INFORMATION AND CONTROL 68, 125–145 (1986)

A Modal Characterization of Observational Congruence on Finite Terms of CCS

S. GRAF AND J. SIFAKIS

IMAG - Génie Informatique,
BP 68, 38402 St Martin-d'Hères Cédex, France

We propose a translation method of finite terms of CCS into formulas of a modal language representing their class of observational congruence. For this purpose, we define a modal language and a function associating with any finite term of CCS a formula of the language, satisfied by the term. Furhtermore, this function is such that two terms are congruent if and only if the corresponding formulas are equivalent. The translation method consists in associating with operations on terms (action, +) operations on the corresponding formulas. This work is a first step towards the definition of a modal language with modalities expressing both possibility and inevitability and which is compatible with observational congruence.

I. INTRODUCTION

When a logic L is used to express program specifications it naturally induces an equivalence relation $\sim^L$ on programs: two programs PROG 1 and PROG 2 are equivalent if they cannot be distinguished by any formula of L, i.e., PROG $1 \sim^L$ PROG 2 iff for any formula F of L PROG $1 \models F$ and PROG $2 \models F$ are equivalent.

Using a logic L as a program specification tool sets the problem of its compatibility with respect to some equivalence relation $\simeq$ derived from the operational semantics of the description language. Such a relation defines a concept of operational equivalence which is supposed to be the most suitable and satisfactory in practice for the comparison of programs. Then, a minimal requirement for the adequacy of L as a specification tool is that $\simeq \subseteq \sim^L$, i.e., if two programs are operationally equivalent then they have the same (equivalent) specifications. The non-validity of this condition implies that there exists a formula F of L and two operationally equivalent programs, the one satisfying F and the other not; thus, using F to express a property, does not allow a characterization of the most general class of behaviors corresponding to this property. If in addition, L is to be used as a verification tool then it is also necessary that $\sim^L \subseteq \simeq$ i.e., if two programs cannot be distinguished by formulas of L then they are

0019-9958/86 $3.00

equivalent. Consequently, the adequacy of L as both a specification and a verification tool, implies that the relations $\simeq$ and $\sim^L$ agree.

The problem of the definition of logics compatible with some operational equivalence relation has been stated in Hennessy and Milner (1980), Brookes and Rounds (1983), and Stirling (1983), where simple modal languages have been proposed to characterize observational equivalence or congruence of CCS. According to these results, an equivalence or congruence class can be characterized as the (infinite) conjunction of the formulas satisfied by processes of this class. This paper is a first step to the definition of a modal logic compatible with observational congruence of CCS by following a different approach. A method is given to obtain a formula representing the congruence class of a CCS-term in a compositional manner. For this, we associate with CCS-operators, rules describing how the formula representing the class of a CCS-term is obtained by composition of formulas of its sub-terms.

We consider a very general modal language $L(A)$ for which labelled trees (CCS-terms) on a vocabulary A constitute a class of models and try to define a sub-language L_0 such that $\sim^{L_0}$ coincides with observational congruence in CCS. $L(A)$ contains as sublanguages the modal languages introduced in Hennessy and Milner (1980) and Stirling (1983). A function $|\ |$ is defined, associating with any finite term t of CCS a formula $|t|$ of $L(A)$ such that $|t|$ is satisfied by all the terms and only the terms congruent to t, i.e., $t \models |t|$ and for t_1, t_2 arbitrary finite terms, $t_1 \simeq t_2$ iff $|t_1| \equiv |t_2|$, where $\simeq$ is the observational congruence. Obviously, L_0 corresponds to the sub-language of $L(A)$ generated by the elements of the image of $|\ |$. This approach has been adopted to (hopefully) avoid limitations of the works mentioned above, concerning the definition of modalities expressing inevitability and the modal characterization of classes of infinite behaviours. However, these two problems are not discussed in this paper.

For the definition of $L(A)$, we have been inspired by Kozen (1982), where a very general modal language with a least fixpoint operator has been introduced. In Section III we first give a modal characterization of strong equivalence of CCS to get the reader familiar with the principle of translation of terms into formulas. Then, we give a translation method of finite CCS terms into formulas representing their class of observational congruence. This method consists of associating with operations on terms (action, $+$) operations on the corresponding formulas. Finally, we discuss the use of these results for the definition of a sufficiently powerful language compatible with observational congruence.

II. Definition of the Modal Language

We introduce as in Kozen (1982) the modal language $L(A)$ as the sublanguage of the closed formulas of $L'(A)$, defined on the logical constants true, false, a set of constants A and a set of variables X as follows,

— true, false $\in L'(A)$,

— $A \cup X \subseteq L'(A)$,

— $f, f' \in L'(A)$ implies $\neg f, f \vee f' \in L(A)$

— $f \in L'(A)$ implies $\langle f \rangle \in L'(A)$,

— $x \in X$ and $f(x)$ is a functional, positive in the variable x, implies $\mu x.\, f(x) \in L'(A)$.

Semantics. The class of models of $L(A)$ is the class of the labelled trees on A, $T(A)$. A labelled tree t is defined as $t = (Q_t, q_0, \{\rightarrow^a\}_{a \in A})$ where,

— Q_t is a set of *states*, the nodes of t,

— $q_0 \in Q_t$ is the *initial state*, the root of t,

— $\{\rightarrow^a\}_{a \in A}$ is a set of transition relations, $\rightarrow^a \subseteq Q_t \times Q_t$;

as t is a tree we have $\exists q \in Q_t\ \nexists a \in A\ q \rightarrow^a q_0$ and $\forall q \in Q_t,\ q \neq q_0,\ q$ has exactly one predecessor.

We define in the usual manner a satisfaction relation

$$\models \subseteq \left(\bigcup_{t \in T(A)} (t \times Q_t) \right) \times L(A).$$

For a formula $f \in L(A)$ we write,

— $t, q \models f$ iff $(t, q, f) \in \models$,

— $t \models f$ iff $t, q_0 \models f$, where q_0 is the root of t,

— $\models f$ iff $t \models f\ \forall t \in T(A)$.

For $t \in T(A)$, $q \in Q_t$, $f, f' \in L(A)$, $g \in L'(A)$, and $a \in A$,

— $t, q \models \text{true}$,

— $t, q \models \neg f$ iff $t, q \not\models f$,

— $t, q \models f \vee f'$ iff $t, q \models f$ or $t, q \models f'$,

— $t, q \models a$ iff $\exists q' \in Q_t\ q' \rightarrow^a q$,

— $t, q \models \langle f \rangle$ iff $\exists q' \in Q_t\ \exists a \in A\ (q \rightarrow^a q'$ and $t, q' \models f)$,

— $t, q \models \mu x.g(x)$ iff $\forall f \in L(A)\ (\models g(f) \supset f$ implies $t, q \models f)$.

The notations false , $\wedge$, $\supset$, $\equiv$ are used in the standard manner. We use the abbreviation $[f] := \neg\langle\neg f\rangle$, i.e.,

— $t, q \models [f]$ iff $\forall q' \in Q_t\ \forall a \in A$ $(q \to^a q'$ implies $t, q' \models f)$.

Notice that each state $q \in Q_t$ in $t = (Q_t, q_0, \{\to^a\}_{a \in A})$ defines a subtree t_q of t, with root q and set of states the set of the states reachable from q in t. Thus, the transition relations $\to^a$ can be considered as relations on $T(A)$ and one can write $t_q \to^a t_{q'}$, instead of $q \to^a q'$. In the sequel we consider the class $L\langle A\rangle$ of the formulas where any element of A is written within the scope of one of the operators $\langle\ \rangle$ or $[\ ]$. For such formulas f we have $t, q \models f$ iff $t_q \models f$, i.e., f is true at a state q of a tree t iff f is true for the subtree t_q of t. So, we consider only the satisfaction relation $\models \in T(A) \times L\langle A\rangle$. The following properties are used:

PROPERTIES 1. For $t \in T(A)$ and $f, f_i, i \in J$, elements of $L\langle A\rangle$,

(a) $t \models \langle a \wedge f\rangle$ iff $\exists t' \in T(A)$ $(t \to^a t'$ and $t' \models f)$,

(b) $t \models [\bigvee_{i \in J} a_i \wedge f_i]$ iff $\forall t' \in T(A)$ $(t \to^a t'$ implies $\exists i \in J$ $(a = a_i$ and $t' \models f_i))$,

(c) $\models \langle f \vee f'\rangle \equiv \langle f\rangle \vee \langle f'\rangle$,

(d) $\models \langle f \wedge f'\rangle \supset \langle f\rangle \wedge \langle f'\rangle$.

Other properties of $L(A)$ can be found in Kozen (1982), where a complete axiomatization is given for a similar logic. In the sequel, we often simply write f instead of $\models f$.

III. MODAL CHARACTERIZATION

III.1 *Strong Equivalence*

In order to get the reader familiar with our approach, we give a modal characterization of strong equivalence of CCS in terms of formulas of the language described in II.

DEFINITION 1. (a) Consider the set of terms $P(A)$ built from a constant Nil, a set of unary operators A and a binary operator $+$, recursively defined by

— $\text{Nil} \in P(A)$,

— $ap \in P(A)$ for $p \in P(A)$ and $a \in A$,

— $p + p' \in P(A)$ for $p, p' \in P(A)$.

(b) For $a \in A$ the relation $\rightarrow^a \subseteq P(A) \times P(A)$ is defined as the smallest relation satisfying

— $ap \rightarrow^a p$,
— $p_1 \rightarrow^a p'$ implies $p_1 + p_2 \rightarrow^a p'$,
— $p_2 \rightarrow^a p'$ implies $p_1 + p_2 \rightarrow^a p'$.

So, with a term p can be associated a labelled tree $t_p = (Q_p, p, \{\rightarrow^a\}_{a \in A}) \in T(A)$, where Q_p is a set of subterms of p and $\rightarrow^a$ is the relation defined above. In the sequel we identify a term $p \in P(A)$ with the tree t_p representing it. So, if f is any formula of $L\langle A' \rangle$ where A' is isomorphic to A, then we can write $p \models f$ instead of $t_p \models f$. As there is no risk of confusion, we shall not distinguish between a unary operator a and the corresponding constant of the modal language.

PROPERTIES 2. (a) $\text{Nil} \models [\text{false}]$,
(b) $p \models f$ implies $ap \models \langle a \wedge f \rangle \wedge [a \wedge f]$,
(c) $p \models \langle a \wedge f \rangle$ implies $p + p' \models \langle a \wedge f \rangle$ and $p' + p \models \langle a \wedge f \rangle$,
(d) $p_1 \models [f_1]$ and $p_2 \models [f_2]$ implies $p_1 + p_2 \models [f_1 \vee f_2]$,
(e) $p + \text{Nil} \models f$ iff $p \models f$,
(f) $p + p' \models [f]$ iff $p \models [f]$ and $p' \models [f]$.

In the sequel we often omit conjunction operators in order to simplify formulas.

DEFINITION 2. (strong equivalence). Let $\sim$ be the greatest relation on $P(A)$ such that for $p_1, p_2 \in P(A)$,

$$p_1 \sim p_2 \text{ iff } \forall a \in A \ (p_1 \rightarrow^a p_1' \text{ implies } \exists p_2'(p_2 \rightarrow^a p_2' \text{ and } p_1' \sim p_2'))$$

and

$$\forall a \in A \ (p_2 \rightarrow^a p_2' \text{ implies } \exists p_1'(p_1 \rightarrow^a p_1' \text{ and } p_1' \sim p_2')).$$

It has been shown that $\sim$ is a congruence (Milner, 1980), and it can be characterized by the axioms:

(A1) $(p_1 + p_2) + p_3 = p_1 + (p_2 + p_3)$,
(A2) $p_1 + p_2 = p_2 + p_1$,
(A3) $p + p = p$,
(A4) $p + \text{Nil} = p$.

DEFINITION 3. Consider the function $|\ | \in P(A) \to L\langle A\rangle$ recursively defined by

$$
\begin{aligned}
&- |\,\mathrm{Nil}\,| = [\mathrm{false}]\\
&- |\,ap\,| = \langle a \wedge |p|\rangle \wedge [a \wedge |p|]\\
&- |\,p_1 + p_2| = A_1 \wedge A_2 \wedge [B_1 \vee B_2], && \text{if } |\,p_i| \text{ is of the form } A_i \wedge [B_i]\\
&\qquad\qquad && \text{with } A_i \text{ of the form } \textstyle\bigwedge_{i\in J}\langle f_i\rangle.\\
&\qquad = |\,p_1| && \text{if } \ |\,p_2| = [\mathrm{false}]\\
&\qquad = |\,p_2| && \text{if } \ |\,p_1| = [\mathrm{false}].
\end{aligned}
$$

It can easily be shown that $|\ |$ is a function associating with any term p a formula $|p|$ of the general form,

$$
|\,p| = [\mathrm{false}]
$$

$$
= \bigwedge_{i\in I} \langle a_i \wedge |\,p_i|\rangle \left[\bigvee_{i\in I} a_i \wedge |\,p_i|\right], \text{ where } I \text{ is a finite set of indices.}
$$

EXAMPLE 1. Computation of $|\,p|$ for $p = a\,\mathrm{Nil} + c(a\,\mathrm{Nil} + b\,\mathrm{Nil})$,

$$
\begin{aligned}
&|\,a\,\mathrm{Nil}\,| = \langle a[\mathrm{false}]\rangle[a[\mathrm{false}]]\\
&|\,b\,\mathrm{Nil}\,| = \langle b[\mathrm{false}]\rangle[b[\mathrm{false}]]\\
&|\,a\,\mathrm{Nil} + b\,\mathrm{Nil}\,| = \langle a[\mathrm{false}]\rangle\,\langle b[\mathrm{false}]\rangle[a[\mathrm{false}] \vee b[\mathrm{false}]]\\
&|\,c(a\,\mathrm{Nil} + b\,\mathrm{Nil})| = \langle c\,|\,a\,\mathrm{Nil} + b\,\mathrm{Nil}\,|\rangle\,[c\,|\,a\,\mathrm{Nil} + b\,\mathrm{Nil}\,|\,]\\
&|\,a\,\mathrm{Nil} + c(a\,\mathrm{Nil} + b\,\mathrm{Nil})| = \langle a[\mathrm{false}]\rangle\langle c|\,a\,\mathrm{Nil} + b\,\mathrm{Nil}\,|\rangle[c\,|\,a\,\mathrm{Nil} + b\,\mathrm{Nil}\,|\\
&\qquad \vee a[\mathrm{false}]].
\end{aligned}
$$

The following theorem shows that the formula $|\,p|$ corresponding to a term p characterizes the equivalence class of p.

THEOREM 1. *For any terms p, p' of $P(A)$, $p' \models |\,p|$ iff $p' \sim p$.*

Proof. Proving this theorem amounts to proving the following three propositions:

(P1) $p \models |\,p|$,

(P2) $p' \models |\,p|$ implies $p' \sim p$,

(P3) $p' \sim p$ implies $|\,p'| \equiv |\,p|$.

(P1) By induction on the structure of the terms of $P(A)$:

— $\mathrm{Nil} \models [\mathrm{false}]$ by property 2a).

— $p \models |\,p|$ implies $ap \models \langle a\,|\,p\,|\rangle[a|\,p\,|\,]$ by Property 2(b), implies $ap \models |\,ap|$ by Definition 3.

— $p \models |p|$, where $|p| = \bigwedge_{i \in I} \langle a_i | p_i | \rangle [\bigvee_{i \in I} a_i | p_i |]$, and $p' \models |p'|$, where $|p'| = \bigwedge_{i \in J} \langle b_i | p'_i | \rangle [\bigvee_{i \in J} b_i | p'_i |]$ implies $p + p' \models \bigwedge_{i \in I} \langle a_i | p_i | \rangle \bigwedge_{i \in J} \langle b_i | p'_i | \rangle [\bigvee_{i \in I} a_i | p_i | \vee \bigvee_{i \in J} b_i | p'_i |]$, by Properties 2(c) and 2(d) which implies $p + p' \models |p + p'|$ by Definition 3.

(P2) The proof is done by induction on the structure of the formulas $|p|$:

— $p \models [\text{false}]$ implies $\nexists\, p' \in P(A)\ \nexists a \in A\ p \to^a p'$, implies $p \sim \text{Nil}$.

— Consider a formula $|p|$ such that $\forall\, p' \in P(A)\ p' \models |p|$ implies $p' \sim p$. Then, for any term $p_1 \in P(A)$, $p_1 \models |ap|$ implies $p_1 \models \langle a | p | \rangle [a | p |]$ by Definition 3,

implies $\exists\, p_2 (p_1 \to^a p_2$ and $p_2 \models |p|)$ and $\forall\, p_2\ \forall b (p_1 \to^b p_2$ implies $b = a$ and $p_2 \models |p|)$,

implies $\exists\, p_2 (p_1 \to^a p_2$ and $p_2 \sim p)$ and $\forall\, p_2\ \forall b (p_1 \to^b p_2$ implies $b = a$ and $p_2 \sim p)$,

implies $p_1 \sim ap$ by Definition 2;

— A similar proof can be done for $|p_1 + p_2|$.

(P3) It is easy to verify that $|\ |$ preserves the axioms (A1)–(A4), that is for any instance of an axiom of the form $p = p'$ we have $|p| \equiv |p'|$. As (A1)–(A4) is a complete axiomatization of $\sim$, we obtain the result. ∎

III.2. *Observational Congruence*

In the rest of the paper we give results characterizing the observational congruence $\simeq$ of CCS. In this case the set of the terms on an alphabet A containing a special symbol τ is considered; τ represents a hidden or unobservable action. As in the previous section we define a function $|\ | \in P(A) \to L\langle A \rangle$ associating with a term p a formula $|p|$ satisfied by all the terms observationally congruent to p. We recall below the definition and some important properties of $\simeq$ given in Milner; Hennessy and Milner (1980).

DEFINITION 4. (a) For $s = s_0 \cdots s_n$ a sequence of A^*, write

$$p \xrightarrow{s} p' \text{ iff } \exists\, p_1 \cdots p_n \in P(A)\ p \xrightarrow{s_0} p_1 \cdots p_n \xrightarrow{s_n} p'.$$

(b) For s a sequence of $(A - \{\tau\})^*$, write

$$p \overset{s}{\Rightarrow} p' \quad \text{iff} \quad p \xrightarrow{\tau^* s_0 \tau^* \cdots s_n \tau^*} p' \text{ if } s = s_0 \cdots s_n$$

$$\text{iff} \quad p \xrightarrow{\tau^*} p' \text{ if } s = \varepsilon \text{ the empty word of } A^*.$$

(c) The observational equivalence $\cong = \bigcap_{k=0}^{\infty} \cong^k$, where

— $p \cong^0 p'$ for any $p, p' \in P(A)$,

— $p \cong^{k+1} p'$ if $\forall s \in (A - \{\tau\})^*$
$[p \Rightarrow^s p_1$ implies $\exists p_1'(p' \Rightarrow^s p_1'$ and $p_1 \cong^k p_1'))$ and
$(p' \Rightarrow^s p_1'$ implies $\exists p_1(p \Rightarrow^s p_1$ and $p_1 \cong^k p_1'))]$.

It is shown that $\cong$ is an equivalence relation. Denote by $\simeq$ the greatest congruence on $P(A)$ such that $\simeq \subseteq \cong$ Milner (1980).

In Hennessy and Milner a slightly different definition of observational equivalence has been introduced, by taking $s \in (A - \{\tau\})$ instead of $s \in (A - \{\tau\})^*$ in Definition 4c.

Furthermore, a complete axiomization has been given for the congruence relation induced. By using these results, it is easy to deduce that the following is a complete axiomatization of $\simeq$ on $P(A)$.

(A1)–(A4) as defined in III.1,

(A5) $a\tau p = ap$,

(A6) $\tau p + p = \tau p$,

(A7) $a(p_1 + \tau p_2) + ap_2 = a(p_1 + \tau p_2)$.

We do not consider the parallel composition operator $\|$, as it is not primitive in the case of finite terms.

PROPERTIES 3 (Hennessy and Milner (1980)).

(a) $\tau(p_1 + p_2) + p_1 = \tau(p_1 + p_2)$.

(b) $p \cong p'$ iff $p \simeq p'$ or $p \simeq \tau p'$ or $\tau p \simeq p'$.

III.2.1. *Translation of a Term into its Characteristic Formula.* The following definitions are used to introduce the function $|\ |$ translating terms into their characteristic formulas.

DEFINITION 5. For the class of the formulas $f = \bigwedge_{i \in I} \langle a_i \wedge f_i \rangle \wedge [\bigvee_{i \in K} a_i \wedge f_i]$ such that the f_i's belong to $L\langle A \rangle$ and $\not\models f \equiv$ false, define $\hat{f}$ as the formula $\hat{f} := \bigvee_{i \in K} a_i \wedge f_i$.

PROPOSITION 1. $\hat{}$ *is a partial function from* $L\langle A \rangle$ *into* $L(A)$.

Proof. Suppose that for some formula f of $L\langle A \rangle$ we have,

$$f \equiv f_1 = \bigwedge_{i \in I_1} \langle a_1 f_i \rangle \left[\bigvee_{i \in K_1} a_i f_i \right] \tag{1}$$

and

$$f \equiv f_2 = \bigwedge_{i \in I_2} \langle b_1 f_1' \rangle \left[\bigvee_{i \in K_2} b_i f_i' \right] \tag{2}$$

We have to prove that

$$\forall t \in T(A)\ \forall q \in Q_t\ (t, q \models \hat{f}_1 \text{ iff } t, q \models \hat{f}_2) \tag{3}$$

Let us first show that

$$(1) \text{ and } (2) \text{ imply } [\hat{f}_1] \equiv [\hat{f}_2] \tag{4}$$

As f is not equivalent to false, there exists a tree t such that $t \models f$. Suppose that for some tree t', $t' \models [\hat{f}_1]$. Then by property (2c) and (2d) $t + t' \models f_1$. Thus, $t + t' \models f_2$ which implies $t + t' \models [\hat{f}_2]$. Then by property $(2f)$ we have $t' \models [\hat{f}_2]$ and consequently by symmetry the proof of (4). We show that (4) implies (3). Suppose that for some $t \in T(A)$ and $q \in Q_t$ $t, q \models \bigvee_{i \in K_1} a_i f_i$. This implies $\exists q' \in Q_t$, $q' \to^{a_i} q$ and $t, q \models f_i$ for an $i \in K_1$. As $f_i \in L\langle A \rangle$ we have for the subtree t_q of t, $t_q \models f_i$. This

implies $a_i t_q \models [a_i f_i]$ by property (2b),
implies $a_i t_q \models [\bigvee_{i \in K_1} a_i f_i]$,
implies $a_i t_q \models [\bigvee_{i \in K_2} b_i f_i']$ by (4),
implies $\exists j \in K_2$ such that $a_i = b_j$ and $t_q \models f_j'$,
implies $t, q \models b_j f_j'$ as $q' \to^{a_i} q$ in t,

thus $t, q \models \bigvee_{i \in K_2} b_j f_j'$. ∎

COROLLARY 1. *For two formulas of* $L\langle A \rangle$, $f_1 = \bigwedge_{i \in I_1} \langle a_i \wedge f_i \rangle [\bigvee_{i \in K_1} a_i \wedge f_i]$ *and* $f_2 = \bigwedge_{i \in I_2} \langle b_i \wedge f_i' \rangle [\bigvee_{i \in K_2} b_i \wedge f_i']$ *such that* $\not\models f_1 \equiv$ *false*, $f_1 \equiv f_2$ *implies* $\bigwedge_{I_1} \langle a_i f_i \wedge \hat{f}_1 \rangle \equiv \bigwedge_{I_2} \langle b_i f_i' \wedge \hat{f}_2 \rangle$ *and* $[\bigvee_{K_1} a_i f_i] \equiv [\bigvee_{K_2} b_i f_i']$. ∎

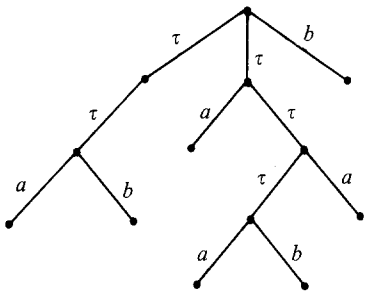
Notice that if for some $p \in P(A)$ $p \models f$ then $\hat{f}$ is such that $p' \models [\hat{f}]$ implies $p + p' \models f$. That is, $[\hat{f}]$ characterizes a class of terms such that their addition to p preserves satisfaction of f.

DEFINITION 6. Let f be a formula such that $\hat{f}$ is defined. Denote by $E(f)$ the formula, $E(f) := \mu x.\ (f \vee \langle \tau \wedge x \rangle \wedge [\tau \wedge x \vee \hat{f}])$.

PROPOSITION 2. $E(f) \equiv \bigvee_{k \in \mathbb{N}} X_k$, *where* $X_0 = f$ *and* $X_{k+1} = X_k \vee \langle \tau \wedge X_k \rangle \wedge [\tau \wedge X_k \vee \hat{f}]$.

Proof. As the trees representing the terms of $P(A)$ are of finite degree, the functional $\lambda x \cdot \langle \tau x \rangle [\tau x \vee \hat{f}]$ is continuous. The result is obtained by application of the Knaster–Tarski theorem. ▮

The interest of defining $E(f)$ will become evident later when it is proved that if f represents a congruence class of a term p then $E(f)$ represents the union of the congruence classes of p and of τp. For example, if $p = a\,\mathrm{Nil} + b\,\mathrm{Nil}$ then the following tree, presenting a term congruent to $\tau(a\,\mathrm{Nil} + b\,\mathrm{Nil})$, satisfies $E(f)$.



We define a function $|\ |\in P(A) \to L\langle A \rangle$ such that for any pair of terms p, p' of $P(A)$, $p' \models |p|$ iff $p' \simeq p$.

Notice that for such a function $|\ |$ the following three propositions hold:

A. $\forall p \in P(A)\ p \models |p|$ (satisfaction),

B. $\forall p, p' \in P(A)\ |p| \equiv |p'|$ implies $p \simeq p'$ (soundness),

C. $\forall p, p' \in P(A)\ p \simeq p'$ implies $|p| \equiv |p'|$ (completeness).

The definition is given inductively by the following four rules. A subset STRICT is also defined in order to make easier the expression of the rules. STRICT is the set obtained by the rules given below and represents the set of formulas corresponding to terms p which are not congruent to some term of the form $\tau p'$.

RULE 1. $-|\mathrm{Nil}| = [\mathit{false}]$;

$-[\mathit{false}] \in \mathrm{STRICT}$.

Notice that $\mathrm{Nil} \models [\mathrm{false}]$ by Property (2a).

RULE 2. $-|\tau p| = \tau^\circ |p|$ *if* $|p| \in \mathrm{STRICT}$

$-|\tau p| = |p|$ *otherwise,*

where $\tau^\circ |p| = \langle \tau \wedge E|p| \rangle \wedge [\tau \wedge E|p| \vee |\hat{p}|]$;

$-|\tau p| \notin \mathrm{STRICT}$.

The reader is invited to compare this rule with the corresponding rule in the case of strong equivalence which is $|\tau p| = \langle \tau \wedge |p| \rangle [\tau \wedge |p|]$. In Rule 2 we have replaced $|p|$ by $E|p|$ in order to take into account (A5). The formula $|\hat{p}|$ has been added to preserve satisfaction for terms congruent to p by Property (3a) (take $p = p_1 + p_2$).

RULE 3. *For* $a \in A - \{\tau\}$

— $|ap| = a^\circ |p'|$ *if there exists* p' *such that* $|p| \equiv \tau^\circ |p'|$

— $|ap| = a^\circ |p|$ *otherwise,*

where $a^\circ |p| = \langle a \wedge E|p| \rangle \wedge [a \wedge E|p|[a/\tau]]$ *and*

$$|\hat{p}|\,[a/\tau] = \bigvee_{i \in I'} a \wedge f_i \qquad \text{whenever } |\hat{p}| \equiv \bigvee_{i \in I} a_i \wedge f_i \text{ and}$$

$$I' = \{i \in I \mid a_i = \tau\} \neq \varnothing$$

$$= \mathit{false} \qquad \text{if } |\hat{p}| \equiv \mathit{false} \text{ or } I' = \varnothing$$

— $|ap| \in$ STRICT.

It is interesting to compare this rule with the corresponding rule in the case of strong equivalence, which is $|ap| = \langle a \wedge |p| \rangle [a \wedge |p|]$. In Rule 3, $|p|$ is replaced by $E|p|$ to take into account (A5). The formula $|\hat{p}|[a/\tau]$ has been added to preserve satisfaction for terms congruent to ap by application of (A7). In fact, for $p = p_1 + \tau p_2$ one gets $ap \simeq ap + ap_2$. The formula added caracterizes all terms ap_2 such that $ap \simeq ap + ap_2$ by (A7). Finally, notice that in the case where $|p| \equiv \tau^\circ |p'|$, using $|p'|$ instead of $|p|$ is necessary in order to preserve (A5).

RULE 4. — $|p_1 + p_2| = |p_1|$ *if* $|p_2| \equiv [\mathit{false}]$

— $|p_1 + p_2| = |p_2|$ *if* $|p_1| \equiv [\mathit{false}]$

— $|p_1 + p_2| = |p_1| \oplus |p_2|$ *otherwise where for*

$$|p_1| = \bigwedge_{i \in I_1} \langle a_i \wedge E|p_i| \rangle \left[\bigvee_{i \in I_1} \widehat{a_i^\circ |p_i|} \right],$$

$$|p_2| = \bigwedge_{i \in I_2} \langle b_i \wedge E|p_i'| \rangle \left[\bigvee_{i \in I_2} \widehat{b_i^\circ |p_i'|} \right],$$

$$|p_1| \oplus |p_2| = \bigwedge_{i \in I_1'} \langle a_i \wedge E|p_i| \rangle \bigwedge_{i \in I_2'} \langle b_i \wedge E|p_i'| \rangle [|\hat{p}_1| \vee |\hat{p}_2|].$$

The sets of indices I_1' and I_2' are defined by

$$I_1' = \{i \in I_1 \mid \nexists\, j \in I_2 c(a_i p_i, b_j p_j')\}, \qquad I_2' = \{j \in I_2 \mid \nexists\, i \in I_1 c(b_j p_j', a_i p_i)\},$$

where c is the predicate:

$$c(ap, bp') \text{ iff } [\widehat{a^\circ | p|}] \supset [\widehat{b^\circ | p|}] \text{ and not } [\widehat{a^\circ | p|}] \equiv [\widehat{b^\circ | p|}];$$

$$-|p_1| \oplus |p_2| \notin \text{STRICT iff } |p_1| \oplus |p_2| \equiv \tau^\circ |p| \text{ for some } |p|.$$

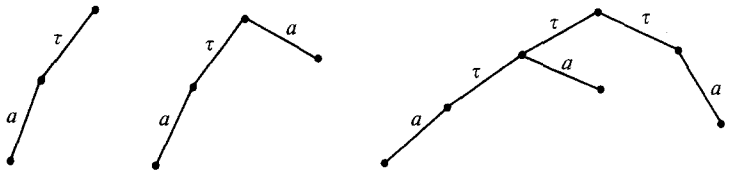
It is shown that $|p| = \bigwedge_{i \in I} \langle a_i \wedge E | p_i | \rangle [\widehat{\bigvee_{i \in I} a_i^\circ | p_i|}]$ is the most general form of the formulas of the image of $|\ |$ for $p = \sum_{i \in I} a_i p_i$. A comparison between this rule and the corresponding rule in the case of strong equivalence shows that the same principle is applied with the difference that a factor may be "eliminated" to take into account (A6) and (A7). The predicate $c(ap, bp')$ has been defined so that it is true whenever $ap + bp' \simeq bp'$ by these axioms but not $ap \simeq bp'$.

EXAMPLE 2. — The formula representing the congruence class of a Nil is $|a \text{ Nil}| = \langle a \wedge E[\text{false}] \rangle [a \wedge E[\text{false}]]$. It characterizes all the processes starting only with a-transitions followed by an arbitrary number of τ-transitions.

— The formula representing the congruence class of τa Nil is

$$|\tau a \text{ Nil}| = \langle \tau \wedge E | a \text{ Nil} | \rangle [\tau \wedge E | a \text{ Nil}| \vee |a \text{ Nil}|]$$
$$= \langle \tau \wedge E | a \text{ Nil} | \rangle [\tau \wedge E | a \text{ Nil}| \vee a \wedge E[\text{false}]].$$

It characterizes all the processes which have at least one starting τ-transition leading to a process satisfying $E | a \text{ Nil}|$ and which can have starting a-transitions leading to $E | \text{Nil}|$; these are the processes congruent to τa Nil, such as



— The formula for $\tau a \text{ Nil} + a \text{ Nil}$ is $|\tau a \text{ Nil}| \oplus |a \text{ Nil}|$. We have

$$|\tau a \text{ Nil}| = \langle \tau \wedge E | a \text{ Nil} | \rangle [\tau \wedge E | a \text{ Nil}| \vee a \wedge E[\text{false}]] \text{ and,}$$
$$|a \text{ Nil}| = \langle a \wedge E[\text{false}] \rangle [a \wedge E[\text{false}]].$$

The predicate c defined in Rule 4 evaluates to $c(a \text{ Nil}, \tau a \text{ Nil}) = |a \text{ Nil}| \supset |\tau a \text{ Nil}| = \text{true}$. So, we get the result $|\tau a \text{ Nil}| \oplus |a \text{ Nil}| = \langle \tau \wedge E | a \text{ Nil} | \rangle [\tau \wedge E | a \text{ Nil}| \vee a \wedge E[\text{false}]] = |\tau a \text{ Nil}|$. In fact $\tau a \text{ Nil} + a \text{ Nil}$ is congruent to τa Nil due to (A6).

— Computation of $|p|$ for $p = a\,\mathrm{Nil} + \tau(a\,\mathrm{Nil} + b\,\mathrm{Nil})$:

$$|a\,\mathrm{Nil}| = \langle aE[\mathrm{false}]\rangle[aE[\mathrm{false}]]$$

$$|b\,\mathrm{Nil}| = \langle bE[\mathrm{false}]\rangle[bE[\mathrm{false}]]$$

$$|a\,\mathrm{Nil} + b\,\mathrm{Nil}| = \langle aE[\mathrm{false}]\rangle\langle bE[\mathrm{false}]\rangle[aE[\mathrm{false}] \vee bE[\mathrm{false}]]$$

$$|\tau(a\,\mathrm{Nil} + b\,\mathrm{Nil})| = \langle \tau E|\, a\,\mathrm{Nil} + b\,\mathrm{Nil}|\rangle[\tau E|\, a\,\mathrm{Nil} + b\,\mathrm{Nil}| \vee aE[\mathrm{false}] \vee bE[\mathrm{false}]]$$

$$|a\,\mathrm{Nil} + \tau(a\,\mathrm{Nil} + b\,\mathrm{Nil})| = \langle \tau E|\, a\,\mathrm{Nil} + b\,\mathrm{Nil}|\rangle[\tau E|\, a\,\mathrm{Nil} + b\,\mathrm{Nil}| \vee aE[\mathrm{false}] \vee bE[\mathrm{false}]].$$

The absence of the factor $\langle aE[\mathrm{false}]\rangle$ in the result is due to the fact that $c(a\,\mathrm{Nil}, \tau(a\,\mathrm{Nil} + b\,\mathrm{Nil}))$ is satisfied, i.e.,

$$[aE[\mathrm{false}]] \supset [|\widehat{\tau(a\,\mathrm{Nil} + b\,\mathrm{Nil})}|] \text{ but not } [aE[\mathrm{false}]]$$
$$\equiv [|\widehat{\tau(a\,\mathrm{Nil} + b\,\mathrm{Nil})}|].$$

PROPOSITION 3. *| | is a function from $P(A)$ into $L\langle A\rangle$.*

Proof. It is easy to prove by structural induction that the general form of the formulas of the image of | | is $|p| = \bigwedge_{i\in I}\langle a_i E|\, p_i|\rangle[\bigvee_{i\in I} a_i^\circ|\, p_i|]$ or $|p| = [\mathrm{false}]$. Thus | | is total.

To prove that | | is a function it remains to prove that if $|p| \equiv \tau^\circ|\, p'| \equiv \tau^\circ|\, p''|$ then $a^\circ|\, p'| \equiv a^\circ|\, p''|$, as it is the only case where the uniqueness of the image is not evident.

Suppose that for some p', p'', $\tau^\circ|\, p'| \equiv \tau^\circ|\, p''|$. We have $\tau^\circ|\, p'| = \langle \tau E|\, p'|\rangle[\tau E|\, p'| \vee |\hat{p}'|]$ and $\tau^\circ|\, p''| = \langle \tau E|\, p''|\rangle[\tau E|\, p''| \vee |\hat{p}''|]$. By the hypothesis and corollary of Proposition 1 we have $\langle \tau E|\, p'|\rangle \equiv \langle \tau E|\, p''|\rangle$, which implies $\langle aE|\, p'|\rangle \equiv \langle aE|\, p''|\rangle$ (1). Furthermore, $[\tau E|\, p'| \vee |\hat{p}'|] \equiv [\tau E|\, p''| \vee |\hat{p}''|]$ by Proposition 1,

implies $[\tau E|\, p'| \vee \tau|\, \hat{p}'|] \equiv [\tau E|\, p''| \vee \tau|\, \hat{p}''|]$,

implies $[aE|\, p'| \vee |\hat{p}'|[a/\tau]] \equiv [aE|\, p''| \vee |\hat{p}''|[a/\tau]]$,

equivalent to $[\widehat{a^\circ|\, p'|}] \equiv [\widehat{a^\circ|\, p''|}]$. Thus with (1) $a^\circ|\, p'| \equiv a^\circ|\, p''|$. ∎

LEMMA 1. *For any term of $P(A)$, $|p| \notin$ STRICT iff $\exists\, p'|\, p| \equiv \tau^\circ|\, p'|$.*

Proof. By the fact that $\tau^\circ|\, p'| \notin$ STRICT and by application of the Rules 1 and 3 it is not possible to obtain a formula $|p| \equiv \tau^\circ|\, p'|$ for some p'. ∎

THEOREM 2 (satisfaction). $\forall p \in P(A)\ p \models |p|$.

Proof. By induction on the structure of $P(A)$:

1. $\mathrm{Nil} \models [\mathrm{false}]$ by Property 2(a).

2. Let $|p|$ be a formula such that $p \models |p|$.

2.1. If $|p| \in \mathrm{STRICT}$ then $|\tau p| = \tau^\circ |p|$. We have $p \models |p|$ implies $\tau p \models \langle \tau | p | \rangle [\tau | p |]$ by property 2(b),

implies $\tau p \models \langle \tau E | p | \rangle [\tau E | p | \vee | \hat{p} |]$ by $|p| \supset E | p |$,
implies $\tau p \models \tau^\circ | p |$.

2.2. If $|p| \notin \mathrm{STRICT}$ then $\exists p' |p| \equiv \tau^\circ |p'|$ and by hypothesis $p \models \tau^\circ |p'|$. Let G be the function $\lambda x \cdot \langle \tau x \rangle [\tau x \vee |\hat{p}|]$. We have $\tau^\circ |p'| = G(E|p'|)$ and $E|p'| \equiv |p'| \vee G(E|p'|)$ by Definition 6. From $p \models \tau^\circ |p'|$ we obtain, $p \models E|p'|$ because $\tau^\circ |p'| \supset E|p'|$,

implies $\exists k \in \mathbb{N}\ p \models X_k$ where X_k is defined as in Proposition 2, by taking $X_0 = |p'|$,
implies $\tau p \models G(X_k)$ by Property 2(b),
implies $\tau p \models G(E|p'|)$ by $X_k \supset E|p'|$,
implies $\tau p \models \tau^\circ |p'|$.

3. Let $|p|$ be a formula such that $p \models |p|$.

3.1. If $|p| \in \mathrm{STRICT}$ then $|ap| = a^\circ |p|$ and the proof can be carried out exactly as in 2.1.

3.2. If $|p| \notin \mathrm{STRICT}$ then $\exists p'\ |p| \equiv \tau^\circ |p'|$. Then $|ap| = a^\circ |p'|$. We have $p \models \tau^\circ |p'|$,

implies $p \models E|p'|$ because $\tau^\circ |p'| \supset E|p'|$,
implies $ap \models \langle aE|p'| \rangle [aE|p'| \vee |p'|[a/\tau]]$ by Property 2(b),
implies $ap \models a^\circ |p'|$.

4. Let p_1 and p_2 be two terms of $P(A)$ such that $p_1 \models |p_1|$ and $p_2 \models |p_2|$. If $p_1 = \mathrm{Nil}$ or $p_2 = \mathrm{Nil}$ then $p_1 + p_2 \models |p_1| \oplus |p_2|$. Otherwise, take $|p_1| = \bigwedge_{i \in I_1} \langle a_i E | p_i | \rangle [|\hat{p}_1|]$ and $|p_2| = \bigwedge_{i \in I_2} \langle b_i E | p_i' | \rangle [|\hat{p}_2|]$. We have $p_1 + p_2 \models f$, where $f = \bigwedge_{i \in I_1} \langle a_i E | p_i | \rangle \bigwedge_{i \in I_2} \langle b_i E | p_i' | \rangle [|\hat{p}_1| \vee |\hat{p}_2|]$ anf $f \supset |p_1| \oplus |p_2|$. ∎

III.2.2. *Soundness of the Translation Method.* The soundness of the translation method will be deduced from a series of lemmas given below which have all the same hypothesis, the induction hypothesis used in the proof of Proposition 4.

Let F be a set of formulas of the image of $|\ |$ such that

(1) $\forall |p| \in F, \forall p' \in P(A)\ |p'|$ subformula of $|p|$ implies $|p'| \in F$.

(2) $\forall |p| \in F, \forall p' \in P(A)\ p' \models |p|$ implies $p' \simeq p$.

The following lemmas give properties of F.

LEMMA 2. $\forall |p| \in F, \forall p' \in P(A)\ p' \models [|\hat{p}|]$ *implies* $p + p' \simeq p$.

Proof. Let p', such that $p' \models [|\hat{p}|]$. From Corollary 1 and Theorem 2, we get $p + p' \models |p|$. Thus by induction hypothesis $p + p' \simeq p$. ∎

LEMMA 3. $\forall |p| \in F, \forall p' \in P(A)\ p' \models E|p|$ *implies* $p' \simeq p$ *or* $p' \simeq \tau p$.

Proof. From Proposition 2 we have $E|p| = \bigvee_{i=0}^{\infty} Y_i$, where $Y_0 = |p|$ and $Y_{k+1} = G(\bigvee_{i \leqslant k} Y_i)$ for $k \geqslant 0$ and $G = \lambda x \cdot \langle \tau x \rangle [\tau x \vee |\hat{p}|]$.

Proof by Induction. For $k = 0$ $p' \models \bigvee_{i \leqslant k} Y_i$ is equivalent to $p' \models |p|$, i.e., $p' \simeq p$. Suppose that for some k, $p' \models \bigvee_{i \leqslant k} Y_i$ implies $p' \simeq p$ or $p' \simeq \tau p$. From $p' \models \bigvee_{i \leqslant k+1} Y_i$ we deduce $p' \simeq p$ or $p' \simeq \tau p$ if $p' \models \bigvee_{i \leqslant k} Y_i$. Otherwise, $p' \models Y_{k+1}$ is equivalent to $p' \models \langle \tau(\bigvee_{i \leqslant k} Y_i) \rangle [\tau(\bigvee_{i \leqslant k} Y_i) \vee |\hat{p}|]$. This implies

(a) $\exists p_0\, p' \to^{\tau} p_0$ and $p_0 \models \bigvee_{i \leqslant k} Y_i$ and by induction hypothesis $p_0 \simeq p$ or $p_0 \simeq \tau p$.

(b) $\forall p_i\, p' \to^{a_i} p_i$ implies ($a_i = \tau$ and $p_i \models \bigvee_{i \leqslant k} Y_i$ or $a_i p_i \models [|\hat{p}|]$).

From (b) we deduce $a_i p_i \simeq \tau p$ or $a_i p_i + p \simeq p$ (by Lemma 2). Thus, p' is of the form $p' = \tau p_0 + \sum_i a_i p_i$, where, $\sum_i a_i p_i + \tau p \simeq \sum_i a_i p_i + p + \tau p \simeq \tau p$ and $\tau p_0 \simeq \tau p$. Consequently $p' \simeq \tau p + \sum_i a_i p_i \simeq \tau p$. ∎

LEMMA 4. $\forall |p| \in F, \forall p' \in P(A)\ p' \models \tau^{\circ}|p|$ *implies* $p' \simeq \tau p$.

Proof. We use the notation of the proof of Lemma 3. $p' \models \tau^{\circ}|p|$ is equivalent to $p' \models G(E|p|)$ (by Rule 2), which implies $p' \models G(\bigvee_{i=0}^{\infty} Y_i)$. As G is continuous, we have $p' \models \bigvee_{j=0}^{\infty} G(\bigvee_{i \leqslant j} Y_i)$ equivalent to $\exists k \in \mathbb{N}$, $p' \models G(\bigvee_{i \leqslant k} Y_i)$. Thus, $p' \models Y_{k+1}$ which implies $p' \simeq \tau p$ by the proof of Lemma 3. ∎

LEMMA 5. $\forall |p| \in F, \forall p' \in P(A)\ p' \models a^{\circ}|p|$ *implies* $p' \simeq ap$.

Proof. $p' \models a^{\circ}|p|$ is equivalent to $p' \models \langle aE|p| \rangle [aE|p| \vee |\hat{p}|[a/\tau]]$. From $p' \models a^{\circ}|p|$ we get

(a) $\exists p_0\, p' \to^{a} p_0$ and $p_0 \models E|p|$, which implies $p_0 \simeq p$ or $p_0 \simeq \tau p$ by Lemma 3, which implies $ap_0 \simeq ap$ by (A5).

(b) $\forall p_i\, p' \to^{a_i} p_i$ implies $a_i = a$ and ($p_i \models E|p|$ or $ap_i \models [|\hat{p}|[a/\tau]]$). From $p_i \models E|p|$ we obtain $p_i \simeq p$ or $p_i \simeq \tau p$, which implies $ap_i \simeq ap$; from $ap_i \models [|\hat{p}|[a/\tau]]$ we obtain $\tau p_i \models [|\hat{p}|]$, and by Lemma 2 $p + \tau p_i \simeq p$, which implies $ap + ap_i \simeq a(p + \tau p_i) + ap_i \simeq a(p + \tau p_i) \simeq ap$ by (A7).

From (a) and (b) we deduce that p' is of the form $p' = ap_0 + \sum_i ap_i$, where $ap_i \simeq ap$ or $ap + ap_i \simeq ap$. Thus $p' \simeq ap + \sum_i ap_i \simeq ap$. ▮

LEMMA 6. $\forall |p_1|, |p_2| \in F$, $[|\hat{p}_1|] \equiv [|\hat{p}_2|]$ *implies* $p_1 \simeq p_2$.

Proof. From $p_i \models [|\hat{p}_i|]$ deduce that $p_1 \models [|\hat{p}_2|]$ and $p_2 \models [|\hat{p}_1|]$. By using Lemma 2 we obtain $p_2 + p_1 \simeq p_2$ and $p_1 + p_2 \simeq p_1$. Thus $p_1 \simeq p_2$. ▮

LEMMA 7. *For* $|p_1|$, $|p_2| \in F$, $p \in P(A)$ $p \models |p_1| \oplus |p_2|$ *implies* $p \simeq p_1 + p_2$.

If $|p_1| \equiv [\text{false}]$ or $|p_2| \equiv [\text{false}]$ the proof is trivial. Otherwise $|p_1|$ and $|p_2|$ are of the form,

$$|p_1| = \bigwedge_{i \in I} \langle a_i E \,|\, p_i| \rangle \left[\bigvee_{i \in I} \widehat{a_i^\circ \,|\, p_i|} \right]$$

and

$$|p_2| = \bigwedge_{i \in J} \langle b_i E \,|\, p_i'| \rangle \left[\bigvee_{i \in J} \widehat{b_i^\circ \,|\, p_i'|} \right],$$

such that

$$|p_1| \oplus |p_2| = \bigwedge_{i \in I'} \langle a_i E \,|\, p_i| \rangle \bigwedge_{i \in J'} \langle b_i E \,|\, p_i'| \rangle [|\hat{p}_1| \vee |\hat{p}_2|],$$

where

$$I' = \{i \in I \,|\, \nexists\, j \in J'\ c(a_i p_i, b_j p_j')\} \text{ and } J' = \{j \in J \,|\, \nexists\, i \in I'\ c(b_j p_j', a_i p_i)\}.$$

From $\sum_{i \in I} a_i p_i \models |p_1|$ and $\sum_{i \in J} b_i p_i' \models |p_2|$ and $|p_1|, |p_2| \in L_0$ we have

$$\sum_{i \in I} a_i p_i + \sum_{i \in J} b_i p_i' \simeq p_1 + p_2.$$

Suppose that for some p, $p \models |p_1| \oplus |p_2|$. This implies

1. $\forall i \in I'\ \exists\, \bar{p}_i\ p \to^{a_i} \bar{p}_i$ and $\bar{p}_i \models E\,|p_i|$, i.e., $a_i \bar{p}_i \simeq a_i p_i$ as in the Proof of Lemma 5.

2. $\forall i \in J' \exists\, \bar{p}_i'\ p \to^{b_i} \bar{p}_i'$ and $\bar{p}_i' \models E\,|p_i|$, i.e., $b_i \bar{p}_i' \simeq b_i p_i'$.

3. $\forall p_i''\ p \to^{c_i} p_i''$ implies $c_i p_i'' \models [|\hat{p}_1|]$ or $c_i p_i'' \models [|\hat{p}_2|]$, i.e., $p_1 + p_2 + c_i p_i'' \simeq p_1 + p_2$ by Lemma 2.

Furthermore, $\forall i \in I - I'\ \exists j \in J'$ such that $[\widehat{a_i^\circ \,|\, p_i|}] \supset [\widehat{b_j^\circ \,|\, p_j'|}]$. Thus

$a_i p_i \models [b_j^\circ \mid p_j' \mid]$ and by Lemma 2 $b_j p_j' + a_i p_i \simeq b_j p_j'$. Symmetrically, $\forall j \in J - J'\ \exists i \in I'$ such that $a_i p_i + b_j p_j' \simeq a_i p_i$. From 1, 2, and 3 we obtain

$$p = \sum_{i \in I'} a_i \bar{p}_i + \sum_{i \in J'} b_i \bar{p}_i' + \sum_i c_i p_i'' \simeq \sum_{i \in I'} a_i p_i + \sum_{i \in J'} b_i p_i' + \sum_i c_i p_i''$$

$$\simeq \sum_{i \in I} a_i p_i + \sum_{i \in J} b_i p_i' + \sum_i c_i p_i'' \simeq p_1 + p_2 + \sum_i c_i p_i'' \simeq p_1 + p_2. \quad \blacksquare$$

PROPOSITION 4. $\forall p, p' \in P(A)\ p' \models \mid p \mid$ *implies* $p' \simeq p$.

Proof. By induction on the structure of the formulas,

(1) $p' \models [\text{false}]$ implies $p' \simeq \text{Nil}$.

(2) Let F be a set of formulas of the image of $\mid\ \mid$ such that

— $\forall \mid p \mid \in F$, $\forall p' \in P(A)$ $\mid p' \mid$ subformula of $\mid p \mid$ implies $\mid p' \mid \in F$.

— $\forall \mid p \mid \in F$, $\forall p' \in P(A)$ $p' \models \mid p \mid$ implies $p' \simeq p$.

By Lemmas 4, 5, and 7 the operations on formulas preserve this property. ∎

Now the soundness theorem follows as in III.1.

THEOREM 3 (soundness). $\forall p' \in P(A)\ \mid p' \mid \equiv \mid p \mid$ *implies* $p' \simeq p$.

Proof. $\mid p' \mid \equiv \mid p \mid$ implies $p' \models \mid p \mid$ by Theorem 2 which implies $p' \simeq p$ by Proposition 4 ∎.

III.2.3. *Completeness of the Translation Method.* As (A1)–(A7) is a complete axiomatization of the observational congruence we can proceed as in the proof of (P3) in Theorem 1.

LEMMA 8. (A1) $\mid (p_1 + p_2) + p_3 \mid \equiv \mid p_1 + (p_2 + p_3) \mid$,

(A2) $\mid p_1 + p_2 \mid \equiv \mid p_2 + p_1 \mid$,

(A3) $\mid p + p \mid \equiv \mid p \mid$,

(A4) $\mid p + \text{Nil} \mid \equiv \mid p \mid$.

Proof. The proofs of (A2), (A3) and (A4) are trivial. So it remains to prove (A1), i.e. $(\mid p_1 \mid \oplus \mid p_2 \mid) \oplus \mid p_3 \mid \equiv \mid p_1 \mid \oplus (\mid p_2 \mid \oplus \mid p_3 \mid)$. If some p_i is such that $\mid p_i \mid \equiv [\text{false}]$ then the result follows by (A4). Otherwise, each $\mid p_i \mid$ is of the general form $\mid p_i \mid = \bigwedge_j \langle a_{ij} E \mid p_{ij} \mid \rangle [\mid \hat{p}_i \mid]$. If some term of the form $\langle aE \mid p \mid \rangle$ of $\mid p_1 \mid$ is eliminated in $\mid p_1 \mid \oplus \mid p_2 \mid$ then it is eliminated in $\mid p_1 \mid \oplus (\mid p_2 \mid \oplus \mid p_3 \mid)$ because the relation defined by the predicate $c(ap, bp') = ([\mid \widehat{ap} \mid] \supset [\mid \widehat{bp'} \mid]) \wedge \neg([\mid \widehat{ap} \mid] \equiv [\mid \widehat{bp'} \mid])$ is transitive and antisymmetrical. ∎

LEMMA 9. (A5) $|a\tau p| \equiv |ap|$.

Proof. If $|p| \notin$ STRICT then $|p| \equiv \tau^\circ |p'|$ for some $|p'| \in$ STRICT. This implies $|\tau p| \equiv \tau^\circ |p'|$, which implies $|a\tau p| \equiv a^\circ |p'|$ and $|ap| \equiv a^\circ |p'|$. If $|p| \in$ STRICT then $|\tau p| = \tau^\circ |p|$ which implies $|a\tau p| = a^\circ |p|$ and $|ap| = a^\circ |p|$. Thus $|a\tau p| \equiv |ap|$. ∎

LEMMA 10. (A6) $|\tau p + p| \equiv |\tau p|$.

(A7) $|a(p_1 + \tau p_2) + ap_2| \equiv |a(p_1 + \tau p_2)|$.

Proof. The proof is done by induction on the structure of the formulas. Let K be any set of formulas of $L\langle A\rangle$ such that

(1) $|p| \in K$ implies for any subformula $|p'|$ of $|p|$, $|p'| \in K$,

(2) $a^\circ |p| \in K$ implies for any $b \in A$, $b^\circ |p| \in K$,

(3) $|p| \in K$ and $p \simeq p'$ implies $|p'| \equiv |p|$:

— $\{[\text{false}]\}$ is such a set.

— Consider a set K and show that $K' = K \cup \{|ap| \mid |p| \in K, a \in A\} \cup \{|p_1| \oplus |p_2| \mid |p_1|, |p_2| \in K\}$ satisfies (1), (2), (3).

Obviously, K' satisfies (1), (2). It remains to prove that from any instance of the axioms (A6), (A7) of the form $p_1 = p_2$ one can deduce $|p_1| \equiv |p_2|$, where $|p_1|$ and $|p_2|$ are formulas of the form $a^\circ |p|$, $\tau^\circ |p|$ and $|p| \oplus |p'|$ with $|p|, |p'| \in K$.

(a) For $|p_1|, |p_2|$ of the form $\tau^\circ |p|$ it has to be shown

(a1) $\forall |p| \in K \; |\tau p| \equiv |\tau p + p|$ (A6)

(a2) $\forall |p_2|, |p_1 + \tau p_2| \in K \; |\tau(p_1 + \tau p_2)| \equiv |\tau(p_1 + \tau p_2) + \tau p_2|$ (A7).

To establish (a1) and (a2) it is sufficient to prove that $\forall |p_3|$, $|p_1 + p_3| \in K$,

(a3) $|\tau(p_1 + p_3)| \equiv |\tau(p_1 + p_3) + p_3|$ (by taking $p_3 = \tau p_2$).

(b) For $|p_1|, |p_2|$ of the form $a^\circ |p|$, where $a \in A - \{\tau\}$ it has to be shown that $\forall |p_2|, \; |p_1 + \tau p_2| \in K \; |a(p_1 + \tau p_2)| \equiv |a(p_1 + \tau p_2) + ap_2|$ (A7).

(c) The cases where $|p_1|, |p_2|$ in instances of (A6), (A7) are of the form $|p| \oplus |p'|$ have already been considered in (a), (b).

Proof of (a3). If $|p_1 + p_3| \in K$, $|p_1 + p_3| \notin$ STRICT then $|\tau(p_1 + p_3)| \equiv |p_1 + p_3| \in K$.

If $|p_1 + p_3| = [\text{false}]$ or $|p_3| = [\text{false}]$ we deduce easily $|\tau(p_1 + p_3) + p_3| \equiv |\tau(p_1 + p_3)|$. Otherwise, $|p_3|$ is of the form $|p_3| =$

$\bigwedge_{i\in I}\langle a_iE|\,p_i|\rangle[\bigvee_{i\in I}\widehat{a_i^\circ|\,p_i|}]$ and $|\tau(p_1+p_3)|$ is of the form $|\tau(p_1+p_3)| = \langle\tau E|\,p_1+p_3|\rangle[\tau E|\,p_1+p_3|\vee|\hat{p}_1|\vee|\hat{p}_3|]$. We have $[\widehat{a_i^\circ|\,p_i|}]\supset[|\tau(p_1+p_3)|]\ \forall i\in I$. This implies

— either $c(a_ip_i,\ \tau(p_1+p_3))\ \forall i\in I$, in which case $|\tau(p_1+p_3)|\oplus|p_3|\equiv\tau(p_1+p_3)|$,

— or $\exists i\in I\ [\widehat{a_i^\circ|\,p_i|}]\equiv[\widehat{\tau^\circ|\,p_1+p_3|}]$.

Thus $a_i=\tau$ and $[\widehat{|p_1+p_3|}]=[\widehat{\tau^\circ|\,p_i|}]$. By Lemma 2 we get $p_1+p_3\simeq\tau p_i$ and from $|\,p_1+p_3|\in K$ we obtain $|\,p_1+p_3|=\tau^\circ|\,p_i|$. This contradicts the hypothesis that $|\,p_1+p_3|\in$ STRICT. ▮

Proof of (b). If $|\,p_1+\tau p_2|\in K$ and $|\,p_1+\tau p_2|\notin$ STRICT then $|\,p_1+\tau p_2|\equiv\tau^\circ\,|p'|$ for some $|\,p'|\in K$, which implies $|a(p_1+\tau p_2)|=a^\circ|\,p'|\in K$. If $|\,p_1+\tau p_2|\in$ STRICT then one can suppose without loss of generality that $|\,p_2|\in$ STRICT. We have $|a(p_1+\tau p_2)|$ is of the form

$$|a(p_1+\tau p_2)| = \langle aE|\,p_1+\tau p_2|\rangle[aE|\,p_1+\tau p_2|\vee|\hat{p}_1|[a/\tau]$$
$$\vee|\hat{p}_2|\,[a/\tau]\vee aE|\,p_2|]$$

and

$$|ap_2| = \langle aE|\,p_2|\rangle[aE|\,p_2|\vee|\hat{p}_2|\,[a/\tau]].$$

We have $[\widehat{a^\circ|\,p_2|}]\supset[\widehat{a^\circ|\,p_1+\tau p_2|}]$. This implis,

— either $c(ap_2,\ a(p_1+\tau p_2))$ in which case $|a(p_1+\tau p_2)|\oplus|ap_2|\equiv|a(p_1+\tau p_2)|$,

— $[\widehat{a^\circ|\,p_2|}]\equiv[\widehat{a^\circ|\,p_1+\tau p_2|}]$. By Lemma 2, $ap_2\simeq a(p_1+\tau p_2)$ which implies $p_2\cong p_1+\tau p_2$.

By Property (3b) this is the case iff $\tau p_2\simeq p_1+\tau p_2$ or $p_2\simeq\tau(p_1+\tau p_2)$ or $p_2\simeq p_1+\tau p_2$. From the last case we deduce $p_2\simeq\tau p_2$. As $|\,p_2|$, $|\,p_1+\tau p_2|\in K$ all three cases contradict the fact that $|\,p_2|$, $|\,p_1+\tau p_2|\in$ STRICT. ▮

By using Lemmas 8, 9, 10 and reasoning as in proof of Theorem 1 (P3) we get

THEOREM 4 (completeness). *$\forall\,p,p'\in P(A)$ $p\simeq p'$ implies $|\,p|\equiv|\,p'|$.*

THEOREM 5 (characterization). *The function $|\ |$ characterizes observational congruence, i.e., for any pair p,p' of terms of $P(A)$, $p'\models|\,p|$ iff $p'\simeq p$.*

Proof. By theorems 2 and 4 and Proposition 4. ▮

IV. Discussion

This work has been motivated by the search for a sufficiently powerful modal language compatible with observational congruence in CCS. By following an approach different from that one of Brookes and Rounds (1983), Hennessy and Milner (1980), and Stirling (1983), we obtained a characterization of congruence classes on finite terms. A similar characterization has been obtained for the class of recursively defined controllable CCS processes, i.e., processes p for which there exists some p' observationally equivalent to p and p' has no τ-transition Graf (1984), Graf and Sifakis (1984). These results brought us to study a language L_0 for the specification of controllable CCS processes which contains the one proposed in Hennessy and Milner (1980). L_0 is a certain subset of the set of formulas built from the constants [true] and [false] by using logical operators and two independant modal operators $\textcircled{\lambda}$ and $\langle\!\langle\lambda\rangle\!\rangle$ for $\lambda \in A$. Their meaning is given by,

$$\langle\!\langle\tau\rangle\!\rangle F = \mu y \cdot (F \vee \langle \tau \wedge y \rangle)$$

$$\langle\!\langle a \rangle\!\rangle F = \langle a \wedge \langle\!\langle\tau\rangle\!\rangle F \rangle$$

$$\textcircled{\tau} F = \mu y \cdot (F \vee \langle \tau \wedge y \rangle \wedge [\tau \wedge y \vee \hat{F}])$$

$$\textcircled{a} F = \langle a \wedge \textcircled{\tau} F \rangle \wedge [a \wedge \textcircled{\tau} F \vee \hat{F}[a/\tau]]$$

where F is a formula and $\hat{F}$ is such that $\forall p \in P(A)$ $p \models [\hat{F}]$ iff $\exists p'$ $p + p' \models F$, i.e., $\hat{}$ is an extension of the function in III.2.1.

Notice that $\textcircled{\tau} F$ and $\textcircled{a} F$ are generalizations of $E(F)$ and $a^{\circ}F$. The formula $\textcircled{\tau} F$ Characterizes all the terms which either satisfy F or their only possible derivations are τ-derivations until some state is reached for which F or $\hat{F}$ is true. In a similar manner $\textcircled{a} F$ characterizes all the terms for which the only possible derivations are of the form $a\tau^*$ until some state is reached satisfying F or $\hat{F}$. Thus the modality $\textcircled{\lambda}$ expresses eventuality or inevitability. On the other hand the formulas $\langle\!\langle\tau\rangle\!\rangle F$ and $\langle\!\langle a \rangle\!\rangle F$ express the fact that it is possible to satisfy F by exectuting a sequence of τ^* or a sequence of $a\tau^*$, respectively. Obviously, $\langle\!\langle a \rangle\!\rangle$ in Hennessy and Milner (1980) is equivalent to $\langle\!\langle\tau\rangle\!\rangle \langle\!\langle a \rangle\!\rangle$ in L_0. This language has been completely studied in Graf (1984), Graf and Sifakis (1984).

Received July 30, 1984; accepted August, 1985

References

Brookes, S. D., and Rounds, W. C. (1983), Behavioural equivalence relations induced by programming logics, *in* "Proc. 10th ICALP ", *in* Lecture Notes in Comp. Sci. Vol. 154.

GRAF, S. (1984), Logiques du temps arborescent pour la spécification et la preuve de programmes. Thèse 3ème Cycle, IMAG, Grenoble, February.

GRAF, S., AND SIFAKIS, J. (1983), A modal characterization of observational congruence on finite terms of CCS. R.R. 402, IMAG, November.

GRAF, S., AND SIFAKIS, J. (1984), "A Logic for the Specification and the Proof of Controllable Processes of CCS. Advanced Seminar Logics and Models for Verification and Specification of Concurrent Systems," La Colle sur Loup, France.

HENNESSY, M., AND MILNER, R. (1980), Observing nondeterminism and concurrency, "Proc. 7th Int. Colloq. in Automata. Lang. and Program., *in* "Lecture Notes in Comput. Sci.," Vol. 85, Springer-Verlag, New York/Berlin.

KOZEN, D. (1982), Results on the propositional μ-calculus, "Proc. 9th ICALP, *in* Lecture Notes in Comput. Sci. Vol. 140, Springer-Verlag, New York/Berlin.

MILNER, R. (1980), A calculus of communicating systems, *in* "Lecture Notes in Comput. Sci.,"Vol. 92, Springer-Verlag, New York/Berlin.

STIRLING, C. (1983), A Proof Theoric Characterization of Observational Equivalence," Internal Report CSR-132–83, University of Edinburgh.