B = \{(\langle\rangle, X \cap Y) \mid (\langle\rangle, X) \in A \ \& \ (\langle\rangle, Y) \in B\}$
$\qquad\qquad \cup \{(w,X) \mid w \neq \langle\rangle \ \& \ ((w,X) \in A \vee (w,X) \in B)\}$

(x) $\quad A;B = \{(w,X) \mid w \in (\Sigma^-)^* \ \& \ (w, X \cup \{\surd\}) \in A\}$
$\qquad\qquad \cup \{(wv, X) \mid w \in (\Sigma^-)^* \ \& \ w\langle\surd\rangle \in dom(A) \ \& \ (v,X) \in B\}$

(xi) $\quad A/X = \{(w/X, Y) \mid (w, X \cup Y) \in A\}$
$\qquad\qquad \cup \{(wv, Y) \mid Y \subseteq \Sigma \ \& \{s \in dom(A) \mid s/X = w\}$ is infinite$\}$

(xii) $\quad (A_X \|_Y B) = f_X(A) \otimes f_Y(B) \otimes RUN_{X \cup Y}$, where
$\qquad\qquad C \otimes D = \{(w, Z \cup V) \mid (w,Z) \in C \ \& \ (w,V) \in D\}$;
$\qquad\qquad f_Z(C) = \{(w,V) \mid (w \restriction Z, V) \in C \ \& \ V \subseteq Z\}$
$\qquad$ and $RUN_Z = \{(w,V) \mid w \in Z^* \ \& \ V \cap Z = \emptyset\}$

(xiii) If $\{\Gamma_1, .., \Gamma_k\}$ is a partition of some non-empty indexing set Λ, and if $A_1, .., A_k$ are functions $A_i : M^\Lambda \times \Gamma_i \rightarrow M$ then the recursively defined process

B_λ, where $\quad \xi \in \Gamma_1 \Rightarrow B_\xi \Leftarrow A_1$
$\qquad\qquad\qquad\quad \xi \in \Gamma_2 \Rightarrow B_\xi \Leftarrow A_2$
$\qquad\qquad\qquad\quad \ldots\ldots$
$\qquad\qquad\qquad\quad \xi \in \Gamma_k \Rightarrow B_\xi \Leftarrow A_k$

has the value $(\bigsqcup_{n=0}^{\infty} G^n(CHAOS^\Lambda))_\lambda$, where $G : M^\Lambda \rightarrow M^\Lambda$ is the function defined $G(\underset{\sim}{C})_\xi = A_i(\underset{\sim}{C}, \xi)$ (i chosen so that $\xi \in \Gamma_i$).

Chapter 5 :- Recursion Induction and Buffers

In this chapter we will see how many of the ideas introduced in chapter 2 extend naturally to the non-deterministic model M. We will then make a fairly extensive analysis of one particular predicate, namely "is a buffer", and its relationship with the pipe operator "$\gg$".

The first requirement for this extension is a class of restriction operators $\{\restriction n \mid n \in N\}$. It would be possible to make $A\restriction n$ deterministically "die" after n steps (as was done in 2.6). It is however more in the spirit of our partial order on M to have $A\restriction n$ dissolve into CHAOS after n steps. With this behaviour $A\restriction n$ will in some sense be the minimal process which models A up to stage n whereas in the definition suggested first $A\restriction n$ would be one of many maximal such processes. We will thus normally interpret $\restriction n$ as it is defined below.

5.1 $A\restriction n = \{(w,X) \mid (w,X) \in A \ \& \ |w| < n\} \cup \{(wv,X) \mid w \in dom(A) \ \& |w| = n\}$

Below is a summary of a few simple results about these operators.

5.2 Lemma

a) $A\restriction o = CHAOS$ for all $A \in M$.

b) $(A\restriction n)\restriction m = A \restriction min(m,n)$

c) $A\restriction n \sqsubseteq A\restriction n+1 \sqsubseteq A$

d) $\bigsqcup_{n<\omega} (A\restriction n) = A$

e) $\forall (w,X).\exists n.\forall A.\ (w,X) \in A \Leftrightarrow (w,X) \in A\restriction n$

We extend the definition of $\restriction n$ to vectors of processes in $M^{\wedge}$ as follows:

5.3 $(\underset{\sim}{A}\restriction n)_\lambda = (A_\lambda)\restriction n$.

The definitions of constructive and non-destructive functions and of continuous predicates are exactly the same as before.

5.4 a) A function $F:M^{\wedge} \to M^{\Gamma}$ is said to be <u>constructive</u> if it satisfies $\forall n.\forall \underset{\sim}{A} \in M^{\wedge}.\ F(\underset{\sim}{A})\restriction n+1 = F(\underset{\sim}{A}\restriction n)\restriction n+1$.

b) A function $F:M^{\wedge} \to M^{\Gamma}$ is said to be <u>non-destructive</u> if it satisfies $\forall n.\forall \underset{\sim}{A} \in M^{\wedge}.\ F(\underset{\sim}{A})\restriction n = F(\underset{\sim}{A}\restriction n)\restriction n$.

5.5 A predicate on $M^{\wedge}$ is said to be <u>continuous</u> if it satisfies $\forall \underset{\sim}{A} \in M^{\wedge}.(\forall n.\exists \underset{\sim}{B}.R(\underset{\sim}{B}) \ \& \ (\underset{\sim}{A}\restriction n = \underset{\sim}{B}\restriction n)) \Rightarrow R(\underset{\sim}{A})$.

5.6 Lemma (analogue of 2.11)

a) If $F:M^{\wedge} \to M^{\Gamma}$ and $G:M^{\Gamma} \to M^{\Delta}$ are non-destructive then so is GoF.

b) If a function is constructive then it is non-destructive.

c) If one of $F:M^{\wedge} \to M^{\Gamma}$ and $G:M^{\Gamma} \to M^{\Delta}$ is constructive and the other is non-destructive then GoF is constructive.

d) If $F:M^{\wedge} \to M^{\wedge}$ is constructive then it has a unique fixpoint.

proof

The proof is identical to that of 2.11 since it only depends on the properties of $\lceil n$, namely 2.8 ($\equiv$ 5.2), which hold in both models. The analysis required to show that an arbitrary monotonic function has a fixed point is more complicated on the complete partial order $M^{\wedge}$ than on the complete lattice $P^{\wedge}$.

5.7 Theorem

If $F:M^{\wedge} \to M^{\wedge}$ is a constructive function and if R is a continuous satisfiable predicate then the translation of rule 2.1 into the non-deterministic model is valid.

(i.e $(\forall \underset{\sim}{B}.\ R(\underset{\sim}{B}) \Rightarrow R(F(\underset{\sim}{B}))) \Rightarrow R(fix(F))$)

Again the proof of this is identical to that of 2.14.

It is possible to develop in this model a similar calculus to that used in the deterministic model for proving functions constructive and predicates continuous and satisfiable.

5.8 Theorem

The following predicates are all continuous:

$R(\underset{\sim}{A}) \equiv$

(i) $A_\lambda = B$

(ii) $A_\lambda = A_\kappa$

(iii) $A_\lambda \sqsubseteq B$

(iv) $A_\lambda \sqsupseteq B$

(v) $A_\lambda \sqsupseteq A_\zeta$

(vi) $A_\lambda \neq B$ if there is an upper bound on $\{|w| \mid (w,\emptyset) \in B\}$

(vii) "A_λ is deadlock-free" (in this model this is equivalent to $w \in (\Sigma - \{\surd\})^* \Rightarrow \Sigma \notin A_\lambda(w)$)

(viii) $(w,X) \in A_\lambda \Rightarrow p(w,X)$ if p is any predicate on $\Sigma^* \times \wp(\Sigma)$

(ix) $w \in dom(A_\lambda) \Rightarrow p_w((A_\lambda \text{ after } w)^o)$ if p_w are predicates on $\mathcal{P}(\Sigma)$

(x) $w \in dom(A_\lambda) \Rightarrow p_w(A_\lambda(w))$ if p_w are predicates on $\mathcal{P}(\mathcal{P}(\Sigma))$

(xi) $R_1(F(\underset{\sim}{A}))$ if $\exists g:N \to N$ s.t.
$\forall \underset{\sim}{B}.\forall n.F(\underset{\sim}{B})\lceil n = F(\underset{\sim}{B}\lceil g(n))\lceil n$
($F:M^{\wedge} \to M^{\Gamma}$ monotonic and R_1 a predicate on M^{Γ})

(xii) $F(\underset{\sim}{A}) \sqsubseteq \underset{\sim}{B}$ for any continuous $F:M^{\wedge} \to M^{\Gamma}$

(xiii) $\bigwedge_{\gamma \in \Gamma} R_\gamma(\underset{\sim}{A})$ for any set Γ

(xiv) $R_1(\underset{\sim}{A}) \vee R_2(\underset{\sim}{A})$

where B is any constant process R_1, R_2 and R_γ are all continuous and $\lambda \in \Lambda$.

The proofs of these results are similar to the proofs of 2.18, for example:

(v) $\neg(A_\lambda \supseteq A_\xi) \Rightarrow \exists (w,X) \in A_\lambda - A_\xi$
If $n = |w| + 1$ then clearly $\underset{\sim}{A}\lceil n = \underset{\sim}{B}\lceil n$ implies $(w,X) \in B_\lambda - B_\xi$, so $\neg(B_\lambda \supseteq B_\xi)$.

5.9 Theorem

a) Each of the combinators "a → A", $\|$, $\Box$, ";" , or, "a.A" defines a non-destructive function of its variable(s).

b) If a function $F:M^{\Gamma} \times M^{\wedge} \to M^{\wedge}$ is constructive (non-destructive) in its first variable* then $G:M^{\Gamma} \to M^{\wedge}$ defined $G(\underset{\sim}{A}) = fix(\lambda \underset{\sim}{B}.F(\underset{\sim}{A},\underset{\sim}{B}))$ is constructive (non-destructive).

c) Suppose that the function $F:M^{\wedge} \to M^{\wedge}$ is such that each component of $F(\underset{\sim}{A})$ is a syntactic expression involving only process variables, expressions independent of all process variables, the combinators a → B, a?x:T → B(x), ?x:T → B(x), B;C, B□C, a.B and $(B_X \|_Y C)$, and iterated recursions which bind all instances of process variables which are not $A_\lambda{}^S$. Then provided that every free recursive call of an A_λ is guarded directly or indirectly the function F is constructive.

proof

These are all similar to the correponding results in the deterministic model (namely 2.15, 2.36 & 2.37), the only difference being in the analysis of the individual combinators. The only one to present a slight difficulty is ";" because of the way it "hides" the "✓".

(* and non-destructive in its second variable)

Recall the definition of sequential composition:

$$A;B = \{(w,X) \mid w/\{\surd\} = w \ \&\ (w, X\{\surd\}) \in A\}$$
$$\{(wv,X) \mid w/\{\surd\} = w \ \&\ w\langle\surd\rangle \in dom(A) \ \&\ (v,X) \in B\}$$

We would like to show that $(A\lceil n;B\lceil n)\lceil n = (A;B)\lceil n$.
It is clearly sufficient to show that

a) $(A\lceil n;B\lceil n) \cap \{(w,X) \mid |w| < n\} \Rightarrow A;B \cap \{(w,X) \mid |w| < n\}$

b) $dom(A\lceil n;B\lceil n) \cap \{w \mid |w| = n\} = dom(A;B) \cap \{w \mid |w| = n\}$

In each case the containment of the R.H.S. within the L.H.S. follows from monotonicity.

$(w,X) \in (A\lceil n;B\lceil n) \cap \{(w,X) \mid |w| < n\}$

$\Rightarrow$ <u>either</u> $(w,X) \in \{(w,X) \mid w/\{\surd\} = w \ \&\ (w, X\{\surd\}) \in A\lceil n\}$

$\Rightarrow$ $(w,X) \in \{(w,X) \mid w/\{\surd\} = w \ \&\ (w, X\{\surd\}) \in A\}$ as $|w| < n$

$\Rightarrow$ $(w,X) \in A;B$

<u>or</u> $(w,X) = (uv,X)$ for some u,v s.t. $u/\{\surd\} = u$
$u\langle\surd\rangle \in dom(A\lceil n)$ & $(v,X) \in B\lceil n$
now $|v| < n$ so $(v,X) \in B$
and $|u\langle\surd\rangle| \leq n$ so $u\langle\surd\rangle \in dom(A)$
thus $(uv,X) \in A;B$.

$w \in dom(A\lceil n;B\lceil n) \cap \{w \mid |w| = n\}$

$\Rightarrow$ <u>either</u> $w \in \{w \in dom(A\lceil n) \mid w/\{\surd\} = w\}$

$\Rightarrow$ $w \in \{w \in dom(A) \mid w/\{\surd\} = w\}$ as $|w| = n$

<u>or</u> $w \in \{uv \mid u/\{\surd\} = u \ \&\ u\langle\surd\rangle \in dom(A\lceil n) \ \&\ v \in dom(B)\}$
now either $|u\langle\surd\rangle| \leq n$ & $|v| \leq n$, in which case $uv \in dom(A;B)$ as required,
or $|u\langle\surd\rangle| = n+1$ and $v = \langle\rangle$ in which case $w = u$ and $w \in$ (first clause of $A;B$).

The proofs of the non-destructive nature of the other operators require similar tedious analysis.

Other parts of the deterministic theory to be valid in this model are the extensions for partial predicates and constructiveness relative to partial orders (and also the simple 2.21). In each case it will be seen that the proofs depend only on properties shared by the two models and the classes of functions and operators defined on them. These results are not stated as formal theorems in this model but will be used wherever necessary. It is noteworthy that all the examples of program-proving in

chapter 2 are equally valid over the non-deterministic model M. With the exception of the buffers example, where the predicate needs translation to make sense in M, all the proofs can equally well be read as proofs in the non-deterministic model. This is because the various combinators have much the same properties (commutativity, distributivity, etc.) in both models (with a few exceptions which are not used in any of these proofs). The analysis needed to justify the constructiveness of the master/slave operator in 2.39 over M will be found in the next chapter.

The only part of the theory in chapter 2 which does not seem to transfer effectively to M is the work on unique fixed points and strongly continuous predicates. The main reason for this is that M has no "top" element. It is still possible to define a strongly continuous predicate and show that such predicates are continuous w.r.t. every normal restriction operator class. This is useful, since it saves work when we wish to use different operators.

5.10 Define a sequence of processes to be <u>convergent</u> if it satisfies $\mathrm{limsup}(A_i) = \mathrm{liminf}(A_i)$ where these operators act setwise on M, and if this limit is in M.

$\mathrm{liminf}(A_i) = \tilde{\bigcup}_{j=1}(\tilde{\bigcap}_{i=j} A_i)$, $\mathrm{limsup}(A_i) = \tilde{\bigcap}_{j=1}(\tilde{\bigcup}_{i=j} A_i)$

(Observe that in general $\mathrm{liminf}(A_i)$ and $\mathrm{limsup}(A_i)$ are not necessarily elements of M.)

Define a predicate on M to be <u>strongly continuous</u> if it satisfies "$\langle A_i \mid i \in N\rangle$ convergent with limit A and $\forall i.R(A_i)$ implies $R(A)$".

5.11 Define a class $\{\lceil n \mid n \in N\}$ of restriction operators on M to be <u>normal</u> if they satisfy:

a) $\forall A.\ \forall B.\ A\lceil o = B\lceil o$

b) $\forall A.\ \forall n.\forall m.\ (A\lceil n)\lceil m = A\lceil \min(m,n)$

c) $\forall (w,X).\exists n.\forall A.\ (w,X) \in A \Leftrightarrow w \in A\lceil n$

(This is just a translation of 2.49. Observe that we have already shown that the canonical class of restriction operators is normal (5.2).)

5.12 Theorem

If a predicate R is strongly continuous then it is continuous with respect to every normal class of restriction operators.

The proof of this is the same as that of 2.50.

5.13 Theorem

The following predicates are all strongly continuous.

$R(A) \equiv$ (i) $A = B$

(ii) $A \sqsupseteq B$

(iii) $A \sqsubseteq B$

(iv) $(w,X) \in A \Rightarrow p(w,X)$ where p is any predicate on $\Sigma^* \times \mathcal{P}(\Sigma)$

(v) "A is free of deadlock"

(vi) $F(A) \sqsubseteq B$ if F is continuous

(vii) $\bigwedge_{\gamma \in \Gamma} R_\gamma(A)$

(viii) $R_1(A) \vee R_2(A)$

where B is any constant process and R_1, R_2 and R_γ are all strongly continuous.

Note that freedom from deadlock is strongly continuous in this model, whereas it is not in the deterministic model. The reason for this is that absence of deadlock is represented in M by "$\Sigma \notin A(w)$ for any $w \in dom(A)$ s.t. w has not already terminated successfully". Thus, for any such w, if none of a sequence $\langle A_i \mid i \in N \rangle$ deadlocks after w then $\forall i.(w, \Sigma) \notin A_i$. Therefore $(w, \Sigma) \notin limsup(A_i)$ so $lim(A_i)$ cannot deadlock after w either.

One consequence of this is that the function $F(A) = a.A$ cannot be constructive relative to any normal class of restriction operators (see 2.41). (a.A can be made constructive in P, by defining $A\restriction n = A \cap \Sigma_n^*$, where Σ_n contains all those elements of Σ with less than n "components".)

Henceforth "$\restriction n$" will always be the canonical operator (5.1, 5.3) unless specifically stated otherwise.

We will now prove the two extensions (stated in 2.33 and 2.34 for P) whose proofs were delayed until this chapter.

5.14 Theorem

If $A \in \mathcal{P}(M^{\wedge})$ define $A\lceil n = \{\underset{\sim}{B}\lceil n \mid \underset{\sim}{B} \in A\}$.
Define a function $F: \mathcal{P}(M^{\wedge}) \to \mathcal{P}(M^{\wedge})$ to be constructive if it satisfies $\forall A.\forall n.\ F(A)\lceil n+1 = F(A\lceil n)\lceil n+1$.
Suppose the predicate R on $M^{\wedge}$ is satisfiable and continuous, then we have

$(\forall A'.(\forall \underset{\sim}{B}.(\underset{\sim}{B} \in A' \Rightarrow R(\underset{\sim}{B})))) \Rightarrow (\forall \underset{\sim}{B}.(\underset{\sim}{B} \in F(A') \Rightarrow R(\underset{\sim}{B}))) \ \&\ (A \subseteq F(A))$

implies $(\forall \underset{\sim}{B}.\underset{\sim}{B} \in A \Rightarrow R(\underset{\sim}{B}))$.

proof

If A is empty then the result is trivial, so we may assume that it is not. Clearly for all non-empty sets A' we have $A'\lceil o = \{CHAOS^{\wedge}\}$ so in particular $A_o\lceil o = A\lceil o$, where A_o is the set of processes which satisfy R (non-empty by satisfiability).
Suppose that $(\forall \underset{\sim}{B}.\underset{\sim}{B} \in A \Rightarrow R(\underset{\sim}{B}))$ does not hold. Then there must be some $n \in N$ which is maximal with respect to $\exists A_n.A_n\lceil n = A\lceil n \ \&\ (\forall \underset{\sim}{B}.\underset{\sim}{B} \in A_n \Rightarrow R(\underset{\sim}{B}))$ (by continuity of R).
Then $F(A)\lceil n+1 = F(A\lceil n)\lceil n+1 = F(A_n\lceil n)\lceil n+1 = F(A_n)\lceil n+1$ by constructiveness of F.
Let $C = F(A_n)$. By our assumptions we must have $(\forall \underset{\sim}{B}.\underset{\sim}{B} \in C \Rightarrow R(\underset{\sim}{B}))$.
Also $A \subseteq F(A)$, so $A\lceil n+1 \subseteq F(A)\lceil n+1 = C\lceil n+1$.
Thus $\forall \underset{\sim}{B} \in A.\ \exists \underset{\sim}{B}_{\S}' \in C.\underset{\sim}{B}\lceil n+1 = \underset{\sim}{B}_{\S}'\lceil n+1$.
Let $A_{n+1} = \{\underset{\sim}{B}_{\S}' \mid \underset{\sim}{B} \in A\}$. By definition $A_{n+1}\lceil n+1 = A\lceil n+1$ and $(\forall \underset{\sim}{B}.\underset{\sim}{B} \in A_{n+1} \Rightarrow R(\underset{\sim}{B}))$ since $A_{n+1} \subseteq C$. This contradicts our choice of n, so $(\forall \underset{\sim}{B}.\underset{\sim}{B} \in A \Rightarrow R(\underset{\sim}{B}))$ does hold as claimed.

5.15 Theorem

Suppose that $R_1,\ldots,R_n$ are predicates which are all continuous and satisfiable (but possibly not simultaneously satisfiable). Suppose further that $F: M^{\wedge} \to M^{\wedge}$ is a function which, for each $i \in \{1,2,\ldots n\}$ can be written in the form $F_i^* \circ D$, for some $F: (M^{\wedge})^n \to M^{\wedge}$ which is constructive and where $D(\underset{\sim}{A}) = (\underset{\sim}{A},\underset{\sim}{A},\ldots,\underset{\sim}{A})$ for $\underset{\sim}{A} \in M^{\wedge}$.
Then if for each i we can prove for all $\underset{\sim}{A}_1,\ldots,\underset{\sim}{A}_n \in M^{\wedge}$

$$R_1(\underset{\sim}{A}_1) \ \&\ \ldots\ \&\ R_n(\underset{\sim}{A}_n) \Rightarrow R_i(F_i^*(\underset{\sim}{A}_1,\ldots,\underset{\sim}{A}_n))$$

we can infer $\forall i.R_i(fix(F))$.

proof

This is just an application of 5.7. Define $G:(M^{\wedge})^n \to (M^{\wedge})^n$ by $G(\underset{\sim}{A}_1,\ldots\underset{\sim}{A}_n) = (F_1^*(\underset{\sim}{A}_1,\ldots,\underset{\sim}{A}_n),\ldots,F_n^*(\underset{\sim}{A}_1,\ldots,\underset{\sim}{A}_n))$.
Define the compound predicate R* on $(M^{\wedge})^n$ by
$R^*(\underset{\sim}{A}_1,\ldots\underset{\sim}{A}_n) \equiv R_1(\underset{\sim}{A}_1)\ \&\ R_2(\underset{\sim}{A}_2)\&\ldots\&\ R_n(\underset{\sim}{A}_n)$.
G is constructive since each of the F_i^* is.
R* is continuous since each of the R* is.
R* is satisfiable, by $(\underset{\sim}{A}_1^*,\ldots,\underset{\sim}{A}_n^*)$ where $\underset{\sim}{A}_i^*$ satisfies R_i.

$\underset{\sim}{A} \in (M^{\wedge})^n \Rightarrow (R^*(\underset{\sim}{A}) \Rightarrow R^*(G(\underset{\sim}{A}))$ by the assumptions in the statement of the theorem.
We can therefore infer R*(fix(G)) by 5.7.

Claim that fix(G) = (fix(F),fix(F),...,fix(F)) (= $\underset{\sim}{C}$, say).

G has a unique fixed point by 5.6 (d), but $G(\underset{\sim}{C}) = \underset{\sim}{C}$ since $F_i^*(\underset{\sim}{C}) = F_i^*(D(\text{fix}(F))) = F(\text{fix}(F)) = \text{fix}(F)$.
Thus $\underset{\sim}{C}$ = fix(G) as claimed, and so we can infer $R^*(\underset{\sim}{C})$, which is the result we desired.

As was said in chapter 2 this result will allow us to prove several results of fix(F) by mutual induction, even though we may not know them to be consistent. The proof used must only assume one of the said properties of each recursive call in the proof of each hypothesis. It is however permissible to assume different properties of different calls of the same process, and to assume different properties of the same call provided that these assumptions are in the proofs of different hypotheses.

An example of the use of this rule will be found in 6. , and an example of rule 5.14 in 5.27.

We will now turn our attention to the detailed examination of a specific predicate, namely "is a buffer". This, in addition to being a useful exercise in demonstrating the use of our techniques, is also a useful predicate to have knowledge of. This is because we wish to prove either this property or a very similar one of such processes as operating systems, communication channels, etc.

By the predicate Buff = "is a buffer" we would like not only to be able to prove partial correctness, but also total correctness as was done in 2.20.

We therefore take as our definition of a buffer the following reworking of the predicate used in 2.20.

5.16 $Buff(B) \equiv$

$$(i)\quad w \in dom(B) \Rightarrow w \in (?T \cup !T)^* \;\&\; ins(w) \geqslant outs(w)$$
$$\&\ (ii)\quad (w \in dom(B) \;\&\; ins(w) = outs(w)) \Rightarrow B(w) = \{X \mid X \cap ?T = \emptyset\}$$
$$\&\ (iii)\quad (w \in dom(B) \;\&\; ins(w) > outs(w)) \Rightarrow !T \notin B(w)$$

The motivation for these conditions (i), (ii) & (iii) is the same as that in 2.20.

In almost exactly the same fashion as 2.20 we could prove that the above three conditions are simultaneously satisfied by the canonical one-place buffer $B \Leftarrow ?x{:}T \rightarrow (!x \rightarrow B)$. That Buff is continuous follows immediately from 5.8. It is in fact strongly continuous, since (ii) and (iii) above are easily rewritten in the form 5.13 (iv).

As we will see shortly, the theory of buffers links closely with the theory of the pipe operator "$\gg$". This can be modelled more reasonably in this model since the non-determinism of the hiding can now be expressed. Its formal definition is as follows:

5.17 $(A \gg B) = (strip!(A)\ {}_{T \cup ?T}\|_{T \cup !T}\ strip?(B))/T$

where $stripa(A) = \{(stripa(w), stripa(X - T) \cup Y) \mid (w,X) \in A \;\&\; Y \subseteq \hat{a}.T\}$.

The definition of strip on strings is the same as in chapter 2 and that on sets the natural extension of that on Σ.

Because of the hiding used in its definition, we will assume that the set T of basic values for communication is finite whenever "$\gg$" is used. It is also necessary to assume that $?T = \{?.x \mid x \in T\}$ and $!T = \{!.x \mid x \in T\}$ are both disjoint from T.

This definition is in some sense only reasonable if the processes A and B only communicate in the alphabet $!T \cup ?T$, for otherwise the "strip" operator identifies events which should not be identified. We will therefore ensure that all processes which we expect to to act sensibly when combined by "$\gg$" satisfy this.

We will now spend a little time developing a calculus for "$\gg$" before we start to apply it to buffers.

5.18 Lemma

"$\gg$" is a well-defined continuous operator in $M \times M \to M$ providing that T is finite. Furthermore we have the following criterion for membership of $(A \gg B)$:

$(w,W) \in (A \gg B)$ if and only if

either there is some $w' \leqslant w$ such that

$$\{t \mid (t\restriction(T \cup ?T) \in strip!(dom(A))) \;\&\; (t\restriction(!T \cup ?T) = w') \;\&\; (t\restriction(T \cup !T) \in strip?(dom(B)))\} \text{ is infinite}$$

or there are some $(u,U) \in A$ and $(v,V) \in B$ such that

$$(W \cap (!T \cup ?T)) \cup T = strip!(U - T) \cup strip?(V - T) \text{ and}$$
$$t\restriction(T \cup ?T) = strip!(u) \;\&\; t\restriction(T \cup !T) = strip?(v) \;\&$$
$$t\restriction(?T \cup !T) = w \;.$$

(In this last case say that $((u,U),(v,V))$ is a derivation for (w,W) in $(A \gg B)$ or that $((u,U),(v,V)) \Leftrightarrow (w,W)$ in $(A \gg B)$.)

proof

The first part of this follows from the same result of the various operators from which "$\gg$" is defined. These results are already known except for the "strip" operator, which is easy to verify.

The second part comes straight from the definition of the operator, using the following result on the parallel operator.

$$(w,W) \in (A_X \|_Y B) \Leftrightarrow \exists (u,U) \in A.\ \exists (v,V) \in B \text{ s.t.}$$
$$w\restriction(X \cup Y) = w \;\&\; w\restriction X = u \;\&\; w\restriction Y = v \;\&$$
$$W \cap (X \cup Y) = (U \cap X) \cup (V \cap Y)$$

If the either clause in the above definition is satisfied by some $(w,W) \in (A \gg B)$ then we say that $(A \gg B)$ contains infinite internal chatter.

5.19 Theorem

If $dom(A \text{ or } B \text{ or } C) \subseteq (!T \cup ?T)^*$ and both $(A \gg B)$ and $(B \gg C)$ are free of infinite internal chatter then the associative law holds, viz

$$((A \gg B) \gg C) = (A \gg (B \gg C)) \;.$$

proof

We use the following lemma, which will be proved in an appendix to this chapter (5.35).

If A is free of infinite X-chatter and $X \cap Z = \emptyset$ then

$$(A/X_Y||_Z B) = (A_{X \cup Y}||_Z B)/X \quad .$$

"$\gg$" works by identifying the outputs of its first variable with the inputs of its second and hiding the resulting internal communication. It is possible to change the method of identification without changing the result. Instead of transforming the joint communications to T we can transform them to a.T for "a" any suitable label. Define a replacement operator repab (for replacing label "a" by label "b") as follows for any a,b such that $a \neq b$ and $a.T \cap b.T = \emptyset$.

For $c \in \Sigma$ $\quad repab(c) = b.x$ if $c = a.x$ for any $x \in T$

$\qquad\qquad\qquad\qquad = c \quad$ otherwise

For $w \in \Sigma^*$ and $X \in \mathcal{P}(\Sigma)$ repab(w) and repab(X) are the natural elementwise extensions of the above.

For $A \in M$ $\quad repab(A) =$

$$\{(repab(w), repab(X - b.T) \cup Y) \mid (w,X) \in A \ \& \ Y \subseteq a.\Sigma\}$$

With this definition it is quite easy to show that provided "a" is chosen so that a.T is disjoint from both ?T and !T and A,B satisfy $dom(A \underline{or} B) \subseteq (!T \cup ?T)^*$ then $(A \gg B) = (rep!a(A)_{a.T \cup ?T}||_{a.T \cup !T} rep?a(B))/a.T$.

Thus under the conditions of the theorem, if "a" and "b" are chosen so that !T, ?T, a.T and b.T are all disjoint (if they do not exist then enlarge Σ) then $((A \gg B) \gg C) =$

$(rep!b((rep!a(A)_X||_Y rep?a(B))/a.T)_Z||_W rep?b(C))/b.T$

where $X = ?T \cup a.T$, $Y = !T \cup a.T$, $Z = ?T \cup b.T$, $W = !T \cup b.T$

$= ((rep!a(A)_X||_V rep!b(rep?a(B)))/a.T_Z||_W rep?b(C))/b.T$

where $V = a.T \cup b.T$ (by various properties of "rep")

$= ((rep!a(A)_X||_V rep!b(rep(?a(B)))_{Z \cup a.T}||_W rep?b(C))/(a.T \cup b.T)$

(by 4.7 and the lemma at the head of the page)

A symmetric expression can be derived for $(A \gg (B \gg C))$ using "a" again for the first channel and "b" for the second. These two are then equal by the associative law of || and the commutativity of rep!b and rep?a .

The next result gives us a useful technique for proving that processes of the form $(A \gg B)$ are free of infinite chatter (a desirable result in its own right as well as in its use in proving associativity).

5.20 Theorem

Each of the two predicates:

$P_1(A) \equiv \neg\exists\, w_1 < w_2 < w_3 < \ldots \in dom(A)$ s.t. $\forall i . w_i \restriction ?T = w_1 \restriction ?T$

(A cannot output for ever without inputting)

$P_2(A) \equiv \neg\exists\, w_1 < w_2 < w_3 < \ldots \in dom(A)$ s.t. $\forall i . w_i \restriction !T = w_1 \restriction !T$

(A cannot input for ever without outputting)

satisfies $(i \in \{1,2\})$ (for $dom(A \text{ or } B) \subseteq (?T \cup !T)^*$)

$P_i(A)$ & $P_i(B) \Rightarrow (P_i(A \gg B)$ & $(A \gg B)$ is free of infinite internal chatter) .

proof

We will prove the result for i=1, the proof for i=2 being very similar.

Suppose That P_1 holds of both A & B. We will prove first that $(A \gg B)$ is free of infinite chatter.

If not there is some minimal $w \in dom(A \gg B)$ such that

$\{t \mid (t \restriction (T \cup ?T) \in strip!(dom(A)))$ & $(t \restriction (!T \cup T) \in strip?(dom(B)))$ & $(t \restriction (!T \cup T) = w)\}$ is infinite.

It is easy to show (for the same reasons as 4.6) that the number of minimal elements of this set is finite. König's lemma then gives us that it contains an infinite ascending chain $t_1 < t_2 < t_3 < \ldots$ (because T is finite).

There must therefore be an infinite sequence $\langle u_i \mid i \in N \rangle$ in dom(A) such that $strip!(u_i) = t_i \restriction (T\ ?T)$.

Since $dom(A) \subseteq (!T \cup ?T)^*$ the u_i must be an ascending sequence and $u_i \restriction ?T = (strip!(u_i)) \restriction ?T = t_i \restriction ?T = w \restriction ?T$. Hence the u_i contradict $P_1(A)$. $(A \gg B)$ is thus free of infinite internal chatter as claimed.

In proving that P_1 holds of $(A \gg B)$ we may thus assume that all elements of it arise from the "or" clause in 5.18.

Suppose that $w_1 < w_2 < w_3 < \ldots$ is an infinite sequence in $dom(A \gg B)$ with $w_i \restriction ?T$ constant.

For each w_i there must be some $(u_i, U) \in A$ and $(v_i, V) \in B$ such that $((u_i, U), (v_i, V)) \Leftrightarrow (w_i, \emptyset)$ in $(A \gg B)$.

These must satisfy the relations:

$$u_i \restriction ?T = w_i \restriction ?T = w_1 \restriction ?T \quad \text{(all the same)}$$
$$\text{strip}!(u_i \restriction !T) = \text{strip}?(v_i \restriction ?T) \; (= s_i \text{, say})$$
$$v_i \restriction !T = w_i \restriction !T > v_{i-1} \restriction !T \quad \text{(all different)} .$$

It is easy to see from this that either there are infinitely many s_i or there is some i such that $\{j \mid s_i = s_j\}$ is infinite.
The first case contradicts $P_1(A)$ for then the tree of $u \in \text{dom}(A)$ s.t. $u \restriction ?T = u_1 \restriction ?T$ is infinite.
Claim this would contradict $P_1(A)$ for any $u' \in ?T^*$ (corresponding to $u_1 \restriction ?T$ in the above). If $|u'| = 0$ then $u' = \langle\rangle$ so the tree has one minimal element, and is finite branching as T is finite, and so has an infinite path which contradicts $P_1(A)$.
Assume true of all shorter u". If the tree has infinitely many minimal elements for u' $(= u''\langle a\rangle$, say) then each of these is of the form $u\langle a\rangle$. Thus the tree for u" is infinite, contradicting $P_1(A)$ by induction. If the tree has finitely many minimal elements then by the same argument as above it contains an infinite path which contradicts $P_1(A)$. This completes the induction, and so in particular the infinitude of $\{u \in \text{dom}(A) \mid u \restriction ?T = u_1 \restriction ?T\}$ contradicts $P_1(A)$ as claimed.
The same argument shows that the second case above contradicts $P_1(B)$, for then $\exists v \in \text{dom}(B).\{i \mid v \restriction ?T = v_i \restriction ?T\}$ is infinite.
Hence there can be no such sequence $w_1 < w_2 < w_3 < \ldots$, so $P_1(A \gg B)$ holds as claimed.

Note that under the conditions of the theorem we in addition have $\text{dom}(A \gg B) \subseteq (!T \cup ?T)^*$, this result being a consequence of the lack of infinite chatter and 5.18.

The two predicates P_1 and P_2 are both discontinuous, since at no finite time can their negations be decided. There are however a large class of continuous and strongly continuous predicates which imply one or other of them. For example Buff $\Rightarrow P_1$ (by line (i) of 5.16).

5.21 Corollary .
If for $i \in \{1,2\}$ each of $A_1, A_2, \ldots, A_k$ satisfies P_i then we may bracket $A_1 \gg A_2 \gg \ldots \gg A_k$ however we please and get the same answer. Furthermore the result is free of infinite internal chatter and satisfies P_i.

The proof of this is an easy induction on k using 5.19 and 5.20.

Note that if A & B both satisfy P_i then most of the normal combinators applied to A (& B) produce a process which satisfies P_i, for example "$a \to A$" ($a \in (?T \cup !T)$), "$?x:T \to A$", "$A \Box B$". We will therefore be quite informal in the use of 5.20 & 5.21 in proofs, not always justifying their application to a particular set of processes if they are known to be justified for similar ones. For example if A,B,C are buffers then

$$((A \gg (b \to B)) \gg C) = (A \gg ((b \to B) \gg C)) .$$

(The inclusion of such details would clutter up the proofs, so they are omitted on the basis that we could insert them if challenged.)

The following lemma (which will be used freely and informally in proofs) allows us to do basic "handle turning" in proofs involving "$\gg$".

5.22 Lemma

a) $((!y \to A) \gg (?x:T \to B(x))) = (A \gg B(y)) \quad (y \in T)$

b) $((?x:T \to A(x)) \gg B) = ?x:T \to (A(x) \gg B)$ if $B^o \subseteq ?T$

c) $(A \gg (!y \to B)) = !y \to (A \gg B)$ if $A^o \subseteq !T$ & $y \in T$

d) $((?x:T \to A(x)) \gg (!y \to B)) = ?x:T \to (A(x) \gg (!y \to B)) \;\Box\; !y \to ((?x:T \to A(x)) \gg B)$

e) $((?x:T \to A(x)) \gg C \gg (!y \to B)) =$
$(?x:T \to (A(x) \gg C \gg (!y \to B))) \Box (!y \to ((?x:T \to A(x)) \gg C \gg B))$
provided that the associative law holds ($y \in T$)

f) $(A \text{ or } B \gg C \text{ or } D) = (A \gg C) \text{ or } (A \gg D) \text{ or } (B \gg C) \text{ or } (B \gg D)$

g) If $A^o \cup C^o \subseteq ?T$ and $B^o \cup D^o \subseteq !T$ then let
$E = (\text{strip}!(B)_{T \cup ?T} \|_{T \cup !T} \text{strip}?(C))$.
If $\surd \notin E(\langle\rangle)$ then $((A \Box B) \gg (C \Box D)) \sqsubseteq (B \gg C)$.
(A lower bound can be obtained from (f) by monotonicity.)

provided that the domains of all processes $\subseteq (?T \cup !T)^*$.

The proofs of 5.22 are all tedious manipulations using 5.18 and the definitions of the various operators.

We are now in a position to apply our knowledge to the study of the relationship between pipes and buffers.

5.23 Theorem
If any two of A,B & $(A \gg B)$ are buffers then so is the third (for any $A,B \in M$ s.t. $dom(A \text{ or } B) \subseteq (?T \cup !T)^*$).

proof
Observe that in each case there can be no infinite chatter in $(A \gg B)$, either because buffers satisfy P_1 or because no process which contains infinite chatter can be a buffer.

Thus in each case we can restrict attention to the "or" case of 5.18.
We will examine only the "A & B buffers imply $(A \gg B)$ is a buffer" case in detail here. The proofs of the other two cases are similar in spirit and equally tedious.

Suppose Buff(A) & Buff(B).
To prove Buff$(A \gg B)$ we will prove the three conditions 5.16 (i),(ii) & (iii) in turn.

(i) Suppose $w \in dom(A \gg B)$. $w \in (!T \cup ?T)^*$ follows by the absence of infinite chatter.
There must be some $(u,U) \in A$ & $(v,V) \in B$ such that
$((u,U),(v,V)) \Leftrightarrow (w,\emptyset)$ in $(A \gg B)$.
But then
$$\begin{aligned} ins(w) &= ins(u) && \text{by definition of ins} \\ &\geqslant outs(u) && \text{as A is a buffer} \\ &\geqslant ins(v) && \text{as } ins(v) = outs(u) \\ &\geqslant outs(v) && \text{as B is a buffer} \\ &\geqslant outs(w) && \text{as } outs(v) = outs(w) \end{aligned}$$

(For proving this condition in the other two cases we use the fact that all strings of the process in question must also be strings of $(A \gg B)$ as the one which is known to be a buffer must have all strings in $\{?x!x\rangle \mid x \in T\}^*$ in its domain.)

(ii) Suppose $w \in dom(A \gg B)$ and that $ins(w) = outs(w)$.
Since $(A \gg B)$ satisfies condition (i) we must have
$((A \gg B) \text{ after } w)^{\circ} \subseteq ?T$.

Hence $X \cap ?T = \emptyset \Rightarrow X \in (A \gg B)(w)$ (by 4.1 (c))
so $\{X \mid X \cap ?T = \emptyset\} \subseteq (A \gg B)(w)$. (*)
Suppose then that $X \in (A \gg B)(w)$. By 5.18 there exist
$(u,U) \in A$, $(v,V) \in B$ such that $ins(w) = ins(u) \geqslant outs(u)$
$= ins(v) \geqslant outs(v) = outs(w)$ (using Buff(A) & Buff(B))
and $X \cap (?T \cup !T) = (U \cap ?T) \cup (V \cap !T)$.
But then $ins(u) = outs(u)$ (since $ins(w) = outs(w)$)
so $X \cap ?T = U \cap ?T = \emptyset$ (by line (ii) of Buff(A)).

Thus $(A \gg B)(w) \subseteq \{X \mid X \cap ?T = \emptyset\}$ which together with (*)
above proves line (ii).

(iii) Suppose $w \in dom(A \gg B)$ and $ins(w) > outs(w)$.
We require to show that $!T \notin (A \gg B)(w)$.
Suppose to the contrary that $(w,!T) \in (A \gg B)$.
Then there are some $(u,U) \in A$ and $(v,V) \in B$ such that
$ins(w) = ins(u) \geqslant outs(u) = ins(v) \geqslant outs(v) = outs(w)$
and $!T \cup T = ((T \cup ?T) \cap (strip!(U - T))) \cup ((T \cup !T) \cap (strip?(V - T)))$.
Either $ins(v) > outs(v)$, in which case $V \cap !T \neq !T$ by
line (iii) of Buff(B), contradicting above relation.
Or $ins(v) = outs(v)$, in which case $ins(u) > outs(u)$.
Then $V \cap ?T = \emptyset$, so $strip?(V - T) \cap T = \emptyset$.
Also $U \cap !T \neq !T$, so $strip!(U - T) \cap T \neq \emptyset$.

But then we have $T = (T \cap strip!(U - T)) \cup (T \cap strip?(V - T))$
by the above, giving a contradiction.

Hence $!T \notin (A \gg B)(w)$ as required, completing the proof
that $(A \gg B)$ is a buffer.

One corollary to this is that if $B^n = B \gg B \gg B \gg \ldots \gg B$ (n"B"s)
where B is the canonical one place buffer of 5.16 then
B^n is a buffer.

The following two results on nested buffers can be proved
in much the same way as 5.24.

5.24 Theorem
a) If $A \gg B \gg C$ and B are both buffers then so is $A \gg C$.
b) If $A \gg C$ and B are buffers and A satisfies the "single
inevitable output" condition SIO(A) (see over) or C satisfies $\forall w.\forall x.(w\langle ?x\rangle \in dom(C) \Rightarrow (\forall y.w\langle ?y\rangle \in dom(C)))$, then
$A \gg B \gg C$ is a buffer.

$$SIO(A) = \forall w.\forall x.(w\langle !x\rangle \in dom(A) \Rightarrow (\forall v \in dom(A).v \geq w \Rightarrow (outs(v)\langle x\rangle \geq outs(w)\langle x\rangle))$$

This condition is interpreted as "if at any stage it is possible for A to output x, then the next output of A must be x".

The need for one of these additional conditions to hold in case (b) is created by the possibility of C (in $(A \gg C)$) being able to selectively input from A. When this selective input is necessary for the correct behaviour of $(A \gg C)$ the insertion of B introduces the possibility of deadlock.

e.g. Let $A \Leftarrow ?x:T \rightarrow ((!a \rightarrow !x \rightarrow A) \Box (!b \rightarrow \underline{stop}))$

$B \Leftarrow ?x:T \rightarrow !x \rightarrow B$

$C \Leftarrow ?a \rightarrow (?x:T \rightarrow !x \rightarrow C)$

(for a,b two distinct elements of T)

Then $(A \gg C)$ and B are buffers but $A \gg B \gg C$ is not as B, unlike C, cannot prevent A deadlocking.

5.25 Example

For each $n \geq 1$ define a canonical n-place buffer $B^n_{\langle\rangle}$ by mutual recursion on $M^{\wedge n}$, where $\Lambda_n = \{w \in T^* \mid |w| < n\}$.

$$B^n_{\langle\rangle} \Leftarrow ?x:T \rightarrow B^n_{\langle x\rangle}$$

$$B^n_{w\langle y\rangle} \Leftarrow (?x:T \rightarrow B^n_{\langle x\rangle w\langle y\rangle}) \Box (!y \rightarrow B^n_w) \quad \text{if } |w| < n-1,\ y \in T$$

$$B^n_{w\langle y\rangle} \Leftarrow (!y \rightarrow B^n_w) \quad \text{if } |w| = n-1,\ y \in T$$

Claim that $B^n_{\langle\rangle} = B^n$ (as previously defined).

For $x \in T$ define $B_x = !x \rightarrow B$ (for B the one place buffer).

Observe that $(B_x \gg B) = (!x \rightarrow B) \gg (?x:T \rightarrow (!x \rightarrow B))$

$= (B \gg B_x)$ (by 5.22 (i)).

Define processes C^n_w for each $n \geq 1$ and $|w| \leq n$ as follows.

$$C^n_{\langle\rangle} = B^n, \quad C^1_{\langle a\rangle} = B_a, \quad C^{n+1}_{w\langle a\rangle} = (C^n_w \gg B_a)$$

Thus C^n_w is a string of one-place buffers, with the last ones containing the elements of w, for example $C^3_{\langle ab\rangle} = B \gg B_a \gg B_b$ and $C^3_{\langle abc\rangle} = B_a \gg B_b \gg B_c$.

Claim that $\forall w.\forall n.\ C^n_w = B^n_w$ (this clearly implies the above claim that $B^n_{\langle\rangle} = B^n$). We will prove this by induction on

the definitions of the B^n_w.

For each n the predicate $R_n(\underset{\sim}{B}) \equiv \forall w \in \Lambda_n . B_w = C^n_w$ is clearly continuous and satisfiable. Also the recursion defining the B^n_w is clearly constructive. It thus suffices to show that $\forall \underset{\sim}{B}' \in M^{\Lambda_n} . R_n(\underset{\sim}{B}') \Rightarrow R_n(F_n(\underset{\sim}{B}'))$, where F_n is the function associated with the B^n_w recursion.

If n=1 then $R_1(\underset{\sim}{B}') \Rightarrow F_1(\underset{\sim}{B}')_{\langle\rangle} = ?x:T \to C^1_{\langle x\rangle}$

$= ?x:T \to B_x$ by definition of C^1_x

$= B$ by definition of B

$= C^1_{\langle\rangle}$

$F_1(\underset{\sim}{B}')_{\langle x\rangle} = !x \to C^1_{\langle\rangle}$

$= !x \to B$

$= B_x = C^1_{\langle x\rangle}$

$\Rightarrow R_1(F_1(\underset{\sim}{B}'))$

If n>2 then $R_n(\underset{\sim}{B}') \Rightarrow F_n(\underset{\sim}{B}')_{\langle\rangle} = ?x:T \to C^n_{\langle x\rangle}$

$= ?x:T \to (B^{n-1} \gg B_x)$

$= ?x:T \to (B_x \gg B^{n-1})$

(by repeated use of $(B \gg B_x) = (B_x \gg B)$)

$= (?x:T \to B_x) \gg (B^{n-1})$ (by 5.22)

$= B \gg B^{n-1} = C^n_{\langle\rangle}$

if $|w| < n-1$ then $F_n(\underset{\sim}{B}')_{w\langle y\rangle} = (?x:T \to C^n_{\langle x\rangle w\langle y\rangle}) \,\square\, (!y \to C^n_w)$

$= (?x:T \to (B_x \gg C^{n-2}_w \gg B_y)) \,\square\, (!y \to (B \gg C^{n-2}_w \gg B))$

(by repeated use of $(B \gg B_x) = (B_x \gg B)$)

$= ((?x:T \to B_x) \gg C^{n-2}_w \gg (!y \to B))$

(by 5.22 (e))

$= B \gg C^{n-2}_w \gg B_y$

$= C^n_{w\langle y\rangle}$

if $|w| = n-1$ then $F_n(\underset{\sim}{B}')_{w\langle y\rangle} = (!y \to C^n_w)$

$= !y \to (C^{n-1}_w \gg B)$

(by repeated use of $(B \gg B_x) = (B_x \gg B)$)

$= (C^{n-1}_w \gg (!y \to B))$ (it is easily shown by induction that $|v| = m \Rightarrow (C^m_v)^{\circ} \subseteq !T$)

$= C^n_{w\langle y\rangle}$

The case n=2 is almost identical with the $n > 2$ case, the only difference being in the middle case, where C_w^{n-2} is not now defined. There is of course no need for it to be present in this case (n=2) and we use 5.22 (d) instead of (e).

This completes the proof that $B_w^n = C_w^n$ for all n & w.

We have the following immediate corollaries to this result.

5.25.1 $B_{\langle\rangle}^n$ is a buffer for each $n \geq 1$.

5.25.2 $B_w^n \gg B_v^m = B_{wv}^{n+m}$ (by repeated application of $(B_x \gg B) = (B \gg B_x)$ to $C_w^n \gg C_v^m$)

We will henceforth identify the symbols $B_{\langle\rangle}^n$ and B^n as we are justified in doing by the preceding example.

Observe that in the above example we proved that the "large" process $B_{\langle\rangle}^n$ is a buffer by breaking it down into a lot of small parallel components. We will see this idea employed often from now on.

The next two results, the second of which is a type of inductive generalisation of the first, are both very useful in dealing with practical examples of proofs of correctness of buffers.

5.26 Theorem

Suppose that (for any set S) we are given two sets of processes $\{A_s \mid s \in S\}$ and $\{C_s \mid s \in S\}$ such that for all s $A_s \gg C_s$ is a buffer. Then for any function $g:T \to S$ the process $?x:T \to (A_{g(x)} \gg (!x \to C_{g(x)}))$ is a buffer.

(Note also that the above process is equal to

$$((?x:T \to !x \to A_{g(x)}) \gg (?x:T \to !x \to C_{g(x)}))$$.)

We will find that this result is a corollary to the proof of the next result.

5.27 Theorem

Suppose that for any set S we are given two sets of processes $\{A_s \mid s \in S\}$ and $\{C_s \mid s \in S\}$ and a function $g: S \times T \to S$ such that for all $s \in S$

$$(A_s \gg B_s) = ?x{:}T \to (A_{g(s,x)} \gg (!x \to C_{g(s,x)})) \ .$$

Then for all $s \in S$ $A_s \gg C_s$ is a buffer.

proof

(This is an application of 5.14.)

Define $F: \mathcal{P}(M) \to \mathcal{P}(M)$ as follows:

$$A \in F(E) \Leftrightarrow$$
$$(i) \quad A^{o} = ?T \quad \text{and} \quad A(\langle\rangle) = \{X \mid X \cap ?T = \emptyset\}$$
$$\& \ (ii) \quad \forall t \in T.\ \exists B_t \in E \text{ s.t. } \langle ?t\rangle w \in \mathrm{dom}(A) \ \& \ w \in (?T)^* \Rightarrow w \in \mathrm{dom}(B_t)$$
$$\& \ A(\langle ?t\rangle w) \subseteq \{X \mid !t \notin X\}$$
$$\langle ?t\rangle w \langle !s\rangle v \in \mathrm{dom}(A) \ \& \ w \in (?T)^* \Rightarrow s = t \ \&$$
$$\& \ A(\langle ?t\rangle w \langle !s\rangle v) \subseteq B_t(wv)$$

5.27.1 lemma

F is constructive in the sense of 5.14.

5.27.2 lemma

$(\forall B \in A.\mathrm{Buff}(B)) \Rightarrow (\forall B \in F(A).\mathrm{Buff}(B))$

5.27.3 lemma

For any $g: S \times T \to S$ and $s \in S$

$$(?x{:}T \to (A_{g(s,x)} \gg (!x \to C_{g(s,x)}))) \in F(\{A_s \gg C_s \mid s \in S\})$$

The proofs of these lemmas are just tedious analysis of cases and are omitted.

Lemma 3 above gives us that under the hypotheses of the theorem $\{A_s \gg C_s \mid s \in S\} \subseteq F(\{A_s \gg C_s \mid s \in S\})$.

Now since Buff is continuous and satisfiable 5.14 gives us the desired result that $s \in S \Rightarrow \mathrm{Buff}(A_s \gg C_s)$.

Observe that lemmas 2 & 3 above combine to prove 5.26.

The above result admits much "degeneralisation" by simplifying the form of g. For example by setting S to be a one element set we get for any $A, B \in M$:

$$A \gg B = ?x{:}T \to (A \gg (!x \to B)) \Rightarrow \mathrm{Buff}(A \gg B) \ .$$

5.28 Example

Define $A \Leftarrow ?x{:}T \to !x \to !x \to A$

$C \Leftarrow ?x{:}T \to !x \to ?x \to C$

Now
$$\begin{aligned} A \gg C &= (?x{:}T \to !x \to !x \to A) \gg (?y{:}T \to !y \to ?y \to C) \\ &= ?x{:}T \to ((!x \to !x \to A) \gg (?y{:}T \to !y \to ?y \to C)) \\ &= ?x{:}T \to ((!x \to A) \gg (!x \to ?x \to C)) \quad (*) \\ &= ?x{:}T \to !x \to ((!x \to A) \gg (?x \to C)) \\ &= ?x{:}T \to !x \to (A \gg C) \end{aligned}$$

(by many applications of 5.22)

It is thus an easy induction to show that $A \gg C = B$, the one place buffer.

For $x \in T$ define $A_x = !x \to A$ and $C_x = ?x \to C$.
Thus $A \gg C = ?x{:}T \to (A_x \gg !x \to C_x)$ (by (*) above)
and for each $y \in T$ $A_y \gg C_y = A \gg C = ?x{:}T \to (A_x \gg !x \to C_x)$.

Thus if we put $S = T \cup \{a\}$ for any $a \notin T$ and set $A_a = A$ & $C_a = C$ the $\{A_s \mid s \in S\}$ and $\{C_s \mid s \in S\}$ satisfy the conditions of 5.27 (putting $g(s,x) = x$ for all $s \in S$).

This serves as an alternative proof that $B = A \gg C$ is a buffer (though it is of course circular as we assumed that Buff was satisfiable, and the most basic instance of Buff we have seen was B, all others having been proved from it). It also shows that B, as well as all the other B^n, can be expressed in the form $A \gg C$ for some $A, C \in M$.

5.29 Example (C.A.R.H./A.W.R.)

This example models a simple method for overcoming a "gremlin" on a transmission line which occasionally randomizes information.

Define error generating processes E_i as follows ($i \in \{0,1,2,3\}$).

$$E_o \Leftarrow ?x{:}T \to \bigvee_{y \in T} (!y \to E_3), \quad E_{i+1} \Leftarrow ?x{:}T \to !x \to E_i$$

The E_i randomize every fourth bit, i determining the phasing. To counteract a line behaving like E_i we send every message in triplicate, and take a majority vote at the receiving end.

$X \Leftarrow ?x{:}T \to !x \to !x \to !x \to X$

$Y \Leftarrow ?x{:}T \to (\quad (?x \to (?y{:}T \to Y))$

$\qquad \Box\ (?y{:}T - \{x\} \to ((?x \to !x \to Y) \Box (?y \to !y \to Y))))$

To show that this device is correct we would like to show that each $X \gg E_i \gg Y$ is a buffer, so that these processes both transmit information reliably and are free of deadlock (observe that Y can deadlock if it gets no clear majority in any group of three symbols).

Putting $S = \{0,1,2,3\}$, $A_i = X \gg E_i$ and $C_i = Y$, by 5.27 it will clearly be sufficient to show that $i \in S$ implies

$$(X \gg E_i) \gg Y = ?x:T \to ((X \gg E_{i \oplus 1}) \gg (!x \to Y)),$$

where $\oplus$ represents addition modulo 4.

We can show each of these by repeated application of 5.22.

e.g. $X \gg E_0 \gg Y$ (each process satisfies P_1 so associative law is justified)

$= ?x:T \to ((!x \to !x \to !x \to X) \gg (?x:T \to (\bigvee_{y \in T} !y \to E_3)) \gg Y)$

$= ?x:T \to ((!x \to !x \to X) \gg (\bigvee_{y \in T} !y \to E_3) \gg Y)$

$= ?x:T \to (\bigvee_{y \in T} ((!x \to !x \to X) \gg E_3 \gg Y_y))$ (where $Y_y = Y$ after $?y$)

$= ?x:T \to (((!x \to X) \gg (!x \to E_2) \gg Y_x)) \text{ or } (\bigvee_{y \neq x} (!x \to X \gg !x \to E_2 \gg Y_y)))$

$= ?x:T \to (((!x \to X) \gg E_2 \gg (?y:T \to !x \to Y))$

$\text{or } (\bigvee_{y \neq x} ((!x \to X) \gg E_2 \gg ((?y \to !y \to Y) \,\square\, (?x \to !x \to Y)))))$

$= ?x:T \to ((X \gg E_1 \gg (!x \to Y)) \text{ or } (\bigvee_{y \neq x} (X \gg (!x \to E_1) \gg (***))))$

$= ?x:T \to ((X \gg E_1 \gg (!x \to Y)) \text{ or } (\bigvee_{y \neq x} (X \gg E_1 \gg (!x \to Y))))$

$= ?x:T \to (X \gg E_1 \gg (!x \to Y))$ as desired

(*** represents the same term as at that place in the previous line.)

The other cases are easier than this one.

Many other examples in this vein are possible, for example we might design processes to insert parity checks in streams, and others to check them and remove them. We would then wish to show that when we combine these processes the result is a buffer.

We now turn our attention to recursive definitions which involve "$\gg$". Since its definition involves hiding, this operator is not in general non-destructive. The next result identifies two cases where it is.

5.30 Theorem

a) If $w \in dom(C) \Rightarrow |ins(w)| \leqslant |outs(w)|$ then $(A \gg C)$ is a non-destructive function of A (if $dom(C) \subseteq (?T \cup !T)^*$).

b) If $w \in dom(C) \Rightarrow |ins(w)| \geqslant |outs(w)|$ then $(C \gg A)$ is a non-destructive function of A (if $dom(C) \subseteq (?T \cup !T)^*$).

proof

We will give a proof of (a), result (b) following by symmetry. Suppose that $w \in dom(C) = |ins(w)| \leqslant |outs(w)|$.

This condition clearly implies P_2 (of 5.20). For arbitrary A we must have $(A \gg C)$ free of infinite internal chatter, for the proof of this part of 5.20 only depends on P_2 of the second variable (just as the proof that if A & C satisfy P_1 then $A \gg C$ is chatter-free depends only on $P_1(A)$).
Hence for all A the entirety of $A \gg C$ comes from the "or" clause of 5.18.

Suppose $A \in M$. We wish to show that $(A \gg C)\lceil n = (A\lceil n \gg C)\lceil n$.
We have $(A \gg C)\lceil n \supseteq (A\lceil n \gg C)\lceil n \equiv (A \gg C)\lceil n \subseteq (A\lceil n \gg C)\lceil n$ by monotonicity. It is thus sufficient to show that if $|w| < n$ and $(w,X) \in (A\lceil n \gg C)$ then $(w,X) \in (A \gg C)$ and that if $|w| = n$ and $w \in dom(A\lceil n \gg C)$ then $w \in dom(A \gg C)$.

In the first case there must be some $(u,U) \in A\lceil n$ and $(v,V) \in C$ such that $((u,U),(v,V)) \Leftrightarrow (w,X)$ in $(A\lceil n \gg B)$.

But then $|n| > |w| = |ins(w)| + |outs(w)| = |ins(u)| + |outs(v)|$
$\geqslant |ins(u)| + |ins(v)| = |ins(u)| + |outs(u)| = |u|$.
Hence $(u,U) \in A$ so $((u,U),(v,V)) \Leftrightarrow (w,X)$ in $(A \gg C)$.

The second case follows by a very similar argument.

This completes the proof of 5.30.

5.31 Example

Consider the process defined $C \Leftarrow ?x{:}T \rightarrow (C \gg (!x \rightarrow B))$.
By the above this recursion is constructive. It is easy to show that C is a buffer by induction. We know that Buff is satisfiable and continuous, so suppose

that Buff(D) holds. Then $D \gg B$ is a buffer by 5.24 as both B and D are. Therefore $?x:T \to (D \gg (!x \to B))$ is a buffer.
Thus $Buff(D) \Rightarrow Buff(F(D))$, where F is the function of the C-recursion. Thus Buff(C) holds as claimed.

$$\begin{aligned}
\text{Now } C \gg B &= (?x:T \to (C \gg (!x \to B)) \gg B \\
&= ?x:T \to ((C \gg (!x \to B)) \gg B) \quad \text{as } B^o \subseteq ?T \\
&= ?x:T \to (C \gg ((!x \to B) \gg B)) \quad \text{(buffers are associative)} \\
&= ?x:T \to (C \gg (B \gg (!x \to B))) \quad \text{(as in 5.25)} \\
&= ?x:T \to ((C \gg B) \gg (!x \to B))
\end{aligned}$$

Hence $C \gg B$ is a fixed point of the recursive equation of C, but this equation has a unique fixed point, namely C, so $C = C \gg B$.

$$\begin{aligned}
\text{Also } C \gg C &= (?x:T \to (C \gg (!x \to B)) \gg C \\
&= ?x:T \to ((C \gg (!x \to B)) \gg C) \quad \text{as } C^o \subseteq ?T \\
&= ?x:T \to (C \gg ((!x \to B) \gg (?y:T \to (C \gg (!y \to B))))) \\
&= ?x:T \to (C \gg B \gg C \gg (!x \to B)) \\
&= ?x:T \to ((C \gg C) \gg (!x \to B)) \quad \text{by the above.}
\end{aligned}$$

Thus by the same argument as above $C \gg C = C$.

Define processes C_w $(w \in T^*)$ as follows:

$$C_{\langle\rangle} = C \qquad C_{w\langle y\rangle} = (C_w \gg (!y \to B)) \quad .$$

It is easy to show (by $(C \gg B) = C$, $(B_x \gg B) = (B \gg B_x)$ and definition of C & B) that

$$C_{\langle\rangle} = ?x:T \to C_x$$

$$C_{w\langle y\rangle} = (?x:T \to C_{\langle x\rangle w\langle y\rangle}) \,\square\, (!y \to C_w)$$

It is then an easy induction to show that $C = B^\infty$, where B^∞ is the canonical infinite buffer $B^\infty_{\langle\rangle}$, where

$$B^\infty_{\langle\rangle} \Leftarrow ?x:T \to B^\infty_{\langle x\rangle}$$

$$B^\infty_{w\langle y\rangle} \Leftarrow (?x:T \to B^\infty_{\langle x\rangle w\langle y\rangle}) \,\square\, (!y \to B^\infty_w) \quad .$$

Note that as corollaries to the above proof that B^∞ is a buffer, we have the following identities:

$$B^\infty \gg B^n = B^\infty, \quad B^\infty_w \gg B^n_v = B^\infty_{wv}, \quad B^\infty \gg B^\infty = B^\infty, \quad B^\infty_w \gg B^\infty_v = B^\infty_{wv} \quad .$$

The only obvious omissions from this list are
$B^n \gg B^\infty = B^\infty$ and $B^n_w \gg B^\infty_v = B^\infty_{wv}$.

These two results are both easily proved from $B \gg B^\infty = B^\infty$, which is easily proved by defining $B^*_w = B \gg B^\infty_w$ (for $w \in T^*$) and showing that these B^*_w satisfy the recursive equations of the B^∞_w, so the two systems are the same as these equations are certainly constructive.

In cases where a recursion does not satisfy the conditions of 5.30 the analysis is a little harder. One trick is to show that any fixed point of an equation must be deterministic, for then the equation has a unique fixed point as otherwise it could not have a minimal one. We can then prove predicates which are equalities by the satisfaction of equations with unique fixed points (as was done in 5.31) but we cannot directly prove predicates like Buff.

5.32 Example

Define a process $C^* \Leftarrow ?x:T \to (C^* \gg (!x \to C^*))$.
This recursion is not constructive in our usual sense so it has to be treated with some care.

Suppose that D is any fixed point of this equation. It is quite easy to show, using induction on $|w|$ and 5.18, that all elements of dom(D) satisfy $|ins(w)| \geq |outs(w)|$ and that D is free of infinite chatter. Assuming this result we are justified in using the assocative law on D and its derivatives. Claim that for each $n > 0$ we have

$$D^n = ?x:T \to (D^{2n-1} \gg (!x \to D)) \quad (\text{where } D^m = \overbrace{D \gg D \gg \ldots \gg D}^{(m \text{ terms})})$$

This is true for n=1 as D is a fixed point of the C* equation.

Assume true for n.

$$\begin{aligned}
\text{Then } D^{n+1} &= (?x:T \to (D \gg (!x \to D)) \gg D^n \\
&= ?x:T \to (D \gg (!x \to D) \gg D^n) \quad \text{as } (D^n)^o \subseteq ?T \\
&= ?x:T \to (D \gg (!x \to D) \gg (?y:T \to (D^{2n-1} \gg (!y \to D)))) \\
&= ?x:T \to (D \gg D \gg D^{2n-1} \gg (!x \to D)) \\
&= ?x:T \to (D^{2n+1} \gg (!x \to D)) \quad \text{as desired}
\end{aligned}$$

Hence it is true for all n by induction.

We also have $(!x \to D) \gg D = (!x \to D) \gg (?x{:}T \to (D \gg (!x \to D)))$
$= D \gg D \gg (!x - D)$

Using these two results and 5.22 we have that each process of the form D^n or $D^n \gg (!x \to D) \gg \ldots \gg (!z \to D)$ can either be written in the form $?x{:}T \to A(x)$, where each $A(x)$ is of the same form, or in the form $(?x{:}T \to A(x)) \Box (!y - A')$ where $A(x)$ and A' all have the same form.

Thus define (for $E \in \wp(M)$) $F(E) =$
$\{?x{:}T \to A(x),\ (?x{:}T \to A(x)) \Box (!y \to A') \mid y \in T,\ A(x) \in E,\ A' \in E\}$

This function is easily seen to be constructive in the sense of 5.14. It also preserves the (satisfiable and continuous) predicate "is deterministic".

Setting $E = \{D^n,\ D^n(!x \to D) \ldots (!z \to D) \mid n \in N^+,\ x, \ldots, z \in T\}$ the above shows that $E \subseteq F(E)$. Thus by rule 5.14 we are entitled to deduce that each element of E (and in particular D) is deterministic.

As T is finite hiding is continuous and thus so is H, the function of the C*-recursion.
Thus fix(H) (which we now know to be its unique fixpoint) is equal to $\bigsqcup_{n=1}^{\infty} (H^n(CHAOS))$
Claim that $\forall m. \forall n. H^n(CHAOS) \sqsubseteq C^{*m}$. Prove this by induction on n. It is certainly true for n=0, as CHAOS is the minimal element of M.
Suppose true for n.
Then $C^{*m} = ?x{:}T \to ((C^*)^{2m-1} \gg (!x \to C^*))$ (as on the last page)
$\sqsupseteq ?x{:}T \to (H^n(CHAOS) \gg (!x \to H^n(CHAOS)))$ by induction
$\sqsupseteq H^{n+1}(CHAOS)$ by definition of H

Hence by induction the result holds for all n & m.
But then for each m we have $(C^*)^m \sqsupseteq \bigsqcup_{n=1}^{\infty} (H^n(CHAOS)) = C^*$
and we know that C* is maximal in M as it is deterministic, which gives us the relation $(C^*)^m = C^*$ for all m.

One consequence of this is that C* is a buffer, for we then have $C^* \gg C^* = ?x{:}T \to (C^* \gg (!x \to C^*))$ and $(C^* \gg C^*) \gg C^* = ?x{:}T \to ((C^* \gg C^*) \gg (!x \to C^*))$, which respectively imply $C^* \gg C^*$ and $(C^* \gg C^*) \gg C^*$ are buffers by 2.27. Thus C* is a buffer by 5.23.

If we now define processes C'_w ($w \in T$) corresponding to the C_w of 5.31 we can show that $C^* = B^\infty$ in very much the same way. Let $C'_{\langle\rangle} = C^*$ and $C'_{w\langle y\rangle} = C'_w \gg (!y \to C^*)$. Then as $C^* \gg C^* = C^*$ and $(!x \to C^*) \gg C^* = C^* \gg C^* \gg (!x \to C^*) = C^* \gg (!x \to C^*)$ we can easily show that the C'_w satisfy the recursive equations of B^∞_w, that is

$$C'_{\langle\rangle} = ?x{:}T \to C'_x$$
$$C'_{w\langle y\rangle} = (?x{:}T \to C'_{\langle x\rangle w\langle y\rangle}) \,\Box\, (!y \to C'_w) \quad .$$

and so the two systems must be equal, as in the last example. Hence everything that is true of B^∞ is also true of C^*.

All the buffers we have happened to meet so far have been deterministic (even the "gremlins" example 5.29, where the explicit non-determinism of the definition disappears from the point of view of the external environment). This is certainly not true in general, however. In fact it is easy to show from the definition of Buff (5.16) that if B_1 and B_2 are buffers then so is B_1 or B_2 (and there are certainly more than one buffer). Indeed this result extends to infinite disjunctions and so, for example, the process $\bigvee_{n=1}^{\infty}(B^n)$ is a buffer. (It is a process because T is finite.) It is easy to show that "$\gg$" is a distributive operator in the limited sense that if $(\bigvee_{i=1}^{\infty}(A_i)) \gg B$ is free of infinite chatter then it is equal to the process $\bigvee_{i=1}^{\infty}(A_i \gg B)$. (This comes from the nature of the "or" clause of 5.18.) There is of course a corresponding result for the second variable.

Let $B^* = \bigvee_{n=1}^{\infty}(B^n)$. Clearly $B^* \gg (!x \to B)$ is free of infinite chatter as B^* is a buffer, so we are entitled to use the above law in this case.

Hence
$$?x{:}T \to (B^* \gg (!x \to B)) = \bigvee_{n=1}^{\infty}(?x{:}T \to (B^n \gg (!x \to B)))$$
$$= \bigvee_{n=1}^{\infty}(?x{:}T \to B^{n+1}_{\langle x\rangle}) \quad \text{(by 5.25)}$$
$$= \bigvee_{n=1}^{\infty}(B^{n+1})$$

This proves that $B^* \sqsubseteq F(B^*)$, where F is the recursive equation of C ($= B^\infty$). It is easy then to show that F must have some fixed point above B^*. Thus by the unique fixed point property of F we have $B^\infty \sqsupseteq \bigvee_{n=1}^{\infty}(B^n)$ (the canonical infinite buffer is stronger than the disjunction of all the finite ones).

Postscript: the expressive power of "$\gg$"

To round of our study of buffers and their relationship with the pipe operator we ask the question "are all buffers expressible as $A \gg C$ for some $A,C \in M$?". All the buffers we have met so far with the exception of B* have either been directly expressed in this form or later shown to be so expressible. In fact B* can be expressed in this form by a combination of 5.28 and the distributivity principle of the last page ($B^* = ((A \text{ or } (\bigvee_{n=1}^{\infty}(B^n \gg A))) \gg C$), where A & C are as in 2.28).

In fact there are (unfortunately?) certain pathological buffers which cannot be so expressed.

5.33 Example

Let $A \Leftarrow ?x:T \rightarrow (!x \rightarrow B$

$\quad \Box ?y:T \rightarrow (?z:T \rightarrow (!x \rightarrow !y \rightarrow !z \rightarrow B)$

$\quad\quad \Box !x \rightarrow !y \rightarrow B) \quad)$

Then A is a buffer not expressible as $A_1 \gg A_2$ for $A_1, A_2 \in M$. The fact that A is a buffer can be proved easily from the fact that B is a buffer.

The main reason for A not being expressible as $(A_1 \gg A_2)$ is that when it contains two items it will deterministically accept another, but on outputting its first symbol it immediately loses the ability to output. The point is that if $A = A_1 \gg A_2$ then it must be A_1 doing the inputting and A_2 doing the outputting. The only way that A_1 can lose the ability to input is by a signal passing between A_1 and A_2 after A_2 has output. This however leaves the possibility that A_1 might accept an input before this signal has been executed but after A_2's output.

A formal proof that A is not so expressible will follow easily from the next result.

5.34 Theorem

If A is a buffer expressible as $A_1 \gg A_2$ then A satisfies

$$w\langle !a\rangle \in \mathrm{dom}(A) \Rightarrow \{?x \mid w\langle !a?x\rangle \notin \mathrm{dom}(A)\} \in A(w)$$

(A can refuse before it outputs "a" the whole of what it must refuse after outputting "a".)

proof

Suppose that $w\langle !a\rangle \notin \mathrm{dom}(A)$ and that A is so expressible.

$A = (A_1 \gg A_2)$ must be free of infinite internal chatter as it is a buffer. Thus only the "or" clause of 5.18 applies. Hence $(w,\emptyset)$ must have some derivation $((u,U),(v,V))$ in $(A_1 \gg A_2)$.

Let $X = \{?x \mid w\langle !a?x\rangle \notin dom(A)\}$.
Suppose $?x \in X$ and $u\langle ?x\rangle \in dom(A_1)$.

Now $v\langle !a\rangle \in dom(A_2)$ or else $((u,U),(v,V \cup \{!a\}))$ would be a derivation in $(A_1 \gg A_2)$ of $(w,\{!a\})$, which would contradict the fact that A is a buffer (lines (i) & (iii) of 5.16).
Thus $t\langle !a?x\rangle \in dom(strip!(A_1)_{T \cup ?T} \|_{T \cup !T} strip?(A_2))$ where t corresponds with u & v in the sense of 5.18.
Hence $(t\langle !a?x\rangle) \restriction (?T \cup !T) = w\langle !a?x\rangle \in dom(A_1 \gg A_2)$, which contradicts the fact that $u\langle ?x\rangle \in dom(A_1)$.

Hence $X \cap (A_1 \text{ after } u)^o = \emptyset$, so $((u,U \cup X),(v,V))$ is a derivation for (w,X) in $(A_1 \gg A_2)$, which gives us the desired result.

The author conjectures that the condition on the last page is also sufficient to ensure expressiblity of buffers, but at the time of writing has not had time to prove or disprove this.

This concludes our detailed study of buffers. Note that in the next chapter there is a different method given of defining B^∞ (in terms of the master/slave) operator.

Appendix: Proof of the lemma needed in 5.19

5.35 Lemma

If A is free of infinite X-chatter and $X \cap Z = \emptyset$ then $(A/X_Y\|_Z B) = (A_{X\cup Y}\|_Z B)/X$.

proof

Use the notation $s_X\|_Y t \to w$ to mean (for $X,Y \subseteq \Sigma$ and $s,t,w \in \Sigma^*$) that $w\restriction X = s$, $w\restriction Y = t$ and $w \in (X\cup Y)^*$.

It is easy to check that (for any A,B,X,Y)

$$(w,W) \in (A_X\|_Y B) \Leftrightarrow \exists (s,S) \in A,\ (t,T) \in B \text{ s.t. } s_X\|_Y t \to w \ \&\ W\cap(X\cup Y) \subseteq (X\cap S)\cup(Y\cap T) \quad . \qquad (*)$$

It is also easy to verify that $X \cap Z = \emptyset$ implies

$$s_{X\cup Y}\|_Z t \to w \Rightarrow (s/X)_Y\|_Z t \to (w/X)$$

We will show first that under the stated conditions

$$(A/X_Y\|_Z B) \subseteq (A_{X\cup Y}\|_Z B)/X \ .$$

Suppose $(w,W) \in (A/X_Y\|_Z B)$, then by (*) above, and since A is free of infinite X-chatter, there exist s,t,S,T such that $(s,S\cup X) \in A$, $(t,T) \in B$, $(s/X)_Y\|_Z t \to w$

$$\&\ W\cap(Y\cup Z) \subseteq (S\cap Y)\cup(T\cap Z) \ . \qquad (**)$$

It is easy to see that since $X \cap Z = \emptyset$ and $(s/X)_Y\|_Z t \to w$ there exists some w* such that $s_{X\cup Y}\|_Z t \to w^*$ and $w^*/X = w$. (For example such a w* is obtained by placing each maximal substring of X-symbols occurring in s in w at the leftmost place at which the number of Y-X symbols is the same as at the place the substring occurs in s. If $X = \{x\}$, $Y = \{y\}$ and $Z = \{z\}$, $s = \langle xyxxyy\rangle$, $t = \langle zzz\rangle$ and $w = \langle yzyzyz\rangle$ then in this case w* would be $\langle xyxxzyzyz\rangle$.)

Now we have $(s,S\cup X) \in S$, $(t,T) \in B$ and $(W\cup X)\cap(X\cup Y\cup Z) \subseteq ((S\cup X)\cap(Y\cup X))\cup(T\cap Z)$. (The set relation is obtained by taking the union of each side of (**) with X.)

Hence $(w^*,W\cup X) \in (A_{X\cup Y}\|_Z B)$. (By (*))

This implies $(w^*/X,W) \in (A_{X\cup Y}\|_Z B)/X$ by definition of "/X".

Since $w = w^*/X$ this just says $(w,W) \in (A_{X\cup Y}\|_Z B)/X$, which is what we wanted to prove.

This completes the proof that $(A/X_Y\|_Z B) \subseteq (A_{X\cup Y}\|_Z B)/X$.

To prove that $(A_{X\cup Y}\|_Z B)/X \subseteq (A/X_Y\|_Z B)$ the first step is to show that $(A_{X\cup Y}\|_Z B)$ is free of infinite X-chatter because A is. If this were not so there would be an infinite sequence $w_o < w_1 < \ldots < w_i < \ldots$ of elements of $\mathrm{dom}(A_{X\cup Y}\|_Z B)$ such that $w_i\restriction X = w_o\restriction X$ for all i. But then $w_i\restriction X\cup Y \in \mathrm{dom}A$ for all i, and

$$\begin{aligned}(w_i\restriction X\cup Y)/X &= (w_i/X)\restriction X\cup Y\\ &= (w_o/X)\restriction X\cup Y\\ &= (w_o\restriction X\cup Y)/X\end{aligned}$$

Also it is easily seen that $w_{i+1}\restriction X\cup Y > w_i\restriction X\cup Y$, since the difference between w_i and w_{i+1} occurs in X and is so preserved by restriction to $X\cup Y$.

This contradicts the fact that A is free of infinite X-chatter, so we can conclude that $(A_{X\cup Y}\|_Z B)$ is indeed free of infinite X-chatter.

Now suppose that $(w,W) \in (A_{X\cup Y}\|_Z B)/X$. By the above there is some w* such that $w^*/X = w$ and $(w^*, W\cup X) \in (A_{X\cup Y}\|_Z B)$.

Thus there are some $(s,S) \in A$ and $(t,T) \in B$ such that $s_{X\cup Y}\|_Z t \to w^*$ and $(W\cup X)\cap(X\cup Y\cup Z) \subseteq ((X\cup Y)\cap S)\cup(Z\cap T)$.

Since $X\cap Z = \emptyset$ we see that $X \subseteq S$ (i.e. $S\cup X = S$) and also

$$W\cap(Y\cup Z) \subseteq (Y\cap S)\cup(Z\cap T) \quad . \qquad (+)$$

Now $s_{X\cup Y}\|_Z t \to w^* \;\&\; X\cap Z = \emptyset$

$\Rightarrow s/X_Y\|_Z t \to (w^*/X)$ (by our earlier remark) (++)

Putting these facts together we obtain

$(s/X,S) \in A/X$ (as $S\cup X = S$)

$(t,T) \in B$

$\Rightarrow (w^*/X,W) \in (A/X_Y\|_Z B)$ (by (+) & (++))

This tells us $(w,W) \in (A/X_Y\|_Z B)$, which completes the proof that $(A_{X\cup Y}\|_Z B)/X \subseteq (A/X_Y\|_Z B)$.

This completes the proof of lemma 5.35.

We will see that this lemma is important in several proofs of the well-definedness of parallel/hiding combinators. The reasons why it does not hold in general (i.e. without the assumption of freedom from infinite chatter) will be discussed in chapter 8.