Robin Milner:

# Complete axiomatizations of strong and observational congruence for finite agent.

Edinburgh University
1986

## k.1 Sequentialisation of finite agents

We call an agent sequential if it contains only the combinators NIL, $\mu.$, + and recursion; that is, if does not involve Composition ($|$), Restriction ($\backslash L$) or Relabelling ($[R]$). We call an agent finite if it contains no recursion. In this Chapter we shall show that the equational laws which we have developed earlier are enough to prove the equality of any two finite agents which are observation congruent; that is, the laws are complete for observation congruence of finite agents. They cannot be complete for observation congruence of all agents, for this would imply that we could recursively enumerate the set of pairs $(P,Q)$ of agents such that $P \approx^c Q$, and we shall later outline a proof that this would solve the halting problem for Turing machines.

We begin the task by proving, in this section, that every finite agent can be proved strongly congruent to a finite sequential agent, using the equational laws. Thus the problem is reduced to showing that the equational laws are complete for finite sequential agents — those which contain only the combinators NIL, $\mu.$ and +.

## k.2 Laws for finite sequential agents

For the remainder of the Chapter we deal only with finite sequential agents, i.e. those containing only NIL, $\mu$. and $+$. It is convenient to recall the laws that we shall need, and to group them in two sets. The first set, which we call $\mathcal{A}_1$, are as follows:

Axioms $\mathcal{A}_1$

$(A_1)$ $P+Q = Q+P$ $\qquad$ $(A_3)$ $P+P = P$

$(A_2)$ $P+(Q+R) = (P+Q)+R$ $\qquad$ $(A_4)$ $P+NIL = P$

We shall write $\mathcal{A}_1 \vdash P=Q$ to mean that the equation $P=Q$ can be proved by normal equational reasoning from the axioms $\mathcal{A}_1$. We have already shown that these axioms are sound for strong congruence; that is, if $\mathcal{A}_1 \vdash P=Q$ then $P \sim Q$. Our first task, in the next two sections, is to show the converse, that they are complete for strong congruence of finite sequential agents; that is, if $P \sim Q$ then $\mathcal{A}_1 \vdash P=Q$.

The second set of axioms consists of $\mathcal{A}_1$ with three further axioms:

Axioms $\mathcal{A}_2$

$(A_1)$–$(A_4)$ as in $\mathcal{A}_1$ $\qquad$ $(A_6)$ $P+\tau P = \tau P$

$(A_5)$ $\mu\tau P = \mu P$ $\qquad$ $(A_7)$ $\mu(P+\tau Q)+\mu Q = \mu(P+\tau Q)$

We have already shown that $\mathcal{A}_2$ is sound for observation congruence;

that is, if $\mathcal{A}_2 \vdash P = Q$ then $P \approx^c Q$. Our second task in this Chapter is to show the converse, that they are complete for observation congruence of finite sequential agents; that is, if $P \approx^c Q$ then $\mathcal{A}_2 \vdash P = Q$.

For the remainder of this Chapter we shall assume that all agents are finite sequential, without using this qualification.

## k.3 Standard form

Let us define

$$\sum_{i=1}^{m} \mu_i P_i \triangleq \mu_1 P_1 + \cdots + \mu_m P_m$$

with the proviso that NIL is intended in the case $m=0$. Note that axioms $(A_1)$ and $(A_2)$ allow us to ignore the order and grouping of terms in a summation. We shall say that that $P$ is in <u>standard form</u> if

(1) $P$ is of form $\sum_{i=1}^{m} \mu_i P_i$

(2) Each $P_i$ is also in standard form.

For example NIL, $\alpha$NIL and $\alpha$NIL $+\beta(\gamma$NIL$+\xi$NIL$)$ are in standard form, but $\alpha$(NIL $+\beta$NIL) is not. Our first observation is the following:

<u>Lemma k.1</u> For any $P$, there is a standard form $P'$ such that

$$\mathcal{A}_1 \vdash P = P'$$

<u>Proof</u> It is easy to see that, by use of the axioms particularly $(A_4)$, the term NIL may be eliminated from any summation ...+NIL+... occurring in $P$, and that the result of this elimination is in standard form □

This lemma allows us to confine our attention to standard forms in proving our two completeness theorems.

## k.4 Completeness of axioms $\mathcal{A}_1$ for strong congruence

**Theorem k.2** (Completeness 1). If $P$ and $Q$ are finite sequential and $P \sim Q$, then $\mathcal{A}_1 \vdash P = Q$.

*Proof.* We may assume that $P$ is in standard form $\sum_{i=1}^{m} \mu_i P_i$, and $Q$ is in standard form $\sum_{j=1}^{n} \nu_j Q_j$. The proof is by induction on the maximum depth of $P$ and $Q$, where the depth of $P$ is the maximum number of nested action-prefixes in $P$.

If the maximum depth is 0 then $P$ and $Q$ are both $NIL$, and axiom $(A_3)$ gives the result. Otherwise let $\mu P'$ be a summand of $P$. Then $P \xrightarrow{\mu} P'$, so by strong congruence there is a $Q'$ such that $Q \xrightarrow{\mu} Q'$ and $P' \sim Q'$. But this means that $\mu Q'$ is a summand of $Q$, and by induction $\mathcal{A}_1 \vdash P' = Q'$, so the summand $\mu P'$ of $P$ can be proved equal to a summand of $Q$ from the axioms $\mathcal{A}_1$. Similarly every summand $\nu Q'$ of $Q$ can be proved equal to a summand of $P$. It follows that $\mathcal{A}_1 \vdash P = Q$, by using $(A_1)$ to reorder summands and $(A_3)$ to eliminate duplicate occurrences (of course $(A_2)$ is used implicitly to justify the omission of grouping in a summation).

□

## k 5 Full standard form

Consider the agent $P \equiv a(P_1 + \tau P_2)$. (From now on we shall use "$\equiv$" to mean identity of agents, not to be confused with "$=$", which in this Chapter is only used in the context $\mathcal{A} \vdash P = Q$.). We can see that $P \stackrel{a}{\Rightarrow} P_2$, but not $P \xrightarrow{a} P_2$. However, the axiom $(A_7)$ allows us to prove $\mathcal{A}_2 \vdash P = P'$, where $P' \equiv a(P + \tau P_2) + aP_2$, and now $P' \xrightarrow{a} P_2$.

Now consider the agent $P \equiv \tau(P_1 + aP_2)$. Again, we have $P \stackrel{a}{\Rightarrow} P_2$ but not $P \xrightarrow{a} P_2$. We would like to find $P'$ such that $\mathcal{A}_2 \vdash P = P'$ and $P' \xrightarrow{a} P_2$. For this purpose we prove a simple Lemma.

**Lemma k.3** $\quad \mathcal{A}_2 \vdash \tau(P+Q) = \tau(P+Q) + Q$

**Proof**

$$\begin{aligned} \mathcal{A}_2 \vdash \tau(P+Q) + Q & \\ = \tau(P+Q) + P + Q + Q & \quad \text{by } (A_1), (A_6) \\ = \tau(P+Q) + P + Q & \quad \text{by } (A_3) \\ = \tau(P+Q) & \quad \text{by } (A_1), (A_6) \end{aligned}$$

Note that $(A_2)$ is used implicitly. □

Using this lemma on the agent $P \equiv \tau(P_1 + aP_2)$, we find $\mathcal{A}_2 \vdash P = P'$ where $P' \equiv \tau(P_1 + aP_2) + aP_2$, and $P' \xrightarrow{a} P_2$ as we wanted.

The two transformations just illustrated are examples of a general Lemma, which we now prove.

× **Lemma k.4** (Absorption) If $P$ is a standard form, and $P \overset{\mu}{\Longrightarrow} P'$, then $A_2 \vdash P = P + \mu P'$.

**Proof** By induction on the structure of $P$. Consider the three cases for $P \overset{\mu}{\Longrightarrow} P'$:

**Case 1**: $\mu P'$ is a summand of $P$. Then clearly the conclusion holds, mainly via $(A_3)$.

**Case 2**: $\mu Q$ is a summand of $P$, and $Q \overset{\tau}{\Longrightarrow} P'$. Then by induction $A_2 \vdash Q = Q + \tau P'$, so

$$\begin{aligned} A_2 \vdash P &= P + \mu Q && \text{by } (A_3) \\ &= P + \mu(Q + \tau P') \\ &= P + \mu(Q + \tau P') + \mu P' && \text{by } (A_7) \\ &= P + \mu Q + \mu P' \\ &= P + \mu P' && \text{by } (A_3). \end{aligned}$$

Case 3: $\tau Q$ is a summand of $P$ and $Q \not\xRightarrow{\mu} P'$.

Then by induction $\mathcal{A}_2 \vdash Q = Q + \mu P'$, so

$$\begin{aligned}
\mathcal{A}_2 \vdash P &= P + \tau Q && \text{by } (A_3) \\
&= P + \tau(Q + \mu P') \\
&= P + \tau(Q + \mu P') + \mu P' && \text{by Lemma k.3} \\
&= P + \tau Q + \mu P' \\
&= P + \mu P' && \text{by } (A_3).
\end{aligned}$$

This concludes the proof. □

We shall take advantage of this Lemma to find a 'more' standard form for finite agents. We shall say that $P$ is in <u>full standard form</u> if

(1) $P$ is of form $\sum_{i=1}^{m} \mu_i P_i$ where each $P_i$ is in full standard form.

(2) Whenever $P \xRightarrow{\mu} P'$ then $P \not\xrightarrow{\mu}$.

We saw two examples of standard forms which are not full; a more complex example is

$$P \equiv \tau(\alpha(\tau NIL + \beta NIL))$$

for which $P \xrightarrow{\tau\alpha\tau} NIL$ but <u>not</u> $P \xrightarrow{\alpha} NIL$. Lemma k.4 allows us to show $\mathcal{A}_2 \vdash P = P'$ where

$$P' \equiv \tau(\alpha(\tau NIL + \beta NIL)) + \alpha NIL$$

but $P'$ is still not a full standard form. There *is* a full standard form $P''$ such that $\mathcal{A}_2 \vdash P = P''$, namely

$$P'' \equiv \tau\left(\alpha\left(\tau NIL + \beta NIL\right) + \alpha NIL\right) + \alpha\left(\tau NIL + \beta NIL\right) + \alpha NIL$$

In fact we shall need the following important Lemma in our completeness proof.

**Lemma k.5** For any standard form $P$ there is a full standard form $P'$ of equal depth such that $\mathcal{A}_2 \vdash P = P'$.

**Proof** By induction on the depth of $P$. When the depth is zero there is nothing to prove, since $P \equiv NIL$. Otherwise, we may assume by induction — without affecting the depth of $P$ — that every summand $\nu Q$ of $P$ has $Q$ in full standard form.

Now consider all pairs $(\mu_i, P_i)$, $1 \leq i \leq k$ say, such that $P \xRightarrow{\mu_i} P_i$ but *not* $P \xrightarrow{\mu_i} P_i$.
Each $P_i$ must be a full standard form — since it occurs within a summand of $P$ — and hence

$$P' \equiv P + \mu_1 P_1 + \cdots + \mu_k P_k$$

is a full standard form, and moreover by Lemma k.4 (repeatedly) we have $\mathcal{A}_2 \vdash P = P'$! □

We are now ready to prove our second completeness Theorem.

# k 6 Completeness of axioms $\mathcal{A}_2$ for observation congruence

Our proof of the completeness of $\mathcal{A}_2$ for observation congruence is closely modelled on that of $\mathcal{A}_1$ for strong congruence. It is a little more complex, largely because if $P$ and $Q$ are observation congruent their derivatives only match up to observation equivalence (not congruence). However, this defect is beautifully remedied by Hennessy's Theorem

$$P \approx Q \text{ iff } (P \approx^c Q \text{ or } P \approx^c \tau Q \text{ or } \tau P \approx^c Q)$$

which we proved earlier as Theorem ....

Theorem k.6 (Completeness 2). If $P$ and $Q$ are finite sequential and $P \approx^c Q$ then $\mathcal{A}_2 \vdash P = Q$.

Proof We may assume that $P$ and $Q$ are in full standard form, by Lemmas k.1 and k.5, and our proof is by induction on the sum of the depths of $P$ and $Q$.

For the base case there is nothing to prove, since $P \equiv \text{NIL} \equiv Q$. Otherwise let $\mu P'$ be a summand of $P$. Then $P \stackrel{\mu}{\rightarrow} P'$, so by observation congruence there is a $Q'$ such that $Q \stackrel{\mu}{\Rightarrow} Q'$ and $P' \approx Q'$. Moreover $Q \stackrel{\mu}{\rightarrow} Q'$ since $Q$ is full, so $\mu Q'$ is a summand of $Q$.

Now by Hennessy's Theorem, $P' \approx^c Q'$ or $P' \approx^c \tau Q'$ or $\tau P' \approx^c Q'$. In the first case, since $P'$ and $Q'$ are in full standard form and respectively less deep than $P$ and $Q$, by induction $\mathcal{A}_2 \vdash P' = Q'$; so $\mathcal{A}_2 \vdash \mu P' = \mu Q'$. In the second case, we must convert $\tau Q'$ to full standard form before applying induction. From Lemma K5, there exists $Q''$ in full standard form and equal in depth to $\tau Q'$ such that $\mathcal{A}_2 \vdash \tau Q' = Q''$; hence $P' \approx^c Q''$ and by induction (since the depth-sum is reduced by one) we infer $\mathcal{A}_2 \vdash P' = Q''$; hence $\mathcal{A}_2 \vdash P' = \tau Q'$; hence by axiom $(A_5)$ we again infer $\mathcal{A}_2 \vdash \mu P' = \mu Q'$. The third case is similar.

Thus we have shown in each case that the summand $\mu P'$ of $P$ can be proved equal to a summand of $Q$ from the axioms $\mathcal{A}_2$. Similarly every summand $\nu Q'$ of $Q$ can be proved equal to a summand of $P$. As in Theorem K2, it then follows that $\mathcal{A}_2 \vdash P = Q$ as required. □