LFCS

Laboratory for Foundations of Computer Science
Department of Computer Science - University of Edinburgh

A Complete Axiomatisation for Observational Congruence of Finite-state Behaviours

by

Robin Milner

LFCS Report Series ECS-LFCS-86-8

August 1986

LFCS
Department of Computer Science
University of Edinburgh
The King's Buildings
Edinburgh EH9 3JZ

A COMPLETE AXIOMATISATION FOR OBSERVATIONAL CONGRUENCE OF FINITE-STATE BEHAVIOURS

ROBIN MILNER

UNIVERSITY OF EDINBURGH

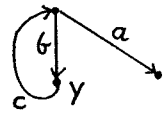
DECEMBER 1985

1. Behaviours and bisimulation

We are concerned in this paper with finite-state behaviours presented as expressions, in which variables from a denumerable set Var = {X,Y,...} may appear either free or bound, and in which atomic actions are represented by members of Act = {a,b,...}. An example is

$$\mu X(a0 + b(cX + Y))$$

Here, μ stands for recursion (binding the variable X), 0 is the empty behaviour capable of no action whatever, and the free variable Y may be understood as a place-holder, designating a place at which further behaviour may be determined by the substitution of a behaviour expression for Y. In a previous paper [Mil2] such behaviour expressions were formally represented also by transition diagrams, called charts; for the above expression the chart would be



In [Mil2] the expression-forming operators (action-prefixing, summation and recursion) were interpreted precisely as operations upon charts, but here we shall concentrate upon expressions and use charts only for illustration.

Definition The class of behaviour expressions $\mathcal{E}$ is defined by the following syntax; we shall use E,F,... as metavariables over $\mathcal{E}$.

E ::=	0	(inaction)
	X	(variable, X∈Var)
	aE	(action, a∈Act)
	μXE	(recursion, X∈Var)
	E+E	(summation)

□

Parenthesis will be used for grouping, but otherwise summation has weakest binding power, so that aμXbX + b0 is the same expression as (a(μX(bX))) + b0. We shall use fv(E) to stand for the set of variables occurring free (i.e. not bound by μ) in E. We shall also take the liberty of identifying expressions which differ only by a change of bound variables; this can be justified by a proof (which we omit) that they have the same interpretation. We shall write $E\{F_1,...,F_n/X_1,...,X_n\}$ for the result of simultaneously substituting ($1 \leq i \leq n$) F_i for each free occurrence of X_i in E, renaming bound variables as necessary.

There are several ways of interpreting behaviour expressions. In classical automata theory an expression is interpreted as a set of (finite or infinite) strings over Act. A second interpretation of an expression, adopted for example by Hennessy [Hen], is as an acceptance tree; this model is also close to that of Hoare et al [BHR]. Here we shall follow [Mil2] and define a congruence relation over expressions, and then an expression stands for its congruence class; the congruence is based upon the treatment of $(\mathcal{E},\rightarrow)$ as a labelled transition system [Kel], where the transition relation $\rightarrow$ is defined as follows:

Definition The transition relation $\rightarrow \subseteq \mathcal{E} \times ACT \times \mathcal{E}$ is the smallest relation satisfying the following conditions, in which (as also later) we write $E \xrightarrow{a} E'$ to mean $(E,a,E') \in \rightarrow$:

(i) $aE \xrightarrow{a} E$

(ii) If $E_1 \xrightarrow{a} E'$ or $E_2 \xrightarrow{a} E'$ then $E_1+E_2 \xrightarrow{a} E'$

(iii) If $E\{\mu XE/X\} \xrightarrow{a} E'$ then $\mu XE \xrightarrow{a} E'$

□

We also need to take account of the free variables occurring in an expression.

Definition A free occurrence of X in E is guarded in E if it occurs within some subexpression aF of E, otherwise it is unguarded in E. If E contains a free unguarded occurrence of X, we write $E \triangleright X$. □

Intuitively, an unguarded occurrence of X in E allows the first action of F to be also a first action of $E\{F/X\}$.

We now define the important notion, from Park [Par], of a bisimulation.

Definition A relation $\mathcal{S} \subseteq \mathcal{E} \times \mathcal{E}$ is a bisimulation if, whenever $(E,F) \in \mathcal{S}$,

(i) If $E \xrightarrow{a} E'$ then, for some F', $F \xrightarrow{a} F'$ and $(E',F') \in \mathcal{S}$

(ii) If $F \xrightarrow{a} F'$ then, for some E', $E \xrightarrow{a} E'$ and $(E',F') \in \mathcal{S}$

(iii) $E \triangleright X$ iff $F \triangleright X$.

If $(E,F) \in \mathcal{S}$ for some bisimulation $\mathcal{S}$, then we say E is congruent to F, and write $E \sim F$. □

For the theory of bisimulation and congruence we refer to [Mil3]; in

particular, we recall that congruence is an equivalence relation and moreover if $F_1 \sim F_2$ then $E\{F_1/X\} \sim E\{F_2/X\}$, i.e. congruence is substitutive. Actually the presence of clause (iii) in the above definition is newly introduced here to take account of expressions with free variables; in [Mil3] congruence was only defined for closed expressions. It is easy to show that $E_1 \sim E_2$ iff, for all (or: for all closed) expressions F, $E_1\{F/X\} \sim E_2\{F/X\}$.

The main result of [Mil2] is a complete equational axiomatisation of congruence; that is, the equation E=

F is deducible from the axiom system iff E~F. Here, we wish to extend this axiom system to deal with a weaker (i.e. larger) congruence relation.

The weaker congruence rests upon the introduction of a special "silent" action $\tau \notin Act$; we shall let u,v,... range over $Act_\tau = Act \cup \{\tau\}$, while a,b,... continue to range over act. Thus $\mathcal{E}$ is extended to $\mathcal{E}_\tau$, by allowing expressions of the form τE. Note that an unguarded occurrence of X in an expression E may still lie within a subexpression τF of E; thus, for example, X occurs unguarded in $\tau(X+a0)$. We extend the transition relation $\rightarrow$ to $\mathcal{E}_\tau$ as follows:

Definition The transition relation $\rightarrow \subseteq \mathcal{E}_\tau \times Act \times \mathcal{E}_\tau$ is the smallest relation such that

(i) $uE \xrightarrow{u} E$

(ii) If $E_1 \xrightarrow{u} E'$ or $E_2 \xrightarrow{u} E'$ then $E_1 + E_2 \xrightarrow{u} E'$

(iii) If $E\{\mu XE/X\} \xrightarrow{u} E'$ then $\mu XE \xrightarrow{u} E'$.

□

Now we wish to weaken the notion of bisimulation to allow that silent actions τ may occur in one behaviour without being matched in the other. To this end we first extend $\rightarrow$ to a relation involving strings $S \in Act_\tau^*$:

Definition $E \xRightarrow{s} E'$, for any $s \in Act_\tau^*$, if $s = u_1 \ldots u_n$ $(n \geq 0)$ and $E \xrightarrow{\tau}{}^* \xrightarrow{u_1} \xrightarrow{\tau}{}^* \ldots \xrightarrow{u_n} \xrightarrow{\tau}{}^* E'$. □

Note in particular that $E \xRightarrow{\varepsilon} E$, where ε is the empty string. If $s \in Act_\tau^*$, then $\hat{s} \in Act^*$ denotes the result of deleting all occurrences of τ from s; in particular, $\hat{\tau} = \varepsilon$.

Definition A relation $\mathcal{R} \subseteq \mathcal{E}_\tau \times \mathcal{E}_\tau$ is a weak bisimulation if whenever $(E,F) \in \mathcal{R}$,

(i) If $E \xrightarrow{u} E'$ then, for some F', $F \overset{\hat{u}}{\Longrightarrow} F'$ and $(E',F') \in \mathcal{R}$

(ii) If $F \xrightarrow{u} F'$ then, for some E', $E \overset{\hat{u}}{\Longrightarrow} E'$ and $(E',F') \in \mathcal{R}$

(iii) $E \rhd X$ iff $F \rhd X$.

If $(E,F) \in \mathcal{R}$ for some weak bisimulation $\mathcal{R}$, then we say that E is weakly (or observationally) equivalent to F, and write $E \approx F$. □

We refer to [Mil4] for the theory of observational equivalence. In particular, we recall that it is indeed an equivalence relation, but that (unlike $\sim$) it is not substitutive. For example, we can easily see that $E \approx \tau E$, in particular $a0 \approx \tau a0$, but it is not the case that $a0 + b0 \approx \tau a0 + b0$. The intuition is that the right-hand behaviour has the capability (via τ-action) of denying the possibility of b-action, while the left-hand behaviour has no such capability. Thus $\approx$ is not a congruence (not substitutive). We therefore define a new relation $\approx^c$, weak (or observational) congruence, as follows:

Definition $E \approx^c F$ iff, for all $G \in \mathcal{E}_\tau$, $E+G \approx F+G$ □

It is easily proved, following [Mil4], that weak congruence is indeed a congruence (i.e. substitutive), and that it is the largest congruence relation over $\mathcal{E}_\tau$ included in $\approx$. Moreover, it has the following characterisation which will be important for the present paper:

Proposition 1.1 $E \approx^c F$ iff

(i) If $E \xrightarrow{u} E'$ then, for some F', $F \overset{\hat{u}}{\Longrightarrow} F'$ and $E' \approx F'$

(ii) If $F \xrightarrow{u} F'$ then, for some E', $E \overset{\hat{u}}{\Longrightarrow} E'$ and $E' \approx F'$

(iii) $E \rhd X$ iff $F \rhd X$.

□

This proposition shows that $\approx^c$ is stronger than $\approx$ in only one respect; an initial τ-action of one behaviour must be matched by at least one τ-action of the other (while for $\approx$ it may be matched by the absence of any action).

2. Axiomatisation

In the previous section we recalled the result of [Mil2], that a certain set of axioms is both sound and complete for the congruence relation $\sim$. On the other hand, in [Mil1] various equational laws were proved to hold for the observational congruence relation $\approx^c$, and a set of such laws were shown in [HM] to be complete for behaviours without recursion; although the definition of $\approx^c$ has here been extended by clause (iii) to allow for the presence of free variables, those laws remain sound. We now present an axiomatisation which will be proved complete for $\approx^c$ in the presence of recursion. The proof occupies all later sections of the paper; in this section we confine ourselves to a discussion of the axioms. The axiomatisation follows; we omit the usual rules for reflexivity, symmetry and substitutivity of equality and for change of bound variables.

The axiom system $\mathcal{A}_\tau$

Summation axioms

S1: $E+F=F+E$

S2: $E+(F+G)=(E+F)+G$

S3: $E+E=E$

S4: $E+0=E$

τ-axioms

T1: $u\tau E=uE$

T2: $E+\tau E=\tau E$

T3: $u(E+\tau F)+uF=u(E+\tau F)$

Recursion axioms

R1: $\mu XE = E\{\mu XE/X\}$

R2: If $F=E\{F/X\}$ then $F=\mu XE$, provided X is guarded in E

R3: $\mu X(X+E) = \mu XE$

R4: $\mu X(\tau X+E) = \mu X\tau E$

R5: $\mu X(\tau(X+E)+F) = \mu X(\tau X+E+F)$

We shall write $\mathcal{A}_\tau \vdash E=F$, or just $\vdash E=F$, when $E=F$ may be proved from $\mathcal{A}_\tau$. Several subsets of $\mathcal{A}_\tau$ are interesting:

1. $\mathcal{A}^f$, consisting of S1-S4, is sound and complete for congruence ($\sim$) over the recursion-free subset of $\mathcal{E}$ [HM].

2. $\mathcal{A}^f_\tau$, consisting of $\mathcal{A}^f$ together with T1-T3, is sound and complete for observation congruence ($\approx^c$) over the recursion free subset of $\mathcal{E}_\tau$ [HM].

3. $\mathcal{A}$, consisting of $\mathcal{A}^f$ together with R1-R3, is sound and complete

for congruence ($\sim$) over $\mathcal{E}$ [Mil2].

4. $\mathcal{A}_\tau^g$ consisting of $\mathcal{A}_\tau^f$ together with R1 and R2, will be shown sound and complete for $\approx^c$ over $\mathcal{E}_\tau^g$, the subset of $\mathcal{E}_\tau$ in which, for every recursion μXE, X is guarded in E. We call the members of $\mathcal{E}_\tau^g$ guarded expressions.

5. $\mathcal{A}_\tau$, the full axiom system, will be shown sound and complete for $\approx^c$ over $\mathcal{E}_\tau$.

We begin by stating, without proof, that $\mathcal{A}_\tau$ is indeed sound. The proof is not hard, involving for each axiom the construction of an appropriate weak bisimulation, and we prefer to concentrate here upon the much more challenging proof of completeness.

Proposition 2.1 (Soundness). If $\mathcal{A}_\tau \vdash E=F$ then $E \approx^c F$. □

We shall now outline the structure of the completeness proof, and attempt to indicate its main difficulties.

First, we consider the proof that $\mathcal{A}_\tau^g$ is complete for $\approx^c$ over $\mathcal{E}_\tau^g$. This proof follows the lines of [Mil2] where $\mathcal{A}$ is proved complete for $\sim$ over $\mathcal{E}$. The crucial theorem (Theorem 3.2) shows that if $E \approx^c F$ and E provably satisfies a certain kind of equation set, while F provably satisfies another such equation set, then both E and F provably satisfy a single equation set. This refines Theorem 5.10 of [Mil2] showing the completeness of $\mathcal{A}$; a subtler approach is needed due to τ. The completeness result (Theorem 4.3) requires two further theorems; Theorem 4.1 states that every guarded expression satisfies an appropriate equation set, while Theorem 4.2 states that whenever two guarded expressions satisfy the same appropriate equation set then they may be proved equal in $\mathcal{A}_\tau^g$.

The principal difficulty in proving completeness of $\mathcal{A}_\tau$ over $\mathcal{E}_\tau$ has been to find axioms which are sufficient to prove every expression in $\mathcal{E}_\tau$ equal to a guarded expression; this is clearly all that is needed to reduce the full completeness problem to the completeness of $\mathcal{A}_\tau^g$ over $\mathcal{E}_\tau^g$. In a sense, the problem was solved by J. Bergstra and J. Klop [BK], though they relied upon the introduction of certain additional operators to the language of expressions, and their axiom system was uncomfortably large. Interestingly, their method was in strong contrast to that adopted here; instead of transforming every expression to a guarded one - which may be seen as

removing all τ-loops from recursions - they introduced τ-actions wherever possible (while preserving $\approx^c$) and thereby reduced the problem to the completeness of $\mathcal{A}$ for congruence ($\sim$) over $\mathcal{E}_\tau$. Nevertheless, the present approach was inspired by a reading of their perceptive work, for which I am strongly indebted to them.

Thus, Section 5 is mainly devoted to a proof that, with the help of the axiom R3-R5, every expression may be proved equal to a guarded one (Theorem 5.2). Note that axiom R3 was already present in $\mathcal{A}$, which is complete for congruence ($\sim$) over $\mathcal{E}$, but R4 and R5 are new and - though simple - have taken a long time to discover.

3. Transforming sets of equations

In this section we shall present the crucial part of our proof of completeness. Roughly speaking, we show that if two expressions E and F are semantically equal, $E \approx^c F$, and if E has been proved to satisfy a given set of equations and F another set, then an equation set may be constructed from the two given sets such that it is provably satisfied by both E and F.

Let $\tilde{X} = \{X_1,\ldots,X_m\}$ and $\tilde{W} = \{W_1,W_2,\ldots\}$ be disjoint sets of variables. Let $\tilde{H} = \{H_1,\ldots,H_m\}$ be expressions with free variables in $\tilde{X} \cup \tilde{W}$; then we shall call the set S of formal equations

$$S : \tilde{X} = \tilde{H}$$

standard if each H_i takes the form $\sum_j u_{ij} X_{f(i,j)} + \sum_k W_{g(i,k)}$. We also define the relations $\rightarrow_S \subseteq \tilde{X} \times Act_\tau \times \tilde{X}$ and $\rhd_S \subseteq \tilde{X} \times \tilde{W}$ as follows:

$$X_i \xrightarrow{u}_S X \quad \text{iff} \quad uX \text{ occurs in } H_i$$

$$X_i \rhd_S W \quad \text{iff} \quad W \text{ occurs in } H_i$$

(we shall usually omit the subscript S in these relations, when the context can supply it). We shall call S guarded if there is no cycle $X_i \xrightarrow{\tau}{}^+ X_i$. Furthermore, we shall call S saturated if, for all $X \in \tilde{X}$,

(i) $X \xrightarrow{\tau}{}^* \xrightarrow{u} \xrightarrow{\tau}{}^* X'$ implies $X \xrightarrow{u} X'$

(ii) $X \xrightarrow{\tau}{}^* \rhd W$ implies $X \rhd W$

We say that E provably satisfies S if there are expressions $\tilde{E} = \{E_1,\ldots,E_m\}$, with $E_1 \equiv E$ and $fv(\tilde{E}) \subseteq \tilde{W}$, such that

$$\mathcal{A}_\tau \vdash \tilde{E} = \tilde{H}\{\tilde{E}/\tilde{X}\}$$

We can now state more precisely the role played by this Section in the completeness proof. In a later section we shall show that every E provably satisfies a standard guarded equation set

$$S : \tilde{X} = \tilde{H}$$

Here we show that if $E \approx^c F$, where F provably satisfies another such equation set

$$T : \tilde{Y} = \tilde{J}$$

then there is a third such equation set

$$U : \tilde{Z} = \tilde{K}$$

provably satisfied by both E and F. The final stage, in Section 4, is to show

that whenever E and F provably satisfy the same standard guarded equation set, then $\vdash E=F$. Note that in both this and the next section we are working in $\mathcal{M}_\tau^g$, i.e. without axioms R3-R5.

Lemma 3.1 Let E provably satisfy S, standard and guarded. Then there is a saturated, standard and guarded equation set S' provably satisfied by E.

Proof S' may be obtained from S by adding further terms to the right-hand side of each equation, using the τ-laws (T1)-(T3). It is sufficient to show how this is done by an example. Suppose S is as follows:

$$X_1 = \tau X_2$$
$$X_2 = aX_3 + bX_1 + W$$
$$X_3 = \tau X_2$$

Then we have $\vdash E_1 = \tau E_2$, and so

$$\vdash E_1 = \tau(a(\tau E_2) + bE_1 + W)$$

which, using the τ-laws, yields

$$\vdash E_1 = \tau E_2 + aE_3 + aE_2 + bE_1 + bE_2 + W$$

and the first (saturated) equation of S' is taken to be

$$X_1 = \tau X_2 + aX_3 + aX_2 + bX_1 + bX_2 + W$$

The remaining equations of S' are obtained similarly, and it is clear that no τ-cycles are introduced by the process. □

To help understanding of the theorem to follow, we first illustrate its construction by a simple example. Suppose that $E_1 \approx^c F_1$, and that E_1 provably satisfies S and F_1 provably satisfies T, where the standard guarded equation sets S and T are as follows:

S : $X_1 = bX_2$
$X_2 = aX_3 + \tau X_4$
$X_3 = aX_3$
$X_4 = aX_4$

T : $Y_1 = bY_2$
$Y_2 = aY_2$

Note that if $E_1,\ldots,E_4$ provably satisfy S, and F_1,F_2 provably satisfy T, then $E_1 \approx^c F_1 \approx^c b(\mu ZaZ)$.

The first step is to saturate S (T is already saturated):

$$\begin{aligned} S : X_1 &= bX_2 + bX_4 \\ X_2 &= aX_3 + \tau X_4 + aX_4 \\ X_3 &= aX_3 \\ X_4 &= aX_4 \end{aligned}$$

Now we observe that there is a relation $\mathcal{R} \subseteq \tilde{X} \times \tilde{Y}$ with $(X_1,Y_1) \in \mathcal{R}$, such that $(X_i,Y_j) \in \mathcal{R} \Rightarrow E_i \approx F_j$, and such that whenever $(X,Y) \in \mathcal{R}$ then

(i) whenever $X \xrightarrow{u}_S X'$, then <u>either</u> $u = \tau$ and $(X',Y) \in \mathcal{R}$

<u>or</u> $Y \xrightarrow{u}_T Y'$ with $(X',Y') \in \mathcal{R}$

(ii) whenever $Y \xrightarrow{u}_T Y'$, then <u>either</u> $u=\tau$ and $(X,Y') \in \mathcal{R}$

<u>or</u> $X \xrightarrow{u}_S X'$ with $(X',Y') \in \mathcal{R}$

The relation is $\mathcal{R} = \{(X_1,Y_1),(X_2,Y_2),(X_3,Y_2),(X_4,Y_2)\}$

We now take new variables $\{Z_{ij} | (X_i,Y_j) \in \mathcal{R}\}$ and form the following equation set:

$$\begin{aligned} U : Z_{11} &= bZ_{22} + bZ_{24} \\ Z_{22} &= aZ_{32} + \tau Z_{42} + aZ_{42} \\ Z_{32} &= aZ_{32} \\ Z_{42} &= aZ_{42} \end{aligned}$$

(the formation of the equation for W_{ij} is guided by the relation $\mathcal{R}$ in a way which will be made precise in the proof of the theorem).

Now, we can see that E_1 provably satisfies U by substituting E_1,E_2,E_3,E_4 for $Z_{11},Z_{22},Z_{32},Z_{42}$; also, F_1 provably satisfies U by substituting $F_1,\tau F_2,F_2,F_2$ for these variables (this depends on $\vdash \tau F_2 = F_2 + \tau F_2$).

The following theorem is a refinement of Theorem 5.10 of [Mil2]. That theorem showed that if E and F are <u>strongly</u> congruent, $E \sim F$, and provably satisfy standard equation sets S and T respectively, then S and T can be expanded to a single equation set U provably satisfied by both E and F. The extra difficulty encountered here is that observational congruence, $\approx^c$, is defined not directly but in terms of the auxiliary relation $\approx$, observational equivalence.

Theorem 3.2 Let E provably satisfy S, and F provably satisfy T, where both S and T are standard, guarded sets of equations, and let $E \approx^c F$. Then there is a standard, guarded equation set U provably satisfied by both S and T.

Proof We may suppose that $\tilde{X} = \{X_1,\ldots,X_m\}$, $\tilde{Y} = \{Y_1,\ldots,Y_n\}$ and $\tilde{W} = \{W_1,W_2,\ldots\}$ are disjoint sets of variables, that the given equation-sets (assumed saturated, by the Lemma) are

$$S : \tilde{X} = \tilde{H}$$
$$T : \tilde{Y} = \tilde{J}$$

with $fv(\tilde{H}) \subseteq \tilde{X}\cup\tilde{W}$, $fv(\tilde{J}) \subseteq \tilde{Y}\cup\tilde{W}$, and that there are expressions $\tilde{E} = \{E_1,\ldots,E_m\}$, $\tilde{F} = \{F_1,\ldots,F_n\}$ with $E_1 \equiv E$, $F_1 \equiv F$ and $fv(\tilde{E})\cup fv(\tilde{F}) \subseteq \tilde{W}$, so that

$$\vdash \tilde{E} = \tilde{H}\{\tilde{E}/\tilde{X}\}$$
$$\vdash \tilde{F} = \tilde{J}\{\tilde{F}/\tilde{X}\}$$

Now, because $E \approx^c F$ and S,T are saturated, we know that

(i) Whenever $X_1 \xrightarrow{u}_S X_i$ then, for some j, $Y_1 \xrightarrow{u}_T Y_j$ and $E_i \approx F_j$

(ii) Whenever $Y_1 \xrightarrow{u}_T Y_j$ then, for some i, $X_1 \xrightarrow{u}_S X_i$ and $E_i \approx F_j$

(iii) $X_1 \rhd W$ iff $Y_1 \rhd W$, for each $W \in \tilde{W}$.

Now, using the definition of observation equivalence - noting that in clauses (i) and (ii) above we cannot assume $E_i \approx^c F_j$ but only $E_i \approx F_j$ - we can extend this correspondence between X_1 and Y_1 to a relation $\mathcal{R} \subseteq \tilde{X} \times \tilde{Y}$ such that

1. Whenever $(X,Y) \in \mathcal{R}$ then

   (i) Whenever $X \xrightarrow{u} X'$, then either (a) $u=\tau$ and $(X',Y) \in \mathcal{R}$

   or (b) for some Y', $Y \xrightarrow{u} Y'$ and $(X',Y') \in \mathcal{R}$

   (ii) Whenever $Y \xrightarrow{u} Y'$, then either (a) $u=\tau$ and $(X,Y') \in \mathcal{R}$

   or (b) for some X', $X \xrightarrow{u} X'$ and $(X',Y') \in \mathcal{R}$

   (iii) $X \rhd W$ iff $Y \rhd W$, for each $W \in \tilde{W}$.

2. $(X_1,Y_1) \in \mathcal{R}$, and when $(X,Y) \equiv (X_1,Y_1)$ then cases (i)(a) and (ii)(a) do not obtain.

Furthermore, since we may suppose that S and T contain only variables which are reachable from X_1 and Y_1 respectively, we can assume that $dom\mathcal{R} = \tilde{X}$, $ran\mathcal{R} = \tilde{Y}$. (Note that $\mathcal{R}$ is a kind of bisimulation between S and

T considered as transition systems.)

In terms of $\mathcal{R}$, we now construct a new equation set

$$U : \tilde{Z} = \tilde{K}$$

using a new set $\tilde{Z}$ of variables, as follows:

$$\tilde{Z} = \{Z_{ij} \mid (X_i, Y_j) \in \mathcal{R}\}$$
$$\tilde{K} = \{K_{ij} \mid (X_i, Y_j) \in \mathcal{R}\}$$

where each expression K_{ij} contains the following terms:

(i) uZ_{kl}, whenever $X_i \xrightarrow{u} X_k$ and $Y_j \xrightarrow{u} Y_l$ and $(X_k, Y_l) \in \mathcal{R}$

(ii) τZ_{kj}, whenever $X_i \xrightarrow{\tau} X_k$ and $(X_k, Y_j) \in \mathcal{R}$

(iii) τZ_{il}, whenever $Y_j \xrightarrow{\tau} Y_l$ and $(X_i, Y_l) \in \mathcal{R}$

(iv) W, whenever $X_i \triangleright W$ and $Y_j \triangleright W$.

We now assert that E provably satisfies the equation set U (with Z_{11} as distinguished variable). In fact, we choose expressions G_{ij} as follows:

$$G_{ij} \equiv \begin{cases} \tau E_l \text{ if } \tau Z_{il} \text{ occurs in } K_{ij} \text{ for some } l \\ E_i \text{ otherwise} \end{cases}$$

and we assert that

$$\vdash G_{ij} = K_{ij}\{\tilde{G}/\tilde{Z}\} \qquad (*)$$

i.e. that the equations U are provably satisfied by the expressions $\tilde{G}$. For in the case that τZ_{il} does not occur in K_{ij}, for any l, then $K_{ij}\{\tilde{G}/\tilde{Z}\}$ contains (with possible repetitions) exactly the terms uE_k and/or $u\tau E_k$ for which $X_i \xrightarrow{u} X_k$, and exactly the terms W for which $X_i \triangleright W$, and (using $\vdash u\tau E_k = uE_k$) the assertion (*) follows from $\vdash E_i = H_i\{\tilde{E}/\tilde{X}\}$. On the other hand if τZ_{il} does occur in K_{ij}, for some l, then $K_{ij}\{\tilde{G}/\tilde{Z}\}$ contains in addition the term τE_i and/or $\tau\tau E_i$; in this case we have $G_{ij} \equiv \tau E_i$, so the assertion (*) follows from $\vdash \tau E_i = \tau E_i + E_i = \tau E_i + H_i\{\tilde{E}/\tilde{X}\}$.

In exactly the same way we can also show that F provably satisfies U.

It remains to show that U, which is clearly standard, is also guarded. But it is easy to show that any τ-cycle $Z_{ij} \xrightarrow{\tau}{}^{+} Z_{ij}$ implies either a τ-cycle $X_i \xrightarrow{\tau}{}^{+} X_i$ or a τ-cycle $Y_j \xrightarrow{\tau}{}^{+} T_j$, which cannot exist since S and T are guarded. Hence U is also guarded. □

4. Completeness for guarded expressions

In this section we show that the axiom system $\mathcal{A}_\tau^g$ - that is, the system $\mathcal{A}_\tau$ without axioms R3-R5 - is complete for guarded behaviour expressions. The proof requires two theorems in addition to that of the last section. First, we show that every guarded expression provably satisfies a guarded standard equation set; second, we show that any two guarded expressions which provably satisfy such an equation set are provably equal.

Definition A recursion μXE is guarded if X is guarded in E. An expression F is guarded if every subexpression of F which is a recursion is guarded.

Definition The variable W is guarded in the equation set $S:\tilde{X} = \tilde{H}$ if it is not the case that $X_1 \xrightarrow{\tau}{}^* X_i \rhd W$.

Theorem 4.1 (Equational characterisation) Every guarded expression E with free variables $\tilde{W}$ provably satisfies a standard guarded equation set S with free variables in $\tilde{W}$. Moreover, if W is guarded in E then W is guarded in S.

Proof We proceed by induction on the structure of E.

(i) $E \equiv 0$. Take S to be the single equation $X = 0$.

(ii) $E \equiv W$. Take S to be the single equation $X = W$.

(iii) $E \equiv uE'$. If X' is the distinguished variable of the equation set S' for E', add the equation $X = uX'$ to S' to form S, with the new variable X distinguished.

(iv) $E \equiv E'+E''$. If $X'=H'$ and $X''=H''$ are the leading equations in the equation sets S' and S'' (with distinct formal variables) for E' and E'' respectively, add the equation $X=H'+H''$ to form S with the new variable X distinguished.

(v) $E \equiv \mu W'E'$, with W' guarded in E'. Let S' be the equation set provably satisfied by E', with leading equation $X=H$. Since W' is guarded in S', it does not occur as a summand of H. Form S from S' by replacing every equation $X'=H'$ of S' by the equation $X'=H'\{H/W\}$; notice that this leaves the leading equation unchanged. It is a routine matter to show that S is guarded, and that any guarded free variable of E is guarded in S. With the help of recursion axiom R1,

it is easy to show that E provably satisfies S. □

The next theorem shows that every guarded equation set (not necessarily standard) has a unique solution up to provable equality. It follows Theorem 5.7 of [Mil2] closely; we give the full proof here to show how guardedness is employed in the presence of τ.

Theorem 4.2 (Unique solution of equations). If S is a guarded equation set with free variables in $\tilde{W}$, then there is an expression E which provably satisfies S. Moreover if F (with free variables in $\tilde{W}$) provably satisfies S, then $\vdash E=F$.

Proof By induction on the number m of equations in S : $\tilde{X}=\tilde{H}$, we find expressions $\tilde{E}$ with free variables in $\tilde{W}$ such that $\vdash \tilde{E} = \tilde{H}\{\tilde{E}/\tilde{X}\}$, and show that if expressions $\tilde{F}$ with free variables in $\tilde{W}$ are such that $\vdash \tilde{F} = \tilde{H}\{\tilde{F}/\tilde{X}\}$, then $\vdash \tilde{E}=\tilde{F}$.

If m=1, then S consists of the single equation X=H where X is guarded in H. By recursion rule R1, the expression μXH provably satisfies S; by recursion rule R2, if $\vdash F = H\{F/X\}$ then $\vdash F = \mu XH$.

Now assume the result for m, and let S contain the m+1 equations $\tilde{X}=\tilde{H}$, $X_{m+1}=H_{m+1}$. We first wish to find expressions $\tilde{E}$ and E_{m+1} such that

$$\begin{aligned} &\vdash \tilde{E} = \tilde{H}\{\tilde{E}/\tilde{X},E_{m+1}/X_{m+1}\} \\ &\vdash E_{m+1} = H_{m+1}\{\tilde{E}/\tilde{X},E_{m+1}/X_{m+1}\} \end{aligned} \qquad (1)$$

To this end, define the m expressions $\tilde{J} \equiv \tilde{H}\{\mu X_{m+1}H_{m+1}/X_{m+1}\}$, and consider the equation set $\tilde{X}=\tilde{J}$, which is guarded. Thus, by induction, there are m expressions $\tilde{E}$ with free variables in $\tilde{W}$ such that

$$\vdash \tilde{E} = \tilde{J}\{\tilde{E}/\tilde{X}\}$$

If we further choose $E_{m+1} \equiv (\mu X_{m+1}H_{m+1})\{\tilde{E}/\tilde{X}\}$, then the equations (1) are easily proven using routine properties of substitution, depending on the fact that $\tilde{X}$, X_{m+1} and $\tilde{W}$ are distinct variables.

For the second part, suppose that expressions $\tilde{F}$ and F_{m+1} with free variables in $\tilde{W}$ also provably satisfy S; that is

$$\begin{aligned} &\vdash \tilde{F} = \tilde{H}\{\tilde{F}/\tilde{X},F_{m+1}/X_{m+1}\} \\ &\vdash F_{m+1} = H_{m+1}\{\tilde{F}/\tilde{X},F_{m+1}/X_{m+1}\} \end{aligned} \qquad (2)$$

Now the second equation of (2) may be rewritten $\vdash F_{m+1} = H_{m+1}\{\widetilde{F}/\widetilde{X}\}\{F_{m+1}/X_{m+1}\}$. By recursion rule R2, since X_{m+1} is guarded in $H_{m+1}\{\widetilde{F}/\widetilde{X}\}$, we obtain $\vdash F_{m+1} = \mu X_{m+1}(H_{m+1}\{\widetilde{F}/\widetilde{X}\})$, which may be rewritten

$$\vdash F_{m+1} = (\mu X_{m+1} H_{m+1})\{\widetilde{F}/\widetilde{X}\} \qquad (3)$$

This allows us to deduce from the first m equations of (2), with a reordering of substitutions, that

$$\vdash \widetilde{F} = \widetilde{H}\{\mu X_{m+1} H_{m+1}/X_{m+1}\}\{\widetilde{F}/\widetilde{X}\}$$

which is to say that the expressions $\widetilde{F}$ provably satisfy the m equations $\widetilde{X}=\widetilde{J}$. Thus by induction we infer that

$$\vdash \widetilde{E} = \widetilde{F}$$

and hence also, from the definition of E_{m+1} and from (3), that

$$\vdash E_{m+1} = F_{m+1}$$

and the proof is complete. □

We now summarise the completeness of $\mathcal{A}_\tau^g$.

Theorem 4.3 (Completeness of $\mathcal{A}_\tau^g$). If E and F are guarded expressions and $E \approx^c F$, then $\mathcal{A}_\tau^g \vdash E=F$.

Proof By Theorem 4.1, E may be proved in $\mathcal{A}_\tau^g$ to satisfy a guarded equation set; likewise F. By Theorem 3.2, they may be proved to satisfy a single such equation set. Finally, by Theorem 4.2, they may be proved equal in $\mathcal{A}_\tau^g$. □

5. Completeness for all behaviour expressions

This section is mainly devoted to showing that every expression is provably equivalent to a guarded expression. This may be regarded as the entire purpose of the three recursion rules R3, R4 and R5 which extend the axiom system $\mathcal{A}_\tau^g$ to $\mathcal{A}_\tau$, since $\mathcal{A}_\tau^g$ has been proved complete for guarded expressions in the preceding sections. It is convenient to restate these rules here:

R3: $\mu X(X+E) = \mu XE$

R4: $\mu X(\tau X+E) = \mu X\tau E$

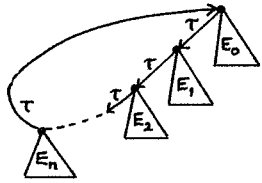
R5: $\mu X(\tau(X+E)+F) = \mu X(\tau X+E+F)$

We shall begin by giving some intuition behind R4 and R5, in graphical terms. For this purpose an alternative version of R5 is more revealing:

R5': $\mu X(\tau E+F) = \mu X(\tau X+E+F)$ provided X occurs unguarded in E

This rule is equipotent with R5, in the presence of other axioms; it was the version which I first proposed, and I am grateful to Gordon Plotkin for suggesting that there should be an alternative which requires no side-condition.

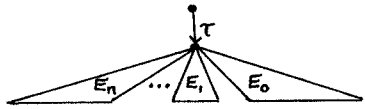
The purpose of R4 and R5 is to remove from μXG any occurrence of X in its body G which is unguarded, but "guarded" by τ (R3 is sufficient to remove any occurrence which is not even "guarded" by τ). If G contains such an occurrence of X, then μXG may be pictured informally as follows:



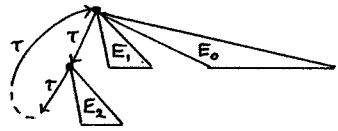
(1)

Now, because the τ-cycle may be followed arbitrarily many times before some E_i is entered ($0 \leq i \leq n$), the order in which these expressions E_i occur on the cycle is immaterial to the meaning of μXG; intuitively, we expect to be able to prove

$\mu XG = \mu X\tau(E_o+....+E_n)$



(Of course each E_i may contain further unguarded occurrences of X, not shown in the picture.) Now μXG - as pictured in (1) - takes the form $\mu X(E_o+\tau(E_1+\tau(E_2....)))$, which can be transformed by R5' to $\mu X(\tau X+E_o+E_1+\tau(E_2+...))$:



(2)

Furthermore, repeated application of R5' will "lift" $E_2,...,E_n$ up to the same level as E_o, and a final application of R4 (to remove τX) completes the transformation.

With this intuition, which is not fully rigorous of course, we proceed to the formal details - where we shall use R5 rather than R5'.

Lemma 5.1 If X occurs unguarded in E, then $\vdash E=X+E$

Proof By induction on the structure of E. Most cases are simple. Note in particular that if $E\equiv\tau E'$ then we need only use $\vdash E=E'+E$, and apply the inductive hypothesis for E'. If $E\equiv\mu YF$, with $X\not\equiv Y$, then by induction $\vdash F=X+F$, so by R1 $\vdash E=F\{E/Y\}=X+F\{E/Y\}$. No other recursion rule is needed in the proof. □

Note that this lemma easily yields the equipotence of R5 and R5', though we do not need this fact.

Theorem 5.2 For every expression E, there exists a guarded expression E' such that $\vdash E=E'$.

Proof We prove a stronger result by induction on the depth of nesting of recursions in E, namely:

For every E, there exists a guarded E' for which

(1) X is guarded in E'

(2) No free unguarded occurrence of any variable Y in E' lies within a recursion in E'

(3) $\vdash \mu XE = \mu XE'$

Assume now that the property holds for every F whose recursion depth is less than that of E. (The induction "basis", when E contains no recursions, is incorporated in our proof which is by transfinite induction).

First, consider any recursion μYF in E, which lies within no other recursion. By inductive assumption there is a guarded expression F' such that Y is guarded in F', no free unguarded occurrence of any variable in F' lies within a recursion, and $\vdash \mu YF=\mu YF'$. These conditions ensure that no free unguarded occurrence of a variable in $F'\{\mu YF'/Y\}$ occurs within a recursion in this expression.

Now let E_1 be the result of simultaneously replacing every such top-level recursion μYF in E by $F'\{\mu YF'/Y\}$; clearly $\vdash E=E_1$. Moreover, no free unguarded occurrence of any variable in E_1 lies within a recursion. In converting E_1 to E' such that $\vdash \mu XE_1=\mu XE'$, it remains only to remove all free unguarded occurrences of X from E_1, knowing that they do not lie within recursions. If there are none, we are done.

Otherwise, designate a free unguarded occurrence of X in E_1. If it occurs as a summand of E_1, i.e. $E_1 \equiv X+\ldots$, then use R3 to remove it. Otherwise it occurs within E_2, where $E_1 \equiv \tau E_2+E_3$. Now by the lemma, we have $\vdash E_2=X+E_2'$ and by R5

$$\vdash \mu X(\tau(X+E_2')+E_3) = \mu X(\tau X+E_2'+E_3)$$

Thus, by transforming E_1 into $E_1' \equiv \tau X+E_2'+E_3$, we have reduced the depth of τ-guarding of our designated occurrence, and have not increased the depth of any other free unguarded occurrence of X.

Proceeding in this way, all such occurrences may be converted into summands X or τX; at any stage a summand X may be removed by R3, and at the end any summand τX may be removed by R4. We have thus obtained E' such that $\vdash \mu XE_1=\mu XE'$ where X is guarded in E'. Moreover, since those subexpressions of E_1 which are recursions have been left unchanged in the transformation, E' is indeed guarded and contains no free unguarded variable within a subexpression which is a recursion. □

We now summarise the completeness of $\mathcal{A}_\tau$

Theorem 5.3 If $E \approx^c F$ then $\mathcal{A}_\tau \vdash E=F$

Proof We need only apply Theorem 5.2 to convert E and F to guarded form, and then apply Theorem 4.5. □

6. Applications and Further Work

Many interesting concurrent systems may be described not by a single behaviour expression, but by a finite set of such expressions (each representing a sequential component) composed "in parallel"; the composite expression represents the behaviour of a system in which the components communicate with one another via the atomic actions of Act. One way of composing behaviour expressions is to use the Composition operator $-|-$ and the Restriction operators $-\backslash A$ (one for each $A \subseteq Act$) of CCS[Mil1]; they are defined by the following rules, extending the definition of $\rightarrow$ in Section 1:

(iv) If $E \xrightarrow{u} E'$ then $E|F \xrightarrow{u} E'|F$

If $F \xrightarrow{u} F'$ then $E|F \xrightarrow{u} E|F'$

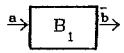
If $E \xrightarrow{a} E'$ and $F \xrightarrow{\bar{a}} F'$ then $E|F \xrightarrow{\tau} E'$

(v) If $E \xrightarrow{u} E'$ and $u \notin A$ then $E\backslash A \xrightarrow{u} E'\backslash A$

In the third rule of (iv) we have assumed that there is a bijection $(\bar{\ })$ over Act, with $\bar{\bar{a}} = a$; $\bar{a}$ is called the complement of a. Further expressive power is gained by adding the Renaming operators $-[S]$ of CCS, where $S : Act \rightarrow Act$ is a function which respects complementation, i.e. $\overline{S(a)} = S(\bar{a})$ (by convention, we set $S(\tau)=\tau$).

(vi) If $E \xrightarrow{u} E'$ then $E[S] \xrightarrow{S(u)} E'[S]$

As a very simple example, we consider an n-buffer (a buffer with storage capacity n) built from n 1-buffers. A 1-buffer B_1



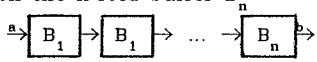
for Boolean values $\{0,1\}$ may be defined as follows:

$$B_1 = \mu X(a_0\bar{b}_0X + a_1\bar{b}_1X)$$

(a_i means "input the value i" and $\bar{b}_i$ means "output the value i"). Now if c/a is the renaming function which converts a_i to c_i, we can define the chaining operator $\frown$ as follows:

$$P \frown Q = (P[c/b] \mid Q[c/a])\backslash\{c_0, c_1\}$$

Then the n-fold buffer B_n



can be simply defined as $B_1 \frown B_1 \frown \ldots \frown B_1$ (n times).

Now any such composition of sequential finite-state behaviours can be

shown, by use of the CCS Expansion Theorem [Mil1], to satisfy a finite equation set; therefore, by a simple extension of the results of this paper, we have a complete proof system for establishing observational congruence of such systems.

CCS is, of course, more general than this. First, it caters for treatment of values drawn from an infinite set; second, it allows for general recursions $\mu X E$ in which E may any of the operators, including composition. This latter, even without infinite value-sets, is enough to preclude the possibility of any effective axiom system. However, a large number of interesting systems can be described without using composition within recursion; this includes in particular the rich family of communications protocols. Such systems, provided that data-values (even though drawn from an infinite set) are treated in a uniform manner, are essentially finite-state, and the proof system presented here is therefore complete for establishing observational congruence. Thus, when the specification of a system can conveniently be presented as a behaviour expression, we have provided a complete method for establishing that a system meets its specification.

We turn now to a suggestion for further research. There is one aspect of observational equivalence or congruence which is often criticised; it is possible that two expressions are congruent, even when one is <u>divergent</u> and the other <u>convergent</u>. There is more than one possible way of defining divergence, but at least it should have the following property : E is divergent, which we write $E\uparrow$, if there is an infinite sequence

$$E \xrightarrow{\tau} E_1 \xrightarrow{\tau} E_2 \xrightarrow{\tau} \ldots.$$

We may also wish to say that μXX is divergent even though it does not possess such an infinite computation. The axiom which most obviously equates a divergent expression with a convergent expression is R4 - indeed, its whole purpose is to excise a τ-loop from a behaviour. For example, by setting $E \equiv 0$ it has $\mu X \tau X = \mu X \tau 0$ as an instance.

It is therefore a natural challenge to refine the definitions of observational congruence so that it never equates a divergent expression with a convergent one, and to find a corresponding axiomatisation. In fact, it is natural first to define an asymmetric version of weak bisimulation such as the following (see also [HP]):

Definition A relation $\mathcal{R} \subseteq \mathcal{E}_\tau \times \mathcal{E}_\tau$ is a weak partial bisimulation if, whenever $(E,F)\in\mathcal{R}$,

(i) If $E \xrightarrow{u} E'$ then, for some F', $F \overset{\hat{u}}{\Longrightarrow} F'$ and $(E',F')\in\mathcal{R}$

(ii) If $E\downarrow$ then (a) $F\downarrow$, (b) If $F \xrightarrow{u} F'$ then, for some E', $E \overset{\hat{u}}{\Longrightarrow} E'$ and $(E',F')\in\mathcal{R}$

(iii) If $E \rhd X$ then $F \rhd X$, and if $E\downarrow$ and $F \rhd X$ then $E \rhd X$.

If $(E,F)\in\mathcal{R}$ for some weak partial bisimulation $\mathcal{R}$, then we write $E \sqsubseteq_{\approx} F$. □

It is clear that $\sqsubseteq_{\approx}$ is a preorder, but that if E and F are convergent then $E \sqsubseteq_{\approx} F$ iff $E \approx F$. As before, we then look for a slight refinement $\sqsubseteq_{\approx}^{c}$ of $\sqsubseteq_{\approx}$ which is also substitutive; the exact definition may depend upon the exact definition of divergence, but we expect that $\sqsubseteq_{\approx} \cap \sqsubseteq_{\approx}^{c}$ will be a stronger congruence relation than $\approx^{c}$, and it is perhaps more acceptable since it respects divergence.

We therefore conclude with an open problem: to find a complete axiomatisation of some such substitutive preorder $\sqsubseteq_{\approx}^{c}$ over $\mathcal{E}_\tau$.

REFERENCES

[BHR] S.D.Brookes, C.A.R.Hoare and A.W.Roscoe, "A Theory of Communicating Sequential Processes", J.ACM 31,3, pp560-599, 1984.

[BK] J.A.Bergstra and J.W.Klop, "A Complete Inference System for Regular Processes with Silent Moves", Report CS-R8420, Centre for Mathematics and Computer Science, Amsterdam, 1984.

[Hen] M.C.Hennessy, "Acceptance Trees", J.ACM. 32,4, pp896-928, 1985.

[HM] M.C.Hennessy and A.J.R.G.Milner, "Algebraic Laws for Nondeterminism and Concurrency", J.ACM 32,1, pp137-161, 1985.

[HP] M.C.Hennessy and G.D.Plotkin, "A Term Model for CCS", in Vol.88 Lecture Notes in Computer Science, pp261-274, 1980.

[Kel] R.Keller, "Formal Verification of Parallel Programs", Comm. ACM 19,7, pp561-572, 1976.

[Mil1] A.J.R.G.Milner, A Calculus for Communicating Systems, Vol.92, Lecture Notes in Computer Science, Springer Verlag, 1980. Also to be reissued as a report of the Computer Science Dept, Edinburgh University.

[Mil2] A.J.R.G.Milner, "A Complete Inference System for a Class of Regular Behaviours", J.Comp. and Sys.Sci 28,3, pp439-466, 1984.

[Mil3] A.J.R.G.Milner, "Calculi for Synchrony and Asynchrony", J.Theor.Comp. Sci. 25, pp267-310, 1983.

[Mil4] A.J.R.G.Milner, "Lectures on a Calculus for Communicating Systems", to appear in Control Flow and Data Flow : Concepts of Distributed Programming, proceedings of NATO International Summer School of Marktoberdorf in 1984, ed. Manfred Broy, Springer Study Edition, Springer-Verlag, 1986.

[Par] D.M.R.Park, "Concurrency and Automata on Infinite Sequences", Proc. 5th GI Conference, LNCS Vol.104, pp167-183, 1981.