LFCS

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

The Nonexistence of Finite Axiomatisations for CCS congruences

by

Faron Moller

LFCS Report Series

ECS-LFCS-89-97
(also published as CSR-315-89)

November 1989

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

The Nonexistence of Finite Axiomatisations for CCS congruences

Faron Moller
Lab for the Foundations of Computer Science
University of Edinburgh

Abstract. In this paper, we examine equational axiomatisations for congruences over a simple sublanguage of Milner's process algebra CCS. We show that no finite set of equational axioms can completely characterise any reasonably-defined congruence which is at least as strong as Milner's strong congruence. In the case of strong congruence, this means that the Expansion Theorem of CCS cannot be replaced by any finite collection of equational axioms. Moreover, we thus also isolate a source of difficulty in axiomatising any reasonable non-interleaving semantic congruence, where the Expansion Theorem fails to hold.

1 Introduction

There are a number of different approaches in existence to the algebraic description of concurrent processes. One of the original and most influential treatments is that of Milner's CCS, the *Calculus of Communicating Systems* ([Mil80], [Mil89]). In his approach, Milner considers only a minimal set of primitive operators, in order to maintain simplicity in his analyses. Thus he has for instance a constant representing the null process (nil $\mathbf{0}$), one operator allowing for sequentiality (atomic action prefix $a.$), one operator allowing choice between various computation paths (nondeterministic sum $+$), and one operator allowing concurrent computation (parallel composition $|$). Milner's approach is very much operational in nature, in particular giving an operational notion of equivalence (the so-called *bisimulation* equivalence of [Par81]), but also involves the development of equational theories for reasoning about equivalences between process terms.

In this paper, we consider equational axiomatisations for the above restricted subset of the process calculus CCS, which we shall refer to as $\mathcal{P}$. Hence, the collection of terms $P \in \mathcal{P}$ is defined by the following BNF-like notation:

$$P \ ::= \ \mathbf{0} \ \Big| \ a.P \ \Big| \ P+P \ \Big| \ P \mid P.$$

Here, the actions a range over some nonempty set **Act**. We shall often omit the dot of the action prefix, and drop trailing **0**'s from expressions, thus for instance writing $ab+c$ instead of $a.b.\mathbf{0}+c.\mathbf{0}$. Furthermore, concurrency will take the form of the full merge operator, so we are for the present prohibiting communication between processes. However, we shall point out later how our results equally apply to the same calculus with communication. With just this simple language, we shall show that any reasonably-defined notion of congruence which is at least as discriminating as Milner's strong (observational) congruence must be axiomatised by an infinite set of equations. In the case of strong congruence, the infinite dimension is provided for by the axiom schema presented by Milner's Expansion Theorem.

Our notion of reasonably-defined congruence will include non-interleaving semantic congruences which have been under study recently, such as the partial order semantic congruence of [Bou86], the distributed bisimulation semantic congruence of [Cas87], and the congruence of [Hen87]. Hence we shall have presented some insight into the trouble found in these works in trying to completely axiomatise their congruences where the infinitary Expansion Theorem is invalid.

2 Transitional Semantics

In this section, we provide our language with an operational semantic definition based on the notion of labelled transition sytems. This method gives a derivation relation on terms in our language which defines the possible actions which a term may perform. Upon giving our transitional semantics, we define strong congruence using the notion of bisimulation based on this transition system.

The transitional semantics for $\mathcal{P}$ is given in the usual fashion by the transition system $\longrightarrow \subseteq \mathcal{P} \times \mathbf{Act} \times \mathcal{P}$ (written as $P \xrightarrow{a} Q$ for $(P,a,Q) \in \longrightarrow$) defined to be the least relation satisfying the inferential derivation laws presented in Figure 1. Thus using the first rule we have $a.P \xrightarrow{a} P$, and for each of the other rules, whenever we can derive the transition above the line, then we can derive the transition below the line.

Our equivalence $\sim \subseteq \mathcal{P} \times \mathcal{P}$ is then defined to be the largest relation satisfying the following bisimulation condition: $P \sim Q$ if and only if for all $a \in \mathbf{Act}$,

(i) $P \xrightarrow{a} P'$ *implies* $\exists Q'$ *such that* $Q \xrightarrow{a} Q'$ *and* $P' \sim Q'$; *and*

$$a.P \xrightarrow{a} P$$

$$\frac{P \xrightarrow{a} P'}{P + Q \xrightarrow{a} P'} \qquad \frac{Q \xrightarrow{a} Q'}{P + Q \xrightarrow{a} Q'}$$

$$\frac{P \xrightarrow{a} P'}{P \mid Q \xrightarrow{a} P' \mid Q} \qquad \frac{Q \xrightarrow{a} Q'}{P \mid Q \xrightarrow{a} P \mid Q'}$$

Figure 1: Derivation Laws

(ii) $Q \xrightarrow{a} Q'$ *implies* $\exists P'$ *such that* $P \xrightarrow{a} P'$ *and* $P' \sim Q'$.

This relation can be shown to be a congruence over the language $\mathcal{P}$, referred to as *strong (observational) congruence*, and to be completely characterised by the equational theory given in Figure 2. Notice that this gives an infinite axiomati-

$$A_1.\ (x+y)+z = x+(y+z) \qquad A_3.\ x+x = x$$
$$A_2.\ x+y = y+x \qquad A_4.\ x+\mathbf{0} = x$$
$$Exp_{mn}.\ \text{For } t = \sum_{i=1}^{m} a_i x_i \text{ and } u = \sum_{j=1}^{n} b_j y_j, \quad (m,n \geq 0)$$
$$t \mid u = \sum_{i=1}^{m} a_i\big(x_i \mid u\big) + \sum_{j=1}^{n} b_j\big(t \mid y_j\big)$$

Figure 2: Axioms for $\mathcal{P}$

sation, due to the presence of the axiom schema Exp_{mn}, commonly referred to as the *Expansion Theorem*. This paper will prove that such a sound and complete axiomatisation for strong congruence is by necessity infinite. Moreover, we shall show that this property holds of *any* reasonable congruence which is at least as strong as strong congruence.

In the remainder of the paper, we shall often use $=$ to represent semantic equivalence $\sim$, and $\equiv$ to represent syntactic identity modulo associativity and commutativity of $+$ and $|$. We shall also extend the transition system $\longrightarrow$ to allow $P \xrightarrow{a} R$ whenever there exists some $P' = R$ such that $P \xrightarrow{a} P'$.

3 Reasonable Congruences

In this section, we define a property of equivalences which we argue should be exhibited by any "reasonable" equivalence over our language $\mathcal{P}$. This property will take the form of a sequence of laws which we argue represent sensible identities, and thus should be valid with respect to any reasonable equivalence.

There is much division in concurrency theory regarding the question of exactly what identities should hold in a sensible semantic equivalence (see, *e.g.,* [deN87]). It is generally accepted that an equivalence should be a congruence, thus allowing for the validity of substitutivity of program parts. Furthermore, there are arguments that any terms which are identified should be at least strongly congruent (*e.g.,* [Mil89]); the arguments which distinguish observationally distinct processes will hold valid for our hypothetical "reasonable" equivalence. Of course, this is also arguably a somewhat strong restriction. For example, we are not allowing our semantics to abstract away from internal events which should not be observable to the environment. Also, we are ignoring several other sensible classes of equivalences, for example those based on the notion of *"testing"* ([deN84], [Hen88]). However, for the present paper, we shall maintain the strength of this restriction.

Outside of this, there is little agreement as to how fine a congruence should be. Some strong arguments stem from the Petri net community and other proponents of *noninterleaving semantics* (see, *e.g.,* [Rei85], [Pra86]). The objections to the weakness of observational congruence arise due to its property, expressed by the Expansion Theorem, of identifying terms involving distinct causal dependencies on their actions. For instance, a simple application of the Expansion Theorem would quickly lead us to conclude that

$$a \mid b = ab + ba.$$

However, whereas on the left hand side of this statement, there is no causal dependency expressed between the two actions a and b — the two actions are simply performed independently — the summands of the term on the right hand side each express a definite causal relationship between the actions; in the first summand, action a must occur before action b, whereas this situation is reversed in the second summand. Such an interleaving semantic understanding of processes reduces parallelism to a nonprimitive operation definable in terms of nondeterministic choice and causal dependency. Objections arising against this viewpoint stem from the belief that parallelism should not be expressed as above, but rather

that it has fundamental properties which should guarantee it a place among the set of primitive concepts.

The question now remains as to how far we can cut down on strong congruence whilst still maintaining all of the identities which should hold in a reasonable equivalence. Certainly we could strengthen it enough to avoid all possible objections to the treatment of concurrency. For instance, we may not want to allow the following partial application of the Expansion Theorem:

$$a \mid b = a \mid b + ab.$$

This could possibly be considered a valid law in some noninterleaving semantic theory, as the concurrent nature of the atomic processes is still present on both sides of the equation. However, it still allows for the introduction of causal dependency where it had not previously existed, and as such is faced with the same arguments faced originally by the Expansion Theorem.

However, we do not want to allow our "reasonable" congruence to be too fine. For instance, Winskel's *event structure semantics* ([Win83]), as well as the original event structure semantics of Boudol and Castellani ([Bou86], Section 3) only allow process terms to be identified if they are identical modulo the associativity, commutativity and $\mathbf{0}$-absorption of the $+$ and $\mid$ combinators, as well as the associativity of a general sequential combinator in the latter case. Clearly these approaches are too strict, as they do not allow for any non-trivial identities, not even the well-accepted idempotence of nondeterministic choice (law A_3 of Figure 2).

What we argue here is that certain *reduction* laws should hold valid. For instance, the following identity should be made in any sensible semantic congruence:

$$\begin{aligned}(x+y) \mid (u+v) \;+\; x \mid u \;+\; x \mid v \;+\; y \mid u \;+\; y \mid v \\ = \; x \mid (u+v) \;+\; y \mid (u+v) \;+\; (x+y) \mid u \;+\; (x+y) \mid v.\end{aligned}$$

This reduction law can be informally justified as follows. Every possible single-step behaviour which one side of the equation can exhibit is matched by an identical single-step behaviour on the other side of the equation within an identical parallel context. For example, the possibility of the indeterminate process x proceeding in the second summand $x \mid u$ on the left hand side of the equation is matched by the possibility of the same indeterminate process x proceeding in the third summand $(x+y) \mid u$ on the right hand side of the equation. Both allow the indeterminate process x to proceed in the context in which it is running in parallel

with the indeterminate process u. Indeed, every closed instance of this law is derivable in the equational theory of Figure 2, and hence this law represents a valid observational equivalence law. However, this law does not introduce any causal dependency where it did not previously exist. Indeed, it does not mention any actions explicitly. Thus it is not open to the objections faced by the Expansion Theorem.

We can generalise this law in several ways. Of interest to us for the proof of our result is the following generalisation, which can be informally argued in the same way as the above law.

$$(x+y) \mid (\sum_{i=1}^{n} z_i) \;+\; \sum_{i=1}^{n}(x \mid z_i) \;+\; \sum_{i=1}^{n}(y \mid z_i)$$
$$= \; x \mid (\sum_{i=1}^{n} z_i) \;+\; y \mid (\sum_{i=1}^{n} z_i) \;+\; \sum_{i=1}^{n}\big((x+y) \mid z_i\big)$$

If we now consider the following sequences of process terms:

$$\mathcal{A}_0 \stackrel{\text{def}}{=} \mathbf{0} \qquad\qquad \varphi_0 \stackrel{\text{def}}{=} \mathbf{0}$$
$$\mathcal{A}_{i+1} \stackrel{\text{def}}{=} a.\mathcal{A}_i \qquad\qquad \varphi_{i+1} \stackrel{\text{def}}{=} \varphi_i + \mathcal{A}_{i+1}$$

then by an appropriate instantiation, we derive the following sequence of reduction laws.

$$Red_n. \quad \varphi_2 \mid \varphi_n \;+\; \sum_{i=1}^{n}(a \mid \mathcal{A}_i) \;+\; \sum_{i=1}^{n}(aa \mid \mathcal{A}_i)$$
$$= \; a \mid \varphi_n + aa \mid \varphi_n \;+\; \sum_{i=1}^{n}(\varphi_2 \mid \mathcal{A}_i)$$

We shall hence insist that any reasonable congruence over $\mathcal{P}$ should make the identities expressed by the axiom schema Red_n. What we shall prove then is that no finite set of equational laws which are sound with respect to strong congruence can derive every instance of the schema Red_n. This will be enough to prove that no sensible congruence which is at least as strong as strong congruence can be finitely axiomatised. This is true as any law which is sound with respect to such a congruence will also be sound with respect to strong congruence, so no finite set of laws which are valid for such a congruence can derive all instances of Red_n.

Notice that our result will hold over any nonempty set **Act** of atomic actions, including the singleton set $\mathbf{Act} = \{a\}$. The only assumption we make is that there exists some action $a \in \mathbf{Act}$. Indeed, if this were not the case, then all terms would be observationally equivalent to the nil term $\mathbf{0}$, and we would have a trivial finite

equational axiomatisation. Furthermore, our result will still hold in the calculus extended in the usual fashion with communication between processes through synchronisation on complementary actions, under the reasonable assumption that some action a is not its own complement.

4 The Nonexistence of Finite Axiomatisations

4.1 Approach to the Problem

We want to prove that no finite set of laws which are sound with respect to strong congruence can prove every instance of the axiom schema Red_n. That is to say, given any finite set $\mathcal{T}$ of such laws, there is some instance of Red_n for which there is no finite proof tree in a natural deduction style proof system which uses only a small collection of inference rules. These inference rules are as follows. Firstly, we need to allow our axioms to be instantiated. Thus for every closed instantiation $p = q$ of every axiom $t = u$ in our set $\mathcal{T}$, we have the inference

$$\frac{}{p = q}(t = u)$$

Then we need only to allow inferences based on the laws of equational reasoning (reflexivity, symmetry, transitivity, and substitutivity). These are as follows:

$$\frac{}{p = p}(refl) \qquad \frac{p = q}{q = p}(symm) \qquad \frac{p = q, \quad q = r}{p = r}(trans)$$

$$\frac{p = q}{a.p \;=\; a.q}(sub_.) \qquad \frac{p_1 = q_1, \quad p_2 = q_2}{p_1 + p_2 \;=\; q_1 + q_2}(sub_+) \qquad \frac{p_1 = q_1, \quad p_2 = q_2}{p_1 \mid p_2 \;=\; q_1 \mid q_2}(sub_|)$$

To accomplish our goal, we shall present a property Θ_n of statements $P = Q$ (where n is some integer depending on the finite set of axioms $\mathcal{T}$) such that whenever Θ_n holds for the conclusion of some rule of inference (as listed above), Θ_n will hold for one of the premises of the rule as well. In particular, no instantiation of any axiom will be able to introduce the property Θ_n. Hence we can conclude that there cannot be a proof of any statement $P = Q$ satisfying Θ_n. Furthermore, this property Θ_n will hold for the statement Red_n, thus giving our result.

4.2 Preliminary Results

In this section we make some technical definitions and state the technical lemmata which we need to derive our main result in the following section. Firstly, we let

$fv(t)$ represent the set of free variables appearing in the term t, and say that t is a *closed* term if $fv(t) = \emptyset$. Next, the proofs of several preliminary results are often going to use induction on the *depths* $|\bullet|$ of terms as defined as follows.

Definition 4.1

$$\begin{array}{ll} |\mathbf{0}| = 0 & |p+q| = \max\big(|p|,|q|\big) \\ |x| = 0 & |p \mid q| = |p| + |q| \\ |a.P| = 1 + |P| & \end{array}$$

Some simple but important properties of depth which we shall exploit in our inductive proofs are given by the following proposition.

Proposition 4.2 *For closed terms* $p, q \neq \mathbf{0}$,

$$\begin{array}{ll} (i) & |p| > 0; \\ (ii) & |p \mid q| > |p|, |q|. \\ (iii) & p \xrightarrow{a} p' \ \textit{implies} \ |p| > |p'|. \end{array}$$

Next, we define an important semantic class of terms in which we shall be interested.

Definition 4.3 *A term* $p \in \mathcal{P}$ *is prime iff it cannot be expressed as* $p = q \mid r$ *for any* $q, r \neq \mathbf{0}$.

Thus a prime term is one which cannot be decomposed into the parallel composition of simpler processes. The useful (and somewhat surprising) result about these prime terms is given by the following proposition by Milner regarding the decomposition of terms.

Proposition 4.4 (Unique Factorisation Theorem) *Any process term* $p \in \mathcal{P}$ *can be expressed uniquely as a parallel composition of primes.*

The utility of this proposition in the proof of our result is clear. By saying that a term is prime, we are restricting the possible syntactic form of the term. Simple tests for primality are given by the following proposition.

Proposition 4.5

(*i*) *If* $p \xrightarrow{a} \mathbf{0}$, *then* p *is prime.*

(*ii*) *If* $p \xrightarrow{a} p'$ *and* $p \xrightarrow{b} p''$, *where* p' *and* p'' *are distinct primes such that* $p \neq p' \mid p''$, *then* p *itself must be a prime.*

(*iii*) *If* $p \xrightarrow{a} p'$, $p \xrightarrow{b} p''$ *and* $p \xrightarrow{c} p'''$, *where* p', p'' *and* p''' *are distinct primes, then* p *itself must be a prime.*

We shall restrict our class of equivalences in one final mild way by insisting that they all respect **0**-absorption through both the + and | operators, and in the sequel we shall want to deal exclusively with terms which do not contain unnecessary **0** summands or factors. With this in mind, we define $\tilde{t}$ to be the term t with all **0** summands and factors removed. Formally, we have the following definition.

Definition 4.6

$$\begin{aligned} \tilde{\mathbf{0}} &= \mathbf{0} \\ \tilde{x} &= x \\ \widetilde{at} &= a\tilde{t} \end{aligned}$$

$$\widetilde{t+u} = \begin{cases} \tilde{t} & \text{if } |u| = 0 \wedge fv(u) = \emptyset \\ \tilde{u} & \text{if } |t| = 0 \wedge fv(t) = \emptyset \\ \tilde{t} + \tilde{u} & \text{otherwise} \end{cases}$$

$$\widetilde{t \mid u} = \begin{cases} \tilde{t} & \text{if } |u| = 0 \wedge fv(u) = \emptyset \\ \tilde{u} & \text{if } |t| = 0 \wedge fv(t) = \emptyset \\ \tilde{t} \mid \tilde{u} & \text{otherwise} \end{cases}$$

We shall also restrict the type of axiom set which we shall allow in our proof system, to exploit the above **0** absorption properties in our proofs. The special class of axiomatisations will allow us to prove statements without invoking unnecessary **0** factors and summands. However, as we shall see, the restricted class will not be a real restriction with respect to the properties of axiomatisability which we are analysing. That is, given any arbitrary finite, sound and complete axiomatisation, we can produce another finite, sound and complete axiomatisation which is in our special class of axiom sets.

The axiom sets to which we shall restrict ourselves will be *saturated*, as defined as follows.

Definition 4.7 *Let* $\mathcal{T}$ *be an arbitrary set of equational axioms. The* saturation *of* $\mathcal{T}$ *is defined to be*

$$Sat(\mathcal{T}) = \mathcal{T} \cup \tilde{\mathcal{T}},$$

where

$$\tilde{\mathcal{T}} = \left\{ \tilde{t}_0 = \tilde{u}_0 \;\middle|\; \exists t = u \in \mathcal{T}, \bar{x} \subseteq fv(t) \cup fv(u) \right. \\ \left. st\ t_0 = t\left\{\overline{\mathbf{0}}/\bar{x}\right\}\ and\ u_0 = u\left\{\overline{\mathbf{0}}/\bar{x}\right\} \right\}.$$

The important properties of $Sat(\mathcal{T})$ are expressed by the following propositions.

Proposition 4.8 *$\mathcal{T} \vdash t = u$ if and only if $Sat(\mathcal{T}) \vdash t = u$.*

Proposition 4.9 *$\mathcal{T}$ is finite if and only if $Sat(\mathcal{T})$ is finite.*

Thus from now on, we shall restrict ourselves to considering only saturated axiom sets, that is, axiom sets $\mathcal{T}$ such that $\mathcal{T} = Sat(\mathcal{T})$. As we pointed out earlier, the above results show that this assumption is not a restriction if we are interested in finite, sound and complete axioms sets. However, an important simplification of proofs is given as follows.

Proposition 4.10 *If we have a proof of a statement $P = Q$ in our natural deduction style proof system parameterised by a saturated axiom set $\mathcal{T}$, then replacing $p = q$ throughout the proof tree by $\tilde{p} = \tilde{q}$ gives us a valid proof of the statement $\tilde{P} = \tilde{Q}$. Thus using a saturated axiom set, a (shortest) proof of a result containing no occurrences of $\mathbf{0}$ as a summand or as a factor need not contain any occurrence of $\mathbf{0}$ as a summand or factor in any of its intermediate terms.*

Proof:

It is not hard to see that any inference

$$\frac{\cdots\ p_i = q_i\ \cdots}{p = q}(rule)$$

can be changed to the valid inference

$$\frac{\cdots\ \tilde{p}_i = \tilde{q}_i\ \cdots}{\tilde{p} = \tilde{q}}(rule').$$

The only nontrivial case is in dealing with axioms. In this case, we have

$$\frac{}{p = q}(t = u)$$

where $p = q$ is axiom $t = u$ instantiated by some substitution σ. This inference can be replaced by

$$\frac{}{\tilde{p} = \tilde{q}}(\tilde{t}_0 = \tilde{u}_0)$$

where $t_0 = t\left\{\bar{\mathbf{0}}/_{\bar{x}}\right\}$ *and* $u_0 = u\left\{\bar{\mathbf{0}}/_{\bar{x}}\right\}$, *where* $\bar{x} = \left\{x \mid \sigma_x = \mathbf{0}\right\}$.

Clearly $\tilde{p} = \tilde{q}$ *is axiom* $\tilde{t_0} = \tilde{u_0}$ *instantiated with substitution* $\tilde{\sigma}$ *defined by* $\tilde{\sigma} = (\widetilde{\sigma_x})$. □

Thus we restrict our proof system to be parameterised by saturated axiom sets.

Next, we shall want to restrict our attention to just a certain subset of process terms as defined as follows.

Definition 4.11 *We define* $\mathcal{S}_n$ *to be the derivation and a-prefix of derivation closure of the set* $\{\varphi_2 \mid \varphi_n\}$. *That is,* $\mathcal{S}_n$ *is the smallest set satisfying:*

$$\begin{array}{ll} i) & \varphi_2 \mid \varphi_n \in \mathcal{S}_n; \text{ and} \\ ii) & P \in \mathcal{S}_n,\ P \xrightarrow{a} P' \implies P', a.P' \in \mathcal{S}_n. \end{array}$$

We can express this set explicitly as follows.

Proposition 4.12

$$\begin{aligned} \mathcal{S}_n = \left\{\varphi_2 \mid \varphi_n\right\} &\cup \left\{\mathcal{A}_i \mid \mathcal{A}_j \;\middle|\; 0 \le i \le 2,\ 0 \le j \le n\right\} \\ &\cup \left\{\mathcal{A}_i \mid \varphi_n \;\middle|\; 0 \le i \le 2\right\} \cup \left\{\varphi_2 \mid \mathcal{A}_j \;\middle|\; 0 \le j \le n\right\} \\ &\cup \left\{a.(\mathcal{A}_i \mid \varphi_n) \;\middle|\; 0 \le i < 2\right\} \cup \left\{a.(\varphi_2 \mid \mathcal{A}_j) \;\middle|\; 0 \le j < n\right\} \\ &\cup \left\{a.(\mathcal{A}_i \mid \mathcal{A}_j) \;\middle|\; 0 \le i \le 2,\ 0 \le j \le n,\ i + j \le n + 1\right\}. \end{aligned}$$

Some technical properties which this set satisfies in which we shall be interested are given by the following propositions.

Proposition 4.13 *If* $P + Q = \sum S$ *for some* $S \subseteq \mathcal{S}_n$, *then* $P = \sum T$ *for some* $T \subseteq \mathcal{S}_n$.

Proof:

Let $P \xrightarrow{a} P'$.

Then $\sum S \xrightarrow{a} P'' = P'$, *so* $P_0 \xrightarrow{a} P''$ *for some* $P_0 \in S \subseteq \mathcal{S}_n$.

But then by **Definition 4.11**, $a.P'' \in \mathcal{S}_n$.

Thus letting $T = \{a.P'' \in \mathcal{S}_n \mid \exists P' = P''$ *st* $P \xrightarrow{a} P'\}$, *we have* $P = \sum T$. □

Corollary 4.14 *If $P = \sum S$ for some $S \subseteq \mathcal{S}_n$, and $P \xrightarrow{a^j} P'$ for some $j > 0$, then there is some $R \in \mathcal{S}_n$ such that $R = P'$.*

Proof:

Suppose $P \xrightarrow{a} P'' \xrightarrow{a^{j-1}} P'$.

Then by **Definition 4.11**, *$\sum S \xrightarrow{a} P_0 = P''$ for some $P_0 \in \mathcal{S}_n$;*

Hence also by **Definition 4.11**, *$P_0 \xrightarrow{a^{j-1}} R = P'$ for some $R \in \mathcal{S}_n$.* □

Proposition 4.15 *Let $m > 2$, and $0 < r_1 < r_2 < \cdots < r_m$. If there is some $P \in \mathcal{S}_n$ such that for some Q, $\mathcal{A}_{r_1} + \mathcal{A}_{r_2} + \cdots + \mathcal{A}_{r_m} + Q = P$, with $|P| \leq n$, then*

$$P = \mathcal{A}_{r_1} + \mathcal{A}_{r_2} + \cdots + \mathcal{A}_{r_m} + Q = \varphi_n.$$

Proof:

Straightforward check through all of the possibilities for $P \in \mathcal{S}_n$ given by the alternate definition of $\mathcal{S}_n$ of **Proposition 4.12.** □

We are now ready to define our property Θ_n of statements $P = Q$ as described above.

Definition 4.16 *For $U, V \subseteq \mathcal{P}$ being two sets of terms, we first define $\Theta_n^L(U,V)$ to be the proposition which states the following:*

$$\begin{aligned} P \in U \cup V \implies & P \equiv \tilde{P}, \quad \textit{and} \quad P \not\equiv \mathbf{0},\ P' + P'', \\ & \textit{and} \quad \textstyle\sum U = \sum V = \sum S \quad \text{for some } S \subseteq \mathcal{S}_n, \\ & \textit{and} \quad \exists P \in U \textit{ st } P = \varphi_2 \mid \varphi_n, \\ & \textit{and} \quad \nexists Q \in V \textit{ st } Q = \varphi_2 \mid \varphi_n. \end{aligned}$$

Thus $\Theta_n^L(U,V)$ states (among other things) that the equation $\sum U = \sum V$ expresses a (valid) equality between terms in which the term $\varphi_2 \mid \varphi_n$ is captured by a single summand on the left hand side of the equality, but not by any single summand on the right hand side.

We then define $\Theta_n(U,V) = \Theta_n^L(U,V) \vee \Theta_n^L(V,U)$.

It is easy to check that the law Red_n is of the form $\sum U = \sum V$ where $\Theta_n(U,V)$ is true. We shall now proceed to show that given any finite saturated set of strong congruence axioms, there is some n such that no equivalence $\sum U = \sum V$ where $\Theta_n(U,V)$ holds can be proven. To do this, we start with the following basic lemmata.

Proposition 4.17 *Let $n > 1$ and $U, V \subseteq \mathcal{P}$ be such that $\Theta_n(U,V)$. If $P \in U \cup V$ is the term satisfying $P = \varphi_2 \mid \varphi_n$, then $P \equiv P_2 \mid P_n$, where $P_2 = \varphi_2$ and $P_n = \varphi_n$.*

Proof:

$\varphi_2 \mid \varphi_n \xrightarrow{a} \varphi_n$ and $\varphi_2 \mid \varphi_n \xrightarrow{a} a \mid \varphi_n \neq \varphi_n$.

Hence $P \not\equiv a.P'$, as $a.P' \xrightarrow{a} P'$ only.

Thus $P \equiv P' \mid P''$ where $P', P'' \neq \mathbf{0}$.

Since φ_2 and φ_n are prime, we must have that P' and P'' are precisely φ_2 and φ_n.

Hence $P \equiv P_2 \mid P_n$ where $P_2 = \varphi_2$ and $P_n = \varphi_n$. □

Proposition 4.18 *Let t be an open term in $\mathcal{P}$, and let σ be a substitution such that $t\sigma \equiv \widetilde{t\sigma}$, and such that for some $x \in fv(t)$, $\sigma_x = a\varphi_n + aa\varphi_n$. Then $t\sigma \neq \varphi_2 \mid \varphi_n$.*

Proof:

Let t, σ and x be as above.

t is of the form

$$t \equiv t_1 + t_2 + \cdots + t_m,$$

where each $t_i \not\equiv t' + t''$.

Let k be such that $x \in fv(t_k)$.

Thus $t_k \not\equiv \mathbf{0}$.

If $t_k \equiv bt'$, then $x \in fv(t')$, so $|t\sigma| > |t'\sigma| \geq |\sigma_x| = n + 2$;

but $|\varphi_2 \mid \varphi_n| = n + 2$, so $t\sigma \neq \varphi_2 \mid \varphi_n$.

If $t_k \equiv t' \mid t''$, then $x \in fv(t')$ or $x \in fv(t'')$,

so $|t\sigma| = |t'\sigma| + |t''\sigma| \geq |\sigma_x| = n+2$;

so again $t\sigma \neq \varphi_2 \mid \varphi_n$.

Finally, if $t_k \equiv x$ *then* $t\sigma \xrightarrow{a} a\varphi_n$;

but $\varphi_2 \mid \varphi_n \not\xrightarrow{a} a\varphi_n$, *so again* $t\sigma \neq \varphi_2 \mid \varphi_n$. □

The following lemma is the main crux of our proof, that the properties Θ_n eventually transcend any finite set of valid axioms. The lengthy proof of this result relies heavily on the use of the Unique Factorisation Theorem in syntactically analysing terms, as well as the special nature of the class of terms $\mathcal{S}_n$.

Proposition 4.19 *Let $\mathcal{T}$ be a finite saturated set of sound (with respect to strong congruence) axioms, and let n be bigger than twice the number of operators in any axiom in $\mathcal{T}$. Then no axiom $t = u$ in $\mathcal{T}$ can be instantiated to a statement $p = q$ where $p \equiv \sum U$ and $q \equiv \sum V$ such that $\Theta_n(U,V)$.*

Proof:

Let n be as above, and suppose $t = u$ is an axiom in $\mathcal{T}$ such that under substitution σ, $t = u$ instantiates to $p = q$ where $p \equiv \sum U$ and $q \equiv \sum V$ such that $\Theta_n(U,V)$.

Without loss of generality, assume that $\Theta_n^L(U,V)$.

Clearly, $fv(t) = fv(u)$, as $t = u$ is assumed to be a valid axiom.

Now, $t \equiv t_1 + t_2 + \cdots + t_k$ and $u \equiv u_1 + u_2 + \cdots + u_{k'}$ for some $k, k' > 0$,

where each $t_i, u_i \not\equiv v + v'$.

If $\Theta_n^L(U,V)$, then for some i, either $t_i\sigma \equiv P_2 \mid P_n$ or $t_i\sigma \equiv P_2 \mid P_n + Q$,

where $P_2 = \varphi_2$ and $P_n = \varphi_n$.

Consider the structure of t_i:

$t_i \equiv \mathbf{0} \implies t_i\sigma \equiv \mathbf{0}$ (contradiction);

$t_i \equiv x \implies \sigma_x \equiv t_i\sigma$ *and* $x \in fv(u_j)$ *for some* j

$\implies u_j \not\equiv \mathbf{0}, au', u' + u'', u' \mid u''$

$\implies u_j \equiv x$ *and* $P_2 \mid P_n \in V$

(contradicting $\Theta_n^L(U,V)$)

$t_i \equiv at' \implies t_i\sigma \equiv a(t'\sigma)$ (contradiction);

$t_i \equiv t' + t'' \implies$ (contradiction);

Thus $t_i \equiv t' \mid t''$ *and* $t_i\sigma \equiv t'\sigma \mid t''\sigma \equiv P_2 \mid P_n$.

Hence $t_i \equiv t' \mid t''$ *with* $t'\sigma \equiv P_2 = \varphi_2$ *and* $t''\sigma \equiv P_n = \varphi_n$.

Now $t'' \equiv v_1 + v_2 + \cdots v_l$ *where* $l < \frac{n}{2}$ *and each* $v_h \not\equiv v + v'$.

$t''\sigma \equiv v_1\sigma + v_2\sigma + \cdots v_l\sigma = \varphi_n = \mathcal{A}_1 + \mathcal{A}_2 + \cdots + \mathcal{A}_n$,

so some $v_h\sigma = \mathcal{A}_{r_1} + \mathcal{A}_{r_2} + \cdots + \mathcal{A}_{r_m}$ *for some* $m > 2$ *and*

$0 < r_1 < r_2 < \cdots < r_m$.

Thus clearly $v_h \not\equiv \mathbf{0}, av, v + v', v \mid v'$, *so* $v_h \equiv x$ *for some variable* x *where*

$$\sigma_x = \mathcal{A}_{r_1} + \mathcal{A}_{r_2} + \cdots + \mathcal{A}_{r_m}.$$

Clearly $x \notin fv(t')$, *as* $|t'\sigma| = 2 < r_m = |\sigma_x|$.

Let $\sigma' = \sigma\left\{{}^{a\varphi_n + aa\varphi_n}/_{x}\right\}$.

Then $t'\sigma' \equiv t'\sigma$, *and* $t\sigma' \xrightarrow{a} t'\sigma' \mid \varphi_n = \varphi_2 \mid \varphi_n$.

Therefore for some j, $u_j\sigma' \xrightarrow{a} \varphi_2 \mid \varphi_n$.

Now $|u_j\sigma'| > n + 2 = |u\sigma|$, *so clearly* $x \in fv(u_j)$.

Consider the structure of u_j*:*

$u_j \equiv \mathbf{0} \implies x \notin fv(u_j)$ (contradiction);

$u_j \equiv x \implies u_j\sigma' \equiv a\varphi_n + aa\varphi_n \not\xrightarrow{a} \varphi_2 \mid \varphi_n$
(contradiction);

$u_j \equiv au' \implies u_j\sigma' \equiv a(u'\sigma')$
$\implies u'\sigma' = \varphi_2 \mid \varphi_n$ *and* $x \in fv(u')$
(contradicting **Proposition 4.18***)*

$u_j \equiv u' + u'' \implies$ (contradiction);

Hence $u_j \equiv u' \mid u''$ *with* $u''\sigma' \xrightarrow{a} p$ *st* $u'\sigma' \mid p = \varphi_2 \mid \varphi_n$.

If $x \in fv(u')$, *then* $n + 2 = |u'\sigma'| + |p| \geq |\sigma'_x| + |p| \geq n + 2 + |p|$;

so $p = \mathbf{0}$ *and* $u'\sigma' = \varphi_2 \mid \varphi_n$.

(contradicting **Proposition 4.18***)*

Hence $x \notin fv(u')$, *and so* $x \in fv(u'')$.

Now $u'\sigma \mid p = \varphi_2 \mid \varphi_n$, *and* $u'\sigma \neq \mathbf{0}$,

so $u'\sigma = \varphi_2$ *or* $u'\sigma = \varphi_n$ *or* $u'\sigma = \varphi_2 \mid \varphi_n$.

But $|u'\sigma| = |u_j\sigma| - |u''\sigma| \leq |u\sigma| - |\sigma_x| < (n + 2) - 2 = n$.

Therefore $u'\sigma = \varphi_2$.

Thus also $|u''\sigma| \leq n$.

Now, $x \in fv(u'') \implies u''\sigma \xrightarrow{a^j} \sigma_x + Q$ *for some* Q, $j \geq 0$.

Hence $u\sigma \xrightarrow{a^{j+1}} \sigma_x + Q$.

Thus by **Proposition 4.14**, $\exists P \in \mathcal{S}_n$ *st* $\sigma_x + Q = P$.

But $\sigma_x = \mathcal{A}_{r_1} + \mathcal{A}_{r_2} + \cdots + \mathcal{A}_{r_m}$ *for some* $m > 2$

with $0 < r_1 < r_2 < \cdots < r_m$.

Hence by **Proposition 4.15**, $\sigma_x + Q = \varphi_n$.

Thus $u''\sigma \xrightarrow{a^j} \varphi_n$.

Now $n \geq |u''\sigma| \geq j + n$, *so* $j = 0$.

Therefore $u''\sigma = \varphi_n$.

But then $u'\sigma \mid u''\sigma \equiv P_2 \mid P_n \in V$ *for some* $P_2 = \varphi_2$ *and* $P_n = \varphi_n$
(contradicting $\Theta_n^L(U,V)$*)*

.

Therefore no axiom $t = u$ *in* $\mathcal{T}$ *can be instantiated to a statement* $p = q$ *where* $p \equiv \sum U$ *and* $q \equiv \sum V$ *such that* $\Theta_n(U,V)$. □

Given that the property Θ_n cannot be introduced into a proof tree through the application of an axiom, the next step in our proof is to show that it also cannot be introduced through the application of the rules for transitivity or substitutivity of the + operator. The cases involving the final few inference rules are trivial.

Proposition 4.20 *Suppose in a sound proof, we have an inference:*

$$\frac{p = r \quad r = q}{p = q}(trans)$$

where $p \equiv \sum U$, $q \equiv \sum V$, $r \equiv \sum W$,
and $R \in W \implies R \equiv \tilde{R}$, *and* $R \not\equiv \mathbf{0}, R' + R''$;

Then

$$\Theta_n(U,V) \implies \Theta_n(U,W) \vee \Theta_n(W,V).$$

Similarly for the (sub_+) *rule; corresponding to the inference:*

$$\frac{p = q \quad p' = q'}{p + p' = q + q'}(sub_+)$$

where $p \equiv \sum U$, $q \equiv \sum V$, $p' \equiv \sum U'$, *and* $q' \equiv \sum V'$,
we have the result that

$$\Theta_n(U \cup U', V \cup V') \implies \Theta_n(U, V) \vee \Theta_n(U', V').$$

Proof:

Consider the (trans) *rule case:*

Assume $\Theta_n^L(U, V)$. *We know immediately that*

$$P \in U \cup V \cup W \implies P \equiv \tilde{P} \text{ and } P \not\equiv \mathbf{0}, P' \mid P'',$$

and (from $\Theta_n^L(U, V)$, *and the soundness of the proof in which the inference appears) that for some* $S \subseteq \mathcal{S}_n$,

$$\sum U = \sum V = \sum W = \sum S.$$

Now if $\nexists R \in W$ *st* $R = a \mid \varphi_n$, *then clearly* $\Theta_n^L(U, W)$.
Also, if $\exists R \in W$ *st* $R = a \mid \varphi_n$, *then clearly* $\Theta_n^L(W, V)$.
Similarly, $\Theta_n^L(V, U) \implies \Theta_n^L(W, U) \vee \Theta_n^L(V, W)$.
Hence $\Theta_n(U, V) \implies \Theta_n(U, W) \vee \Theta_n(W, V)$.

The (sub_+) *rule case is similarly straightforward:*

Assume $\Theta_n^L(U \cup U', V \cup V')$. *Again we know immediately that*

$$P \in U \cup U' \cup V \cup V' \implies P \equiv \tilde{P} \text{ and } P \not\equiv \mathbf{0}, P' + P'',$$

and that for some $S \subseteq \mathcal{S}_n$,

$$\sum(U \cup U') = \sum(V \cup V') = \sum S,$$

and

$$\exists P \in U \cup U' \text{ such that } P = a \mid \varphi_n.$$

Suppose this $P \in U$. *Then from* $\Theta_n^L(U \cup U', V \cup V')$, *and the soundness of the proof in which the inference appears, and from* **Proposition 4.13**, *we have for some* $S' \subseteq \mathcal{S}_n$,

$$\sum U = \sum V = \sum S',$$

so clearly $\Theta_n^L(U,V)$.
Likewise, if this $P \in U'$, *then* $\Theta_n^L(U',V')$.
Similarly, $\Theta_n^L(V \cup V', U \cup U') \implies \Theta_n^L(V,U) \vee \Theta_n^L(V',U')$.
Hence $\Theta_n(U \cup U', V \cup V') \implies \Theta_n(U,V) \vee \Theta_n(U',V')$. □

4.3 Main Theorem

We are now ready to state and prove as a corollary of the above lemmata our main theorem, the non-finite-axiomatisability of any reasonable semantic congruence.

Theorem 4.21 *Let* $\mathcal{T}$ *be a finite saturated set of sound (with respect to any fixed reasonable congruence which is at least as strong as strong congruence) equational axioms. Let* n *be large enough (as allowed by* **Proposition 4.19***) so that no axiom in* $\mathcal{T}$ *can be instantiated to express any truth* $\sum U = \sum V$ *where* $\Theta_n(U,V)$. *Then our natural deduction style proof system cannot prove the valid statement* Red_n.

Therefore no finite complete axiom system can exist for any reasonable congruence which is at least as strong as strong congruence.

Proof:

Suppose we have a (shortest) proof of the statement Red_n

$$\varphi_2 \mid \varphi_n + \sum_{i=1}^{n}(a \mid \mathcal{A}_i) + \sum_{i=1}^{n}(aa \mid \mathcal{A}_i) = a \mid \varphi_n + aa \mid \varphi_n + \sum_{i=1}^{n}\varphi_2 \mid \mathcal{A}_i$$

which involves no terms containing $\mathbf{0}$ *as a summand or a factor. The proof takes the following form:*

$$\frac{\vdots}{p = q}(rule),$$

where $p \equiv \sum U_0$ *and* $q \equiv \sum V_0$ *for*

$$U_0 = \{\varphi_2, \varphi_n\} \cup \{\mathcal{A}_i \mid \mathcal{A}_j \mid 1 \le i \le 2, 1 \le j \le n\}$$

and

$$V_0 = \{a \mid \varphi_n, aa \mid \varphi_n\} \cup \{\varphi_2 \mid \mathcal{A}_j \mid 1 \le j \le n\}$$

so clearly $\Theta_n(U_0, V_0)$ *holds.*

Since this must be a finite *proof, somewhere in the proof tree is an inference*

$$\frac{\mathcal{D}}{\sum U = \sum V}(rule) \qquad \text{where} \quad \Theta_n(U,V),$$

such that the list $\mathcal{D}$ *of premises of the inference contains no equality*

$$\sum U' = \sum V' \quad \text{where} \quad \Theta_n(U',V').$$

By **Proposition 4.20**, $(rule)$ *can be neither of* $(trans)$ *nor* (sub_+). *Furthermore, by* **Proposition 4.19**, *we know that* $(rule)$ *cannot be* $(t = u)$ *for any axiom* $t = u \in \mathcal{F}$. *Also clearly* $(rule)$ *cannot be* $(symm)$, *as* $\Theta_n(U,V) \iff \Theta_n(V,U)$. *Finally,* $(rule)$ *cannot be any of* $(refl)$, $(sub_\bullet)$, *or* $(sub_|)$, *as this would contradict* $\Theta_n(U,V)$. *Hence we have shown that the original statement cannot be proven.* □

5 Conclusion

We have shown that any reasonable semantic congruence over our simple process language which is at least as strong as strong congruence can only be completely axiomatised using an infinite number of equational axioms. This partially explains the problems faced by [Hen87] for example in his attempt to axiomatise his noninterleaving semantic congruence.

There are two remedies to this situation. The first requires the introduction of some axiom schema which will finitely represent the required infinite dimension of axioms. Such is the case for example with Milner's Expansion Theorem for his observational congruence, and also with the noninterleaving semantic congruence of [Bou86] where such a new axiom schema derived from the Expansion Theorem is introduced.

An alternative solution to the problem is to introduce new syntactic constructs into the language which will increase the expressibility of the language to the point of allowing a finite sound and complete set of laws to be provided. This latter approach is the one taken in [Ber84], [Ber85], [Cas87], [Hen87] and [Mol89] in the introduction of the so-called *left-merge* operator.

Bibliography

[Ber84] Bergstra, J.A., J.W. Klop, *"Process Algebra for Synchronous Communication"*, Information and Computation, Vol 60, No 1/3, 1984.

[Ber85] Bergstra, J.A., J.W. Klop, *"Algebra of Communicating Processes with Abstraction"*, Theoretical Computer Science, Vol 37, No 1, 1985.

[Bou86] Boudol, G., I. Castellani, *"On the Semantics of Concurrency: Partial Orders and Transition Systems"*, Proc. TAPSOFT '87, Vol I, LNCS 249, Springer–Verlag, 1987.

[Cas87] Castellani, I., M. Hennessy, *"Distributed Bisimulation"*, University of Sussex Computer Science Report No. 5/87, July 1987.

[Hen87] Hennessy, M., *"Axiomatising Finite Concurrent Processes"*, University of Sussex Computer Science Department Report No 4/87, July 1987.

[Hen88] Hennessy, M., *"Algebraic Theory of Processes"*, MIT Press, 1988.

[Mil80] Milner, R., *A Calculus of Communicating Systems*, Lecture Notes in Computer Science 92, Springer–Verlag, 1980.

[Mil89] Milner, R., *Communication and Concurrency*, Prentice–Hall International, 1989.

[Mol89] Moller, F., *"The Importance of the Left Merge Operator in Process Algebras"*, University of Strathclyde Computer Science Department Report, 1989.

[deN84] De Nicola, R., M.C.B. Hennessy, *"Testing Equivalence for Processes"*, Theoretical Computer Science, Vol 34, No 1/2, 1984.

[deN87] De Nicola, R., *"Extensional Equivalences for Transition Systems"*, Acta Informatica, Vol 24, 1987.

[Par81] Park, D.M.R., *"Concurrency and Automata on Infinite Sequences"*, Proceedings of the 5^{th} G.I. Conference, Lecture Notes in Computer Science 104, Springer–Verlag, 1981.

[Pra86] Pratt, V., *"Modelling Concurrency with Partial Orders"*, International Journal of Parallel Programming, Vol 15, No 1, 1986.

[Rei85] Reisig, W., *Petri Nets: An Introduction*, EATCS Monographs on Theoretical Computer Science, Springer–Verlag, 1985.

[Win83] Winskel, G., *"Event Structure Semantics for CCS and Related Languages"*, Department of Computer Science Report DAIMI PB-159, Aarhus University, 1983.