CCS with Hennessy's merge has no finite equational axiomatization

CCS with Hennessy's Merge has no Finite Equational Axiomatization

Luca Aceto
BRICS, Department of Computer Science
Aalborg University
9220 Aalborg Ø, Denmark
Email: luca@cs.auc.dk

Wan Fokkink
CWI, Department of Software Engineering,
Kruislaan 413, 1098 SJ Amsterdam, The Netherlands
Email: wan@cwi.nl

Anna Ingólfsdóttir
BRICS, Department of Computer Science
Aalborg University
9220 Aalborg Ø, Denmark
Email: annai@cs.auc.dk

Bas Luttik
Department of Mathematics and Computer Science
Eindhoven Technical University
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
Email: luttik@win.tue.nl

Abstract

This paper confirms a conjecture of Bergstra and Klop's from 1984 by establishing that the process algebra obtained by adding an auxiliary operator proposed by Hennessy in 1981 to the recursion free fragment of Milner's Calculus of Communicationg Systems is not finitely based modulo bisimulation equivalence. Thus Hennessy's merge cannot replace the left merge and communication merge operators proposed by Bergstra and Klop, at least if a finite axiomatization of parallel composition is desired.

2000 MATHEMATICS SUBJECT CLASSIFICATION: 08A70, 03B45, 03C05, 68Q10, 68Q45, 68Q55, 68Q70.
CR SUBJECT CLASSIFICATION (1991): D.3.1, F.1.1, F.1.2, F.3.2, F.3.4, F.4.1.
KEYWORDS AND PHRASES: Concurrency, process algebra, CCS, bisimulation, Hennessy's merge, left merge, communication merge, parallel composition, equational logic, complete axiomatizations, non-finitely based algebras.

1 Introduction

Process algebras are prototype description languages for reactive systems that arose from the pioneering work of figures like Bergstra, Hoare, Klop and Milner. Well known examples of such languages are ACP [7], CCS [26], CSP [23] and Meije [5]. These algebraic description languages for processes differ in the basic collection of operators that they offer for building new process descriptions from existing ones. However, since they are designed to allow for the description and analysis of systems of interacting processes, they all contain some form of parallel composition (also known as merge) operator allowing one to put two process terms in parallel with one another. These operators usually interleave the behaviours of their arguments, and allow for some form of synchronization between them. For example, Milner's CCS offers the binary operator $|$, whose intended semantics is described by the following classic rules in Plotkin-style [32]:

$$\frac{x \xrightarrow{\mu} x'}{x \mid y \xrightarrow{\mu} x' \mid y} \qquad \frac{y \xrightarrow{\mu} y'}{x \mid y \xrightarrow{\mu} x \mid y'} \qquad \frac{x \xrightarrow{\alpha} x',\ y \xrightarrow{\bar{\alpha}} y'}{x \mid y \xrightarrow{\tau} x' \mid y'} \tag{1}$$

(In the above rules, the symbol μ stands for an action that a process may perform, α and $\bar{\alpha}$ are two observable actions that may synchronize, and τ is a symbol denoting the result of their synchronization.)

Although the above rules describe the behaviour of the parallel composition operator in very intuitive fashion, the equational characterization of this operator is not straightforward. In their seminal paper [22], Hennessy and Milner offered, amongst a wealth of other classic results, a complete equational axiomatization of bisimulation equivalence [31] over the recursion free fragment of CCS. The axiomatization proposed by Hennessy and Milner *ibidem* dealt with parallel composition using the so-called *expansion law*—a law that, intuitively, allows one to obtain a term describing the initial transitions of the parallel composition of two terms whose initial transitions are known. This law can be expressed as a conditional equation thus

$$\frac{x = \sum_{i \in I} \mu_i x_i,\ y = \sum_{j \in J} \gamma_j y_j}{x \mid y = \sum_{i \in I} \mu_i (x_i \mid y) + \sum_{j \in J} \gamma_j (x \mid y_j) + \sum_{i \in I, j \in J, \mu_i = \overline{\gamma_j}} \tau (x_i \mid y_j)}$$

(where I and J are two finite index sets, and the μ_i and γ_j are actions), and is nothing but an equational formulation of the aforementioned rules describing the operational semantics of parallel composition.

As already remarked, the expansion law, however, is a conditional equation, which may alternatively be viewed as an equation schema with a countably infinite number of instances. This raised the question of whether the parallel composition operator could be axiomatized in bisimulation semantics by means of a finite collection of equations. This question was answered positively by Bergstra and Klop, who gave in [8] a finite equational axiomatization of the merge operator in terms of the auxiliary left merge and communication merge operators. Moller showed

in [29, 30] that strong bisimulation equivalence is not finitely based over CCS and PA without the left merge operator. (The process algebra PA [8] contains a parallel composition operator based on pure interleaving without communication—viz. an operator described by the first two rules in (1)—and the left merge operator.) Thus auxiliary operators are necessary to obtain a finite axiomatization of parallel composition.

In the arguably less well known paper [21], Hennessy proposed an axiomatization of observation congruence [22] (also known as rooted weak bisimulation) and timed congruence (also known as split-2 congruence) over a CCS-like recursion free process language. (It is worth noting that, although this paper was published in 1988 by the SIAM Journal on Computing as [21], the results reported *ibidem* were actually obtained in 1981–1982.) Those axiomatizations used an auxiliary operator, denoted $\between$ by Hennessy, that is essentially a combination of the left and communication merge operators as its behaviour is described by the first and the last rule in (1). Apart from having soundness problems (see the reference [1] for a general discussion of this problem, and corrected proofs of Hennessy's results), the proposed axiomatization of observation congruence offered in *op. cit.* is *infinite*, as it used a variant of the expansion theorem from [22]. This led Bergstra and Klop to write in [8, page 118] that:

> "It seems that γ does not have a finite equational axiomatization."

(In *op. cit.* Bergstra and Klop used γ to denote Hennessy's merge.) To the best of our knowledge, the non-finite axiomatizability of Hennessy's merge has, however, never been proven. The main result in this paper confirms this conjecture of Bergstra and Klop's by showing that, in the presence of two distinct complementary actions, it is impossible to provide a finite axiomatization of the recursion free fragment of CCS modulo bisimulation using Hennessy's merge operator $\between$. We believe that this result further reinforces the status of the left merge and the communication merge operators as auxiliary operators in the finite equational characterization of parallel composition in bisimulation semantics.

The aforementioned negative result holds in a very strong form. Indeed, we prove that no finite collection of equations over the language we study that are sound with respect to bisimulation equivalence can prove all of the sound closed equalities of the form

$$e_n: \quad a\mathbf{0} \between p_n \;\approx\; ap_n + \sum_{i=0}^{n} \tau a^i \quad (n \geq 0) \ ,$$

where the terms p_n are defined thus:

$$p_n \;=\; \sum_{i=0}^{n} \bar{a} a^i \quad (n \geq 0) \ .$$

The proof of our main result is given along proof theoretic lines that have their roots in those for the aforementioned results of Moller's to the effect that bisimulation equivalence is not finitely based over the recursion free fragment of CCS.

However, the presence of possible synchronizations in the terms used in the family of equations e_n is necessary for our result, and requires careful attention in the proofs. (Indeed, in the absence of synchronization, Hennessy's merge reduces to Bergstra and Klop's left merge operator, and thus affords a finite equational axiomatization.) In particular, the infinite family of equations e_n and our arguments based upon it exploit the inability of any finite axiom system E that is sound with respect to bisimulation equivalence to "expand" the synchronization behaviour of terms of the form $p \between q$, for terms q that, like the terms p_n above eventually do, have a number of inequivalent "summands" that is larger than the maximum size of the terms mentioned in equations in E. As in the original arguments of Moller's, the root of this problem can be traced back to the fact that the choice operator $+$ distributes with respect to $\between$ in the first argument, but *not* in the second.

Related Work The equational characterization of different versions of the parallel composition operator is a classic topic in the theory of computation, and this paper joins the aforementioned seminal references in contributing to this line of research. In particular, the process algebraic literature abounds with results on equational axiomatizations of various notions of behavioural equivalences or preorders over languages incorporating some notion of parallel composition—see, e.g., the textbooks [7, 20, 26] and the classic papers [8, 22, 25] for general references. Early ω-complete axiomatizations are offered in [19, 28]. More recently, Fokkink and Luttik have shown in [17] that the process algebra PA [8] affords an ω-complete axiomatization that is finite if so is the underlying set of actions.

An analysis of the reasons why operators like the left merge and the communication merge are equationally well behaved in bisimulation semantics has led to general algorithms for the generation of (finite) equational axiomatizations for behavioural equivalences from their operational semantics—see, e.g., [3, 6] and the references in [4] for further details.

Parallel composition appears as the shuffle operator in the time-honoured theory of formal languages. Not surprisingly, the equational theory of shuffle has received considerable attention in the literature. Here we limit ourselves to mentioning some results that have a special relationship with process theory.

In [35], Tschantz offered a finite equational axiomatization of the theory of languages over concatenation and shuffle, solving an open problem raised by Pratt. In proving this result he essentially rediscovered the concept of pomset [33]—a model of concurrency based on partial orders whose algebraic aspects have been investigated by Gischer in [18]—, and proved that the equational theory of series-parallel pomsets coincides with that of languages over concatenation and shuffle. The argument adopted by Tschantz was based on the observation that series-parallel pomsets may be coded by a suitable homomorphism into languages, where the series and parallel composition operators on pomsets are modelled by the concatenation and shuffle operators on languages. Tschantz's technique of coding pomsets with languages homomorphically was further extended in the papers [10, 12, 13] to deal

with several other operators, infinite pomsets and infinitary languages, and sets of pomsets. The axiomatizations by Gischer and Tschantz have later been extended in [13, 16] to a two-sorted language with ω powers of the concatenation and parallel composition operators. The axiomatization of the algebra of pomsets resulting from the addition of these iteration operators is, however, necessarily infinite because, as shown in *op. cit.* no finite collection of equations can capture all the sound equalities involving them. (See [14] for closely related developments.)

The results of Moller's on the non-finite axiomatizability of bisimulation equivalence over the recursion free fragment of CCS and PA without the left merge operator given in [29, 30] are paralleled in the world of formal language theory by those offered in [9, 11, 15]. In the first of those references, Bloom and Ésik proved that the valid inequations in the algebra of languages equipped with concatenation and shuffle have no finite basis. Ésik and Bertol showed in [15] that the equational theory of union, concatenation and shuffle over languages has no finite first-order axiomatization relative to the collection of all valid inequations that hold for concatenation and shuffle. Hence the combination of some form of parallel composition, sequencing and choice is hard to characterize equationally both in the theory of languages and in that of processes. Moreover, Bloom and Ésik have shown in [11] that the variety of all languages over a finite alphabet ordered by inclusion with the operators of concatenation and shuffle, and a constant denoting the singleton language containing only the empty word is not finitely axiomatizable by first-order sentences that are valid in the the equational theory of languages over concatenation, union and shuffle.

Roadmap of the Paper We begin by presenting preliminaries on the language CCS_H—the extension of CCS with Hennessy's merge operator—and equational logic (Sect. 2). In particular, Sect. 2.2 offers a detailed discussion of the simplifying assumptions we shall make, without loss of generality, on the equational axiom systems that we shall consider in the rest of the paper. Our main result on the non-existence of a finite equational axiomatization for bisimulation equivalence over the language CCS_H (Theorem 3.1) is stated in Sect. 3. There we show how to reduce the proof of Theorem 3.1 to that of a proposition (Proposition 3.2) to the effect that no finite axiom system over the fragment of the language CCS_H that does not use the parallel composition operator can prove all of the aforementioned equations e_n. The following two technical sections of the paper, viz. Sects. 4 and 5, are entirely devoted to a detailed proof of Proposition 3.2. The paper ends with some concluding remarks (Sect. 6).

2 Preliminaries

We begin by introducing the basic definitions and results on which the technical developments to follow are based.

Table 1: SOS Rules for the CCS Operators ($\mu \in \{a, \bar{a}, \tau\}$ and $\alpha \in \{a, \bar{a}\}$)

$$\frac{}{\mu x \stackrel{\mu}{\to} x} \qquad \frac{x \stackrel{\mu}{\to} x'}{x + y \stackrel{\mu}{\to} x'} \qquad \frac{y \stackrel{\mu}{\to} y'}{x + y \stackrel{\mu}{\to} y'}$$

$$\frac{x \stackrel{\mu}{\to} x'}{x \mid y \stackrel{\mu}{\to} x' \mid y} \qquad \frac{y \stackrel{\mu}{\to} y'}{x \mid y \stackrel{\mu}{\to} x \mid y'} \qquad \frac{x \stackrel{\alpha}{\to} x',\ y \stackrel{\bar{\alpha}}{\to} y'}{x \mid y \stackrel{\tau}{\to} x' \mid y'}$$

2.1 The language CCS$_H$

The language for processes we shall consider in this paper, henceforth referred to as CCS$_H$, is obtained by adding Hennessy's merge operator from [21] to the recursion, restriction and relabelling free subset of Milner's CCS [26]. This language is given by the following grammar:

$$t ::= x \mid \mathbf{0} \mid at \mid \bar{a}t \mid \tau t \mid t + t \mid t \mid t \mid t \between t \ ,$$

where x is a variable drawn from a countably infinite set V, a is an action, and $\bar{a}$ is its complement. We assume that the actions a and $\bar{a}$ are distinct. Following Milner [26], the action symbol τ will result from the synchronized occurrence of the complementary actions a and $\bar{a}$. We let $\mu \in \{a, \bar{a}, \tau\}$ and $\alpha \in \{a, \bar{a}\}$. As usual, we postulate that $\bar{\bar{a}} = a$. We shall use the meta-variables t, u, v, w to range over process terms, and write $var(t)$ for the collection of variables occurring in the term t. The *size* of a term is the number of operator symbols in it. A process term is *closed* if it does not contain any variables. Closed terms will be typically denoted by p, q, r.

In order to obtain the negative results offered in this paper, it will be sufficient to consider the above language. The results we shall present in what follows carry over unchanged to a setting with an arbitrary number of actions, and corresponding unary prefixing operators.

A (closed) substitution is a mapping from process variables to (closed) CCS$_H$ terms. For every term t and (closed) substitution σ, the (closed) term obtained by replacing every occurrence of a variable x in t with the (closed) term $\sigma(x)$ will be written $\sigma(t)$.

In the remainder of this paper, we let a^0 denote $\mathbf{0}$, and a^{m+1} denote $a(a^m)$.

The SOS rules for all of the classic CCS operators are standard, and may be found in Table 1. Those for Hennessy's $\between$ formalize the intuition that this operator is indeed a combination of the left and communication merge operators, and are:

$$\frac{x \stackrel{\mu}{\to} x'}{x \between y \stackrel{\mu}{\to} x' \mid y} \qquad \frac{x \stackrel{\alpha}{\to} x',\ y \stackrel{\bar{\alpha}}{\to} y'}{x \between y \stackrel{\tau}{\to} x' \mid y'}$$

These transition rules give rise to transitions between CCS$_H$ terms. The operational semantics for CCS$_H$ is thus given by the labelled transition system [24] whose

states are CCS$_H$ terms, and whose labelled transitions are those that are provable using the rules. As usual, for each term t and action μ, we write $t \stackrel{\mu}{\rightarrow}$ if $t \stackrel{\mu}{\rightarrow} t'$ holds for some term t'.

The transition relations $\stackrel{\mu}{\rightarrow}$ naturally compose to determine the possible effects that performing a sequence of actions may have on a CCS$_H$ term.

Definition 2.1 For a sequence of actions $s = \mu_1 \cdots \mu_k$ ($k \geq 0$), and CCS$_H$ terms t, t', we write $t \stackrel{s}{\rightarrow} t'$ iff there exists a sequence of transitions

$$t = t_0 \stackrel{\mu_1}{\rightarrow} t_1 \stackrel{\mu_2}{\rightarrow} \cdots \stackrel{\mu_k}{\rightarrow} t_k = t' \ .$$

If $t \stackrel{s}{\rightarrow} t'$ holds for some CCS$_H$ term t', then s is a *trace* of t.

The *depth* of a term t, written $depth(t)$, is the length of the longest trace it affords.

The depth of closed terms can also be characterized inductively thus:

$$\begin{array}{rcl} depth(\mathbf{0}) & = & 0 \\ depth(\mu p) & = & 1 + depth(p) \\ depth(p+q) & = & \max\{depth(p), depth(q)\} \\ depth(p \mid q) & = & depth(p) + depth(q) \\ depth(p \between q) & = & \begin{cases} 0 & \text{if } depth(p) = 0 \ , \\ depth(p) + depth(q) & \text{otherwise} \ . \end{cases} \end{array}$$

In what follows, we shall sometimes need to consider the possible origins of a transition of the form $\sigma(t) \stackrel{\alpha}{\rightarrow} p$, for some action $\alpha \in \{a, \bar{a}\}$, closed substitution σ, CCS$_H$ term t and closed term p. Naturally enough, we expect that $\sigma(t)$ affords that transition if $t \stackrel{\alpha}{\rightarrow} t'$, for some t' such that $p = \sigma(t')$. However, the above transition may also derive from the initial behaviour of some closed term $\sigma(x)$, provided that the collection of initial moves of $\sigma(t)$ depends, in some formal sense, on that of the closed term substituted for the variable x. To fully describe this situation, we introduce the auxiliary notion of configuration of a CCS$_H$ term. To this end, we assume a set of symbols

$$V_d = \{x_d \mid x \in V\}$$

disjoint from V. Intuitively, the symbol x_d (read "during x") will be used to denote that the closed term substituted for variable x has begun executing.

Definition 2.2 The collection of *CCS$_H$ configurations* is given by the following grammar:

$$c ::= t \mid x_d \mid c \mid t \mid t \mid c \ ,$$

where t is a CCS$_H$ term, and $x_d \in V_d$.

For example, the configuration $x_d \mid (a\mathbf{0} \between x)$ is meant to describe a state of the computation of some term in which the (closed term substituted for the) occurrence of variable x on the left-hand side of the $\mid$ operator has begun its execution, but the

Table 2: SOS Rules for the Auxiliary Transitions $\xrightarrow{x}$ ($x \in V$)

$$\frac{}{x \xrightarrow{x} x_d} \qquad \frac{t \xrightarrow{x} c}{t + u \xrightarrow{x} c} \qquad \frac{u \xrightarrow{x} c}{t + u \xrightarrow{x} c}$$

$$\frac{t \xrightarrow{x} c}{t \mid u \xrightarrow{x} c \mid u} \qquad \frac{u \xrightarrow{x} c}{t \mid u \xrightarrow{x} t \mid c} \qquad \frac{t \xrightarrow{x} c}{t \not| u \xrightarrow{x} c \mid u}$$

one on the right-hand side has not. We shall consider the symbols x_d as variables, and use the notation $\sigma[x_d \mapsto p]$, where σ is a closed substitution and p is a closed CCS$_H$ term, to stand for the substitution mapping x_d to p, and acting like σ on all of the variables in V.

The way in which the initial behaviour of a term may depend on that of the variables that occur in it is formally described by an auxiliary transition relation whose elements have the form $t \xrightarrow{x} c$, where t is a term, x is a variable, and c is a configuration. The SOS rules defining these transitions are given in Table 2.

Lemma 2.1 Assume that t is a CCS$_H$ term, σ is a closed substitution and $\alpha \in \{a, \bar{a}\}$. Then the following statements hold:

1. If $t \xrightarrow{\alpha} t'$, then $\sigma(t) \xrightarrow{\alpha} \sigma(t')$.
2. Assume that $t \xrightarrow{x} c$ and $\sigma(x) \xrightarrow{\alpha} p$, for some closed term p. Then $\sigma(t) \xrightarrow{\alpha} \sigma[x_d \mapsto p](c)$.
3. Assume that $\sigma(t) \xrightarrow{\alpha} p$, for some closed term p. Then
   - either $t \xrightarrow{\alpha} t'$ for some t' such that $p = \sigma(t')$
   - or $t \xrightarrow{x} c$ and $\sigma(x) \xrightarrow{\alpha} q$, for some variable x, configuration c and closed term q such that $\sigma[x_d \mapsto q](c) = p$.

In this paper, we shall consider the language CCS$_H$ modulo bisimulation equivalence [26, 31].

Definition 2.3 *Bisimulation equivalence* (also sometimes referred to as *bisimilarity*), denoted by $\leftrightarrow$, is the largest symmetric relation over closed CCS$_H$ terms such that whenever $p \leftrightarrow q$ and $p \xrightarrow{\mu} p'$, then there is a transition $q \xrightarrow{\mu} q'$ with $p' \leftrightarrow q'$.

If $p \leftrightarrow q$, then we say that p and q are *bisimilar*.

It is well-known that, as the name suggests, bisimulation equivalence is indeed an equivalence relation (see, e.g., the references [26, 31]). Moreover, two bisimulation equivalent terms over the language CCS$_H$ afford the same finite non-empty set of traces, and have therefore the same depth. Since the SOS rules defining the operational semantics of the language CCS$_H$ are in de Simone's format [34], we have that:

Fact 2.1 Bisimulation equivalence is a congruence over the language CCS_H.

Bisimulation equivalence is extended to arbitrary CCS_H terms thus:

Definition 2.4 Let t, u be CCS_H terms. Then $t \leftrightarrow u$ iff $\sigma(t) \leftrightarrow \sigma(u)$ for every closed substitution σ.

For instance, we have that

$$\mathbf{0} \between x \leftrightarrow \mathbf{0}$$

because $\mathbf{0} \between p$ affords no transition, for each closed term p.

Definition 2.5 We say that a term t has a $\mathbf{0}$ *factor* if it contains a subterm of the form $t' \mid t''$ or $t' \between t''$, where either t' or t'' is bisimilar to $\mathbf{0}$.

For example, the terms $a(\mathbf{0} \mid x)$ and $(\mathbf{0} \between x) \mid y$ have a $\mathbf{0}$ factor.

2.2 Equational Logic

An *axiom system* is a collection of equations $t \approx u$ over the language CCS_H. An equation $p \approx q$ is derivable from an axiom system E, notation $E \vdash p \approx q$, if it can be proven from the axioms in E using the rules of equational logic (viz. reflexivity, symmetry, transitivity, substitution and closure under CCS_H contexts):

$$t \approx t \quad \frac{t \approx u}{u \approx t} \quad \frac{t \approx u \;\; u \approx v}{t \approx v} \quad \frac{t \approx u}{\sigma(t) \approx \sigma(u)} \quad \frac{t \approx u}{\mu t \approx \mu u}$$

$$\frac{t \approx u \;\; t' \approx u'}{t + t' \approx u + u'} \quad \frac{t \approx u \;\; t' \approx u'}{t \between t' \approx u \between u'} \quad \frac{t \approx u \;\; t' \approx u'}{t \mid t' \approx u \mid u'} \;\; .$$

Without loss of generality one may assume that substitutions happen first in equational proofs, i.e., that the rule

$$\frac{t \approx u}{\sigma(t) \approx \sigma(u)}$$

may only be used when $(t \approx u) \in E$. In this case $\sigma(t) \approx \sigma(u)$ is called a *substitution instance* of an axiom in E.

Definition 2.6 We call a closed substitution σ *substantial* if $depth(\sigma(x)) > 0$ for each variable x.

For reasons of technical convenience, in the proofs of our non-finite axiomatizability results presented in this paper we shall only allow for the use of closed substantial substitutions in the rule of substitution. This does not limit the generality of those results because every finite equational axiomatization E can be converted into a finite equational axiomatization E' such that the closed substitution instances of the axioms of E are the same as the closed substantial substitution instances of the axioms of E' (when equating any closed subterm of depth 0 with $\mathbf{0}$). This is

Table 3: Some Axioms for CCS_H

A1	$x + y$	$\approx$	$y + x$
A2	$(x + y) + z$	$\approx$	$x + (y + z)$
A3	$\mathbf{0} + x$	$\approx$	x
A4	$x + \mathbf{0}$	$\approx$	x
HM1	$\mathbf{0} \between x$	$\approx$	$\mathbf{0}$
HM2	$x \between \mathbf{0}$	$\approx$	x
M1	$x \mid \mathbf{0}$	$\approx$	x
M2	$\mathbf{0} \mid x$	$\approx$	x

done by including in E' any equation that can be obtained from an equation in E by replacing all occurrences of any number of variables by $\mathbf{0}$. (The identification of each CCS_H term that is bisimilar to $\mathbf{0}$ with $\mathbf{0}$ can be done equationally using three equations. See Fact 2.2 to follow.)

Definition 2.7 We say that a substitution σ is a $\mathbf{0}$-*substitution* iff $\sigma(x) \neq x$ implies that $\sigma(x) = \mathbf{0}$, for each variable x.

An axiom system E is *closed with respect to* $\mathbf{0}$-*substitutions* iff $\sigma(t) \approx \sigma(u)$ is contained in E, for each $\mathbf{0}$-substitution σ, if so is $t \approx u$.

Simplifying Assumption 1 In the remainder of this paper, we shall always tacitly assume that equational axiom systems are closed with respect to $\mathbf{0}$-substitutions.

Note that if E is a finite axiom system, then so is its closure with respect to $\mathbf{0}$-substitutions. In fact, for each term t, the collection of terms

$$\{\sigma(t) \mid \sigma \text{ a } \mathbf{0}\text{-substitution}\}$$

is finite.

Moreover, by postulating that for each axiom in E also its symmetric counterpart is present in E, one may assume that applications of symmetry happen first in equational proofs.

Simplifying Assumption 2 In the remainder of this paper, we shall also tacitly assume that our equational axiom systems are closed with respect to symmetry.

Definition 2.8 An equation $t \approx u$ over the language CCS_H is *sound* with respect to $\underline{\leftrightarrow}$ iff $t \underline{\leftrightarrow} u$. An axiom system is sound with respect to $\underline{\leftrightarrow}$ iff so is each of its equations.

An example of a collection of equations over the language CCS_H that are sound with respect to $\underline{\leftrightarrow}$ is given in Table 3. In addition, the following law, which ex-

presses the parallel composition operator in terms of Hennessy's merge, is easily seen to be sound with respect to $\underline{\leftrightarrow}$:

$$x \mid y \approx (x \between y) + (y \between x) \ . \tag{2}$$

The axioms A4, HM1 and M1 in Table 3 (used from left to right) are enough to establish that each CCS_H term that is bisimilar to $\mathbf{0}$ is also provably equal to $\mathbf{0}$. Since we feel that the proof of this little result is instructive, we now proceed to present its sketch.

Fact 2.2 Let t be a CCS_H term. Then $t \underline{\leftrightarrow} \mathbf{0}$ if, and only if, the equation $t \approx \mathbf{0}$ is provable using axioms A4, HM1 and M1 in Table 3 from left to right.

Proof: The "if" implication is an immediate consequence of the soundness of the equations A4, HM1 and M1 with respect to $\underline{\leftrightarrow}$. To prove the "only if" implication, define, first of all, the collection NIL of CCS_H terms as the set of terms generated by the following grammar:

$$t ::= \mathbf{0} \mid t + t \mid t \mid t \mid t \between u \ ,$$

where u is an arbitrary CCS_H term. We claim that:

Claim 1 Each CCS_H term t is bisimilar to $\mathbf{0}$ if, and only if, $t \in$ NIL.

Using this claim and structural induction on $t \in$ NIL, it is a simple matter to show that if $t \underline{\leftrightarrow} \mathbf{0}$, then $t \approx \mathbf{0}$ is provable using axioms A4, HM1 and M1 from left to right, which was to be shown.

To complete the proof, it therefore suffices to show the above claim. To establish the "if" implication in the statement of the claim, one proves, using structural induction on t and the congruence properties of bisimilarity (Fact 2.1), that if $t \in$ NIL, then $\sigma(t) \underline{\leftrightarrow} \mathbf{0}$ for every closed substitution σ. To show the "only if" implication, we establish the contrapositive statement, viz. that if $t \notin$ NIL, then $\sigma(t) \not\underline{\leftrightarrow} \mathbf{0}$ for some closed substitution σ. To this end, it suffices only to show, using structural induction on t, that if $t \notin$ NIL, then $\sigma_a(t) \stackrel{\mu}{\rightarrow}$ for some action $\mu \in \{a, \bar{a}, \tau\}$, where σ_a is the closed substitution mapping each variable to the closed term $a\mathbf{0}$. The details of this argument are not hard, and are therefore left to the reader. □

In light of the above result, we find it convenient to make the following:

Simplifying Assumption 3 In the technical developments to follow, we shall assume, without loss of generality, that each axiom system we consider includes the equations in Table 3.

This assumption means, in particular, that our axiom systems will allow us to identify each term that is bisimilar to $\mathbf{0}$ with $\mathbf{0}$.

In the remainder of this paper, process terms are considered modulo associativity and commutativity of +. In other words, we do not distinguish $t + u$ and $u + t$, nor $(t + u) + v$ and $t + (u + v)$. This is justified because, as previously observed, bisimulation equivalence satisfies axioms A1, A2 in Table 3. In what follows, the symbol $=$ will denote equality modulo axioms A1, A2. We use a *summation* $\sum_{i\in\{1,\ldots,k\}} t_i$ to denote $t_1 + \cdots + t_k$, where the empty sum represents $\mathbf{0}$. It is easy to see that, modulo the equations in Table 3, every CCS_H term t has the form $\sum_{i\in I} t_i$, for some finite index set I, and terms t_i ($i \in I$) that are not $\mathbf{0}$ and do not have themselves the form $t' + t''$, for some terms t' and t''. The terms t_i ($i \in I$) will be referred to as the *summands* of t. Moreover, again modulo the equations in Table 3, each of the t_i can be assumed to have no $\mathbf{0}$ factors. (Recall that this means that, whenever a term of the form $t' \between t''$ or $t' \mid t''$ is a subterm of t_i, then $t' \not\leftrightarrow \mathbf{0}$ and $t'' \not\leftrightarrow \mathbf{0}$.) For example, a term of the form $(a\mathbf{0} + \bar{a}\mathbf{0}) \mid \mathbf{0}$ will *not* be considered a summand in what follows because, using equation M1 in Table 3, that term can be proven equal to $a\mathbf{0} + \bar{a}\mathbf{0}$. The collection of summands of a term t can be inductively characterized thus:

- $\mathbf{0}$ has no summands;
- x and μt are their only summands;
- u is a summand of $t_1 + t_2$ if it is either a summand of t_1 or a summand of t_2;
- the summands of $t_1 \mid t_2$ are
  - those of t_2, if $t_1 \leftrightarrow \mathbf{0}$,
  - those of t_1, if $t_2 \leftrightarrow \mathbf{0}$, and
  - only $t_1 \mid t_2$, otherwise;
- the summands of $t_1 \between t_2$ are
  - none, if $t_1 \leftrightarrow \mathbf{0}$,
  - those of t_1, if $t_2 \leftrightarrow \mathbf{0}$, and
  - only $t_1 \between t_2$, otherwise.

It is well-known (cf., e.g., Sect. 2 in [19]) that if an equation relating two closed terms can be proven from an axiom system E, then there is a closed proof for it. We shall now argue that if E satisfies a further closure property in addition to those mentioned earlier, and that closed equation relates two terms containing no occurrences of $\mathbf{0}$ as a summand or factor, then there is a closed proof for it in which all of the terms have no occurrences of $\mathbf{0}$ as a summand or factor—see [28, Proposition 5.1.5].

Definition 2.9

1. For CCS$_H$ terms t and t', we write $t \rightsquigarrow t'$ if t' can be obtained from t by applying one of the equations A3, A4, HM1, HM2, M1 and M2 from left to right. As usual, we write $\rightsquigarrow^*$ for the reflexive, transitive closure of the relation $\rightsquigarrow$.

2. Let E be an axiom system. We define the axiom system $\mathrm{cl}(E)$ thus:

$$\mathrm{cl}(E) = \{t' \approx u' \mid (t \approx u) \in E,\ t \rightsquigarrow^* t' \text{ and } u \rightsquigarrow^* u'\} \ .$$

3. An axiom system E is *saturated* if $E = \mathrm{cl}(E)$.

Intuitively, one application of the rewrite relation $\rightsquigarrow$ eliminates one occurrence of $\mathbf{0}$ as a summand or a factor in terms. Note that $t \underline{\leftrightarrow} t'$ holds whenever $t \rightsquigarrow t'$.

The following lemma collects some basic sanity properties of the closure operator $\mathrm{cl}(\cdot)$. (Note, in particular, that the application of $\mathrm{cl}(\cdot)$ to an axiom system satisfying our simplifying assumptions is guaranteed to produce a saturated axiom system that also affords them.)

Lemma 2.2 Let E be an axiom system. Then the following statements hold.

1. $E \subseteq \mathrm{cl}(E) = \mathrm{cl}(\mathrm{cl}(E))$.
2. $\mathrm{cl}(E)$ is finite, if so is E.
3. $\mathrm{cl}(E)$ is sound, if so is E.
4. $\mathrm{cl}(E)$ is closed with respect to $\mathbf{0}$ substitutions and symmetry, if so is E.
5. $\mathrm{cl}(E)$ and E prove the same equations, if E contains the equations in Table 3.

Proof: We limit ourselves to sketching a proof of the second statement in the lemma. To prove this claim, we begin by noting that the size of the term t' is smaller than that of t whenever $t \rightsquigarrow t'$. Using this observation, it is not hard to see that, for each term t, the set

$$\{t' \mid t \rightsquigarrow^* t'\}$$

is finite. In fact, the rooted tree with root t resulting from the unfolding of the directed acyclic graph whose nodes are the terms reachable from t via $\rightsquigarrow^*$, and whose edges are given by the $\rightsquigarrow$ relation is finitely branching, and all of its paths are finite because the $\rightsquigarrow$ relation decreases the size of terms. Thus this tree must be finite, or else it would have an infinite path by König's lemma. It follows that, for each equation $t \approx u$ in E, the set $\mathrm{cl}(E)$ contains nm equations, where n and m are the cardinalities of the sets $\{t' \mid t \rightsquigarrow^* t'\}$ and $\{u' \mid u \rightsquigarrow^* u'\}$, respectively. We may therefore conclude that $\mathrm{cl}(E)$ is finite, if so is E. □

We now proceed to characterize syntactically the normal forms of the rewriting relation $\rightsquigarrow$. The syntactic characterization of the normal forms given below will be useful in obtaining the promised result to the effect that if a saturated axiom system

E proves a closed equation relating two terms containing no occurrences of $\mathbf{0}$ as a summand or factor, then there is a closed proof for it in which all of the terms have no occurrences of $\mathbf{0}$ as a summand or factor.

Definition 2.10 For each CCS_H term t, we define $t/\mathbf{0}$ thus:

$$\begin{array}{rclcrcl}
\mathbf{0}/\mathbf{0} & = & \mathbf{0} & \qquad & (t+u)/\mathbf{0} & = & \begin{cases} u/\mathbf{0} & \text{if } t \underline{\leftrightarrow} \mathbf{0} \\ t/\mathbf{0} & \text{if } u \underline{\leftrightarrow} \mathbf{0} \\ (t/\mathbf{0}) + (u/\mathbf{0}) & \text{otherwise} \end{cases} \\
x/\mathbf{0} & = & x & & (t \between u)/\mathbf{0} & = & \begin{cases} \mathbf{0} & \text{if } t \underline{\leftrightarrow} \mathbf{0} \\ t/\mathbf{0} & \text{if } u \underline{\leftrightarrow} \mathbf{0} \\ (t/\mathbf{0}) \between (u/\mathbf{0}) & \text{otherwise} \end{cases} \\
\mu t/\mathbf{0} & = & \mu(t/\mathbf{0}) & & (t \mid u)/\mathbf{0} & = & \begin{cases} u/\mathbf{0} & \text{if } t \underline{\leftrightarrow} \mathbf{0} \\ t/\mathbf{0} & \text{if } u \underline{\leftrightarrow} \mathbf{0} \\ (t/\mathbf{0}) \mid (u/\mathbf{0}) & \text{otherwise} \end{cases}
\end{array} .$$

Intuitively, $t/\mathbf{0}$ is the term that results by removing *all* occurrences of $\mathbf{0}$ as a summand or factor from t.

The following lemma, whose simple proof by structural induction on terms is omitted, collects the basic properties of the above construction. In particular, note that, as expected, the term $t/\mathbf{0}$ is the normal form for t with respect to the rewrite relation $\rightsquigarrow$.

Lemma 2.3 For each CCS_H term t, the following statements hold:

1. $t \rightsquigarrow^* t/\mathbf{0}$ and therefore $t \underline{\leftrightarrow} t/\mathbf{0}$;
2. $t/\mathbf{0} \rightsquigarrow u$ for no term u;
3. the term $t/\mathbf{0}$ has no occurrence of $\mathbf{0}$ as a summand or factor;
4. $t/\mathbf{0} = t$, if t has no occurrence of $\mathbf{0}$ as a summand or factor.

We are now ready to state our counterpart of [28, Proposition 5.1.5].

Proposition 2.1 Assume that E is a saturated axiom system. Suppose furthermore that we have a closed proof from E of the closed equation $p \approx q$. Then replacing each term r in that proof with $r/\mathbf{0}$ yields a closed proof of the equation $p/\mathbf{0} \approx q/\mathbf{0}$. In particular, the proof from E of an equation $p \approx q$, where p and q are terms not containing occurrences of $\mathbf{0}$ as a summand or factor, need not use terms containing occurrences of $\mathbf{0}$ as a summand or factor.

Proof: The proof follows the lines of that of [28, Proposition 5.1.5], and is therefore omitted. □

In light of this result, since the saturation of a finite axiom system that includes the equations in Table 3 results in an equivalent, finite collection of equations (Lemma 2.2(2) and (5)), we put forth our last:

Simplifying Assumption 4 Henceforth, we shall limit ourselves to considering saturated axiom systems.

The use of saturated axiom systems will play an important role in the proof of our main technical results.

3 Hennessy's Merge is not Finitely Based

Our order of business in the remainder of this paper will be to show the following result to the effect that bisimulation equivalence does *not* admit a finite equational axiomatization over the language CCS_H, and that thus Bergstra and Klop were indeed right in writing in [8, page 118] that:

> "It seems that γ does not have a finite equational axiomatization."

(In *op. cit.* Bergstra and Klop used γ to denote Hennessy's merge.)

Theorem 3.1 Bisimulation equivalence admits no finite equational axiomatization over the language CCS_H. In fact, the collection of *closed* equations over that language that hold with respect to bisimulation equivalence has no finite equational axiomatization.

As a first stepping stone towards the proof of this result, we now proceed to argue that it is sufficient to show that bisimulation equivalence admits no finite equational axiomatization over the language CCS_H^-, consisting of the CCS_H terms that do not contain occurrences of the parallel composition operator. Even though this observation is not unexpected—as equation (2) essentially states that parallel composition is a derived operator in the algebra of CCS_H terms modulo bisimulation equivalence—, we now argue for it in some detail for the sake of completeness.

Definition 3.1 For each CCS_H term t, we define $\hat{t}$ thus:

$$\begin{array}{rclcrcl} \hat{\mathbf{0}} & = & \mathbf{0} & \qquad & \widehat{t+u} & = & \hat{t}+\hat{u} \\ \hat{x} & = & x & & \widehat{t \between u} & = & \hat{t} \between \hat{u} \\ \widehat{\mu t} & = & \mu \hat{t} & & \widehat{t \mid u} & = & (\hat{t} \between \hat{u}) + (\hat{u} \between \hat{t}) \end{array} \quad .$$

If E is an axiom system over the language CCS_H, then

$$\widehat{E} = \{\hat{t} \approx \hat{u} \mid (t \approx u) \in E\} \ .$$

Note that, for each CCS_H term t, the term $\hat{t}$ is in the language CCS_H^-. Moreover, if t contains no occurrences of the parallel composition operator, then $\hat{t} = t$. Since equation (2) is sound with respect to bisimulation equivalence, and bisimilarity is a congruence (Fact 2.1), it is not hard to show that:

Fact 3.1 Each term t in the language CCS_H is bisimilar to $\hat{t}$. Therefore if E is an axiom system over the language CCS_H that is sound with respect to bisimilarity, then $\widehat{E}$ is an axiom system over the language CCS_H^- that is sound with respect to bisimilarity.

The following result states the promised reduction of the non-finite axiomatizability of bisimilarity over the language CCS_H to that of bisimilarity over the language CCS_H^-.

Proposition 3.1 Let E be an axiom system over the language CCS_H. Then the following statements hold.

1. If E proves the equation $t \approx u$, then $\widehat{E}$ proves the equation $\hat{t} \approx \hat{u}$.
2. If E gives a complete axiomatization of bisimulation equivalence over the language CCS_H, then $\widehat{E}$ completely axiomatizes bisimulation equivalence over the language CCS_H^-.
3. If bisimulation equivalence admits no finite equational axiomatization over the language CCS_H^-, then it has no finite equational axiomatization over the language CCS_H either.

Proof: We prove the three statements separately.

- PROOF OF STATEMENT 1. Assume that $E \vdash t \approx u$. We shall argue that $\widehat{E}$ proves the equation $\hat{t} \approx \hat{u}$ by induction on the depth of the proof of $t \approx u$ from E. We proceed by a case analysis on the last rule used in the proof. Below we only consider the two most interesting cases in this analysis.
  - CASE $E \vdash t \approx u$, BECAUSE $\sigma(t') = t$ AND $\sigma(u') = u$ FOR SOME EQUATION $(t' \approx u') \in E$. Note, first of all, that, by the definition of $\widehat{E}$, the equation $\widehat{t'} \approx \widehat{u'}$ is contained in $\widehat{E}$. Observe now that

    $$\hat{t} = \hat{\sigma}(\widehat{t'}) \text{ and } \hat{u} = \hat{\sigma}(\widehat{u'}) \ ,$$

    where $\hat{\sigma}$ is the substitution mapping each variable x to the term $\widehat{\sigma(x)}$. It follows that the equation $\hat{t} \approx \hat{u}$ can be proven from the axiom system $\widehat{E}$ by instantiating the equation $\widehat{t'} \approx \widehat{u'}$ with the substitution $\hat{\sigma}$, and we are done.
  - CASE $E \vdash t \approx u$, BECAUSE $t = t_1 \mid t_2$ AND $u = u_1 \mid u_2$ FOR SOME t_i, u_i $(i = 1, 2)$ SUCH THAT $E \vdash t_i \approx u_i$ $(i = 1, 2)$. Using the inductive hypothesis twice, we have that $\widehat{E} \vdash \widehat{t_i} \approx \widehat{u_i}$ $(i = 1, 2)$. Therefore, using substitutivity, $\widehat{E}$ proves that

    $$\hat{t} = (\widehat{t_1} \between \widehat{t_2}) + (\widehat{t_2} \between \widehat{t_1}) \approx (\widehat{u_1} \between \widehat{u_2}) + (\widehat{u_2} \between \widehat{u_1}) = \hat{u} \ ,$$

    which was to be shown.

The remaining cases are simpler, and we leave the details to the reader.

- PROOF OF STATEMENT 2. Assume that t and u are two bisimilar terms in the language CCS_H^-. We shall argue that $\widehat{E}$ proves the equation $t \approx u$. To this end, we begin by noting that the equation $t \approx u$ also holds in the algebra of CCS_H terms modulo bisimulation. In fact, for each term v in the language CCS_H and closed substitution σ mapping variables to CCS_H terms, we have that

  $$\sigma(v) \leftrightarrow \hat{\sigma}(v) \ ,$$

  where the substitution $\hat{\sigma}$ is defined as above.

  Since E is complete for bisimilarity over CCS_H by our assumptions, it follows that E proves the equation $t \approx u$. Therefore, by statement 1 of the proposition, we have that $\widehat{E}$ proves the equation $\hat{t} \approx \hat{u}$. The claim now follows because $\hat{t} = t$ and $\hat{u} = u$.

- PROOF OF STATEMENT 3. This is an immediate consequence of statement 2 because $\widehat{E}$ has the same cardinality of E, and is therefore finite, if so is E.

□

In light of this result, henceforth we shall focus on proving that bisimulation equivalence affords no finite equational axiomatization over the language CCS_H^-. The following infinite family of closed CCS_H^- terms will play a key role in the technical developments to follow:

$$e_n : \quad a\mathbf{0} \between p_n \quad \approx \quad ap_n + \sum_{i=0}^{n} \tau a^i \quad (n \geq 0) \ , \tag{3}$$

where the terms p_n are defined thus:

$$p_n \quad = \quad \sum_{i=0}^{n} \bar{a} a^i \quad (n \geq 0) \ .$$

It is not hard to see that all of the equations e_n ($n \geq 0$) are sound modulo bisimulation. In the remainder of this paper, we shall prove the following result, of which Theorem 3.1 is an immediate consequence, to the effect that no finite collection of equations over the language CCS_H^- that are sound with respect to bisimulation equivalence can prove all of the equations e_n ($n \geq 0$).

Theorem 3.2 Let E be a finite axiom system over the language CCS_H^- that is sound with respect to bisimulation equivalence. Let n be larger than the size of each term in the equations in E. Then E does not prove the sound equation e_n from (3).

The remainder of this paper will be devoted to a proof of the above result, which will be given along proof theoretic lines that have their roots in Moller's arguments to the effect that bisimulation equivalence is not finitely based over the language CCS—see the references [28, 29, 30]. More precisely, to establish Theorem 3.2, we shall show that there is a property of terms associated with each finite axiom system E over the language CCS_H^- that is sound with respect to bisimulation equivalence, such that whenever the equation $p \approx q$ can be derived from E, for some "suitably large" closed terms without $\mathbf{0}$ summands and factors, then either both p and q enjoy the property, or none of them does. The aforementioned property must be chosen so that, for suitably large values of n, the right-hand side of equality e_n, viz. the term $a\mathbf{0} \between p_n$, affords it, whilst the left-hand side, viz. the term $ap_n + \sum_{i=0}^{n} \tau a^i$, does not.

Remark 3.1 In the absence of synchronization, Hennessy's merge reduces to the left merge operator of Bergstra and Klop's. It follows that the collection of closed equations that hold modulo $\leftrightarrows$ over the sub-language of CCS_H obtained by considering those terms that do not contain occurrences of the $\bar{a}$ prefixing operator has a finite equational axiomatization. Therefore the use of synchronization is necessary in the proof of Theorem 3.1.

The following proposition states the property mentioned in the proof strategy outlined above.

Proposition 3.2 Let E be a finite axiom system over the language CCS_H^- that is sound with respect to bisimulation equivalence. Let n be larger than the size of each term in the equations in E. Assume that p and q are closed terms that are bisimilar to $a\mathbf{0} \between p_n$, and contain no occurrences of $\mathbf{0}$ as a summand or a factor. If $E \vdash p \approx q$ and p has a summand bisimilar to $a\mathbf{0} \between p_n$, then so does q.

Using the above proposition, it is a simple matter to prove Theorem 3.2. In fact, since none of the summands of the term

$$ap_n + \sum_{i=0}^{n} \tau a^i \ ,$$

viz. ap_n and τa^i ($i \in \{0, \ldots, n\}$), is bisimilar to $a\mathbf{0} \between p_n$, if $n \geq 1$, Proposition 3.2 yields that the sound equality e_n cannot be proven from E, and thus that E is incomplete.

We shall now begin to develop the technical machinery that will be brought to bear in the proof of Proposition 3.2. This proof will occupy the remainder of this study.

4 Preparatory Results and Observations

Note that terms in the language CCS_H^- may contain some occurrences of variables that can never contribute to the behaviour of their closed instantiations. A typical example of this situation occurs in the term $\mathbf{0} \between x$, which is bisimilar to $\mathbf{0}$.

However, terms that have no $\mathbf{0}$ factors contain no such redundant occurrences of variables. Moreover, each variable occurring in such terms contributes to the behaviour of its closed substantial instantiations. The following basic result, that will be used repeatedly in the technical developments to follow, formalizes this intuition.

Lemma 4.1 Let t be a CCS_H^- term, and let σ be a closed substitution.

1. Assume that t is not bisimilar to $\mathbf{0}$, and σ is substantial. Then $depth(\sigma(t))$ is positive, and thus $\sigma(t) \not\leftrightarrow \mathbf{0}$.

2. If t has no $\mathbf{0}$ factors and $x \in var(t)$, then $depth(\sigma(t)) \geq depth(\sigma(x))$.

Remark 4.1 The requirement that σ be substantial is necessary in statement 1 of the above lemma. For example, $x \not\leftrightarrow \mathbf{0}$, but $\sigma(x) \leftrightarrow \mathbf{0}$ if $depth(\sigma(x)) = 0$.

Similarly, the proviso that t has no $\mathbf{0}$ factors cannot be omitted in statement 2. For instance, if $t = \mathbf{0} \between x$ and $\sigma(x) = a\mathbf{0}$, then $depth(\sigma(t)) < depth(\sigma(x))$.

In the proof of our main result, we shall make use of some notions from [27, 28]. These we now proceed to introduce for the sake of completeness and readability.

Definition 4.1 A closed term p is *irreducible* if $p \leftrightarrow q \mid r$ implies $q \leftrightarrow \mathbf{0}$ or $r \leftrightarrow \mathbf{0}$, for all closed terms q, r.

We say that p is *prime* if it is irreducible and is not bisimilar to $\mathbf{0}$.

For example, each term p of depth 1 is prime because every term of the form $q \mid r$ that does not involve $\mathbf{0}$ factors has depth at least 2, and thus cannot be bisimilar to p. The following proposition states the primality of two families of closed terms that will play a key role in the proof of our main result.

Proposition 4.1

1. Let $m \geq 1$ and $0 \leq i_1 < \ldots < i_m$. Then the term $\bar{a}.a^{i_1} + \cdots + \bar{a}.a^{i_m}$ is prime. In particular, p_n is prime, for each $n \geq 1$.

2. The term $a\mathbf{0} \between p_n$ is prime, for each $n \geq 0$.

Proof: We prove the two claims separately. In each case, since $\bar{a}.a^{i_1} + \cdots + \bar{a}.a^{i_m}$ and $a\mathbf{0} \between p_n$ are not bisimilar to $\mathbf{0}$, it suffices only to show that the relevant term is irreducible.

- PROOF OF CLAIM 1. Suppose, towards a contradiction, that there exist closed terms q, r that are not bisimilar $\mathbf{0}$ such that

$$\bar{a}.a^{i_1} + \cdots + \bar{a}.a^{i_m} \leftrightarrow q \mid r \ .$$

  Then, since $q, r \not\leftrightarrow \mathbf{0}$, in light of the above equivalence we have that $q \stackrel{\bar{a}}{\rightarrow} q'$ and $r \stackrel{\bar{a}}{\rightarrow} r'$, for some q', r'. But then it follows that

$$q \mid r \stackrel{\bar{a}}{\rightarrow} q' \mid r \stackrel{\bar{a}}{\rightarrow} q' \mid r' \ ,$$

whereas the term $\bar{a}.a^{i_1} + \cdots + \bar{a}.a^{i_m}$ cannot perform two subsequent $\bar{a}$-transitions. It follows that such q and r cannot exist, and hence that the term $\bar{a}.a^{i_1} + \cdots + \bar{a}.a^{i_m}$ is irreducible, which was to be shown.

- PROOF OF CLAIM 2. We now proceed to prove that $a\mathbf{0} \between p_n$ is irreducible for $n \geq 0$.

  If $n = 0$ then $a\mathbf{0} \between p_0 = a\mathbf{0} \between \mathbf{0}$ is a term of depth 1, and is therefore irreducible as claimed.

  Let $n \geq 1$. Assume, towards a contradiction, that $a\mathbf{0} \between p_n \leftrightarrow p \mid q$ for two closed terms p and q with $p \not\leftrightarrow \mathbf{0}$ and $q \not\leftrightarrow \mathbf{0}$—that is, $a\mathbf{0} \between p_n$ is *not* irreducible. Since $n \geq 1$, we have that

  $$a\mathbf{0} \between p_n \xrightarrow{\tau} \mathbf{0} \mid \mathbf{0} \leftrightarrow \mathbf{0} \ .$$

  As $a\mathbf{0} \between p_n \leftrightarrow p \mid q$, there is a transition $p \mid q \xrightarrow{\tau} p' \mid q'$, for some p', q' with $p' \mid q' \leftrightarrow \mathbf{0}$. In light of our assumption that $p \not\leftrightarrow \mathbf{0}$ and $q \not\leftrightarrow \mathbf{0}$, the transition $p \mid q \xrightarrow{\tau} p' \mid q'$ must be derived from the synchronization of two transitions $p \xrightarrow{\alpha} p'$ and $q \xrightarrow{\bar{\alpha}} q'$ with $\alpha \in \{a, \bar{a}\}$. This means that $p \mid q \xrightarrow{\bar{a}}$, contradicting the assumption that $a\mathbf{0} \between p_n \leftrightarrow p \mid q$. Thus $a\mathbf{0} \between p_n$ is irreducible, which was to be shown.

□

Lemma 4.2 Let t be a term in the language CCS_H^- with neither $\mathbf{0}$ summands nor factors that does not have $+$ as head operator. Assume that σ is a closed substantial substitution, and that

$$\sigma(t) \leftrightarrow \bar{a}.a^{i_1} + \cdots + \bar{a}.a^{i_m} \ ,$$

for some $m > 1$ and $0 \leq i_1 < \ldots < i_m$. Then $t = x$, for some variable x.

Proof: Assume, towards a contradiction, that t is not a variable. We proceed by a case analysis on the possible form this term may have.

1. CASE $t = \mu t'$ FOR SOME TERM t'. Then $\mu = \bar{a}$ and $a^{i_1} \leftrightarrow \sigma(t') \leftrightarrow a^{i_m}$. However, this is a contradiction because, since $i_1 \neq i_m$, the terms a^{i_1} and a^{i_m} are not bisimilar.

2. CASE $t = t' \between t''$ FOR SOME TERMS t', t''. Since t has no $\mathbf{0}$ factors, we have that neither t' nor t'' is bisimilar to $\mathbf{0}$. As σ is a substantial substitution, it follows that $\sigma(t') \not\leftrightarrow \mathbf{0}$ and $\sigma(t'') \not\leftrightarrow \mathbf{0}$.

   Observe now that $\bar{a}.a^{i_1} + \cdots + \bar{a}.a^{i_m} \xrightarrow{\bar{a}} a^{i_m}$. Thus, as

   $$\sigma(t) = \sigma(t') \between \sigma(t'') \leftrightarrow \bar{a}.a^{i_1} + \cdots + \bar{a}.a^{i_m} \ ,$$

   there is a term p such that

   $$\sigma(t') \xrightarrow{\bar{a}} p \text{ and } p \mid \sigma(t'') \leftrightarrow a^{i_m} \ .$$

As $\sigma(t'') \not\leftrightarrow \mathbf{0}$, this implies that $\sigma(t'') \stackrel{a}{\rightarrow} q$, for some q. This leads to a contradiction, because the term $\sigma(t) = \sigma(t') \between \sigma(t'')$ affords an initial τ-transition, viz.

$$\sigma(t) = \sigma(t') \between \sigma(t'') \stackrel{\tau}{\rightarrow} p \mid q \ ,$$

whereas $\bar{a}.a^{i_1} + \cdots + \bar{a}.a^{i_m}$ does not.

We may therefore conclude that t must be a variable, which was to be shown. □

The following decomposition property will find application in the proof of our main technical result, viz. Proposition 5.1 to follow.

Lemma 4.3 Let $n \geq 1$. Assume that $p \between q \leftrightarrow a\mathbf{0} \between p_n$, where q is a closed term that is not bisimilar to $\mathbf{0}$. Then $p \leftrightarrow a\mathbf{0}$ and $q \leftrightarrow p_n$.

Proof: Since $p \between q \leftrightarrow a\mathbf{0} \between p_n$ and $a\mathbf{0} \between p_n \stackrel{a}{\rightarrow} \mathbf{0} \mid p_n \leftrightarrow p_n$, there is a p' such that $p \stackrel{a}{\rightarrow} p'$ and $p' \mid q \leftrightarrow p_n$. It follows that $q \leftrightarrow p_n$ and $p' \leftrightarrow \mathbf{0}$, because p_n is prime (Proposition 4.1) and $q \not\leftrightarrow \mathbf{0}$. We are therefore left to prove that p is bisimilar to $a\mathbf{0}$. To this end, note, first of all, that, as $\leftrightarrow$ is a congruence over the language CCS_H, we have that

$$p \between p_n \leftrightarrow a\mathbf{0} \between p_n \ .$$

Assume now that $p \stackrel{\mu}{\rightarrow} p''$ for some action μ and closed term p''. In light of the above equivalence, one of the following two cases may arise:

1. $\mu = a$ and $p'' \mid p_n \leftrightarrow p_n$ or
2. $\mu = \tau$ and $p'' \mid p_n \leftrightarrow a^i$, for some $i \in \{0, \ldots, n\}$.

In the former case, p'' must have depth 0 and is thus bisimilar to $\mathbf{0}$. The latter case is impossible, because the depth of $p'' \mid p_n$ is at least $n + 1$.

We may therefore conclude that every transition of p is of the form $p \stackrel{a}{\rightarrow} p''$, for some $p'' \leftrightarrow \mathbf{0}$. Since we have already seen that p affords an a-labelled transition leading to $\mathbf{0}$, modulo bisimulation equivalence, it follows that $p \leftrightarrow a\mathbf{0}$, which was to be shown. □

Lemma 4.4 Let $t \approx u$ be an equation over the language CCS_H^- that is sound with respect to bisimulation equivalence, where t and u are terms that have neither $\mathbf{0}$ summands nor factors. Assume that some variable x occurs as a summand in t. Then x also occurs as a summand in u.

Proof: Recall that, for some finite index sets I, J, we can write

$$t = \sum_{i \in I} t_i \quad \text{and} \tag{4}$$

$$u = \sum_{j \in J} u_j \ , \tag{5}$$

where none of the t_i ($i \in I$) and u_j ($j \in J$) is $\mathbf{0}$ or a sum. Assume that variable x occurs as a summand in t—i.e., that there is an $i \in I$ with $t_i = x$. We shall argue that x also occurs as a summand in u—i.e., that there is a $j \in J$ with $u_j = x$.

Consider the substitution $\sigma_{\mathbf{0}}$ mapping each variable to $\mathbf{0}$. Pick an integer m larger than the depth of $\sigma_{\mathbf{0}}(t)$ and of $\sigma_{\mathbf{0}}(u)$. Let σ be the substitution mapping x to the term a^{m+1} and agreeing with $\sigma_{\mathbf{0}}$ on all the other variables.

As $t \approx u$ is sound with respect to bisimulation equivalence, we have that

$$\sigma(t) \leftrightarrow \sigma(u) \ .$$

Moreover, the term $\sigma(t)$ affords the transition $\sigma(t) \stackrel{a}{\rightarrow} a^m$, for $t_i = x$ and $\sigma(x) = a^{m+1} \stackrel{a}{\rightarrow} a^m$. Hence, for some closed term p,

$$\sigma(u) = \sum_{j \in J} \sigma(u_j) \stackrel{a}{\rightarrow} p \leftrightarrow a^m \ .$$

This means that there is a $j \in J$ such that $\sigma(u_j) \stackrel{a}{\rightarrow} p$. We claim that this u_j can only be the variable x. To see that this claim holds, observe, first of all, that $x \in var(u_j)$. In fact, if x did not occur in u_j, then we would reach a contradiction thus:

$$m = depth(p) < depth(\sigma(u_j)) = depth(\sigma_{\mathbf{0}}(u_j)) \leq depth(\sigma_{\mathbf{0}}(u)) < m \ .$$

Using this observation and Lemma 4.1(2), it is not hard to show that, for each of the other possible forms u_j may have, $\sigma(u_j)$ does not afford an a-labelled transition leading to a term of depth m. We may therefore conclude that $u_j = x$, which was to be shown. □

5 Proof of Proposition 3.2

We now proceed to present a detailed proof of Proposition 3.2. The following result, stating that the property mentioned in the statement of that proposition holds for all closed substantial instantiations of axioms in E, will be the crux in such a proof.

Proposition 5.1 Let $t \approx u$ be an equation over the language CCS_H^- that is sound with respect to bisimulation equivalence, where t and u are terms without $\mathbf{0}$ summands or factors. Let n be larger than the size of t. Assume that σ is a substantial substitution. Let $p = \sigma(t)$ and $q = \sigma(u)$. Suppose that p and q are bisimilar to $a\mathbf{0} \not| \ p_n$. If p has a summand bisimilar to $a\mathbf{0} \not| \ p_n$, then so does q.

Proof: We can assume that, for some finite non-empty index sets I, J,

$$t = \sum_{i \in I} t_i \quad \text{and} \tag{6}$$

$$u = \sum_{j \in J} u_j \ , \tag{7}$$

where none of the t_i ($i \in I$) and u_j ($j \in J$) is $\mathbf{0}$ or a sum. (That is, none of the t_i ($i \in I$) and u_j ($j \in J$) has $+$ as its head operator.) Note that, as t and u have no $\mathbf{0}$ summands or factors, then none of the t_i ($i \in I$) and u_j ($j \in J$) does either.

Since $p = \sigma(t)$ has a summand bisimilar to $a\mathbf{0} \between p_n$, there is an index $i \in I$ such that

$$\sigma(t_i) \leftrightarrow a\mathbf{0} \between p_n \ .$$

Our aim is now to show that there is an index $j \in J$ such that

$$\sigma(u_j) \leftrightarrow a\mathbf{0} \between p_n \ ,$$

proving that $q = \sigma(u)$ also has a summand bisimilar to $a\mathbf{0} \between p_n$. This we proceed to do by a case analysis on the form t_i may have.

1. CASE $t_i = x$ FOR SOME VARIABLE x. In this case, we have that

   $$\sigma(x) \leftrightarrow a\mathbf{0} \between p_n \ ,$$

   and t has x as a summand. As $t \approx u$ is sound with respect to bisimulation equivalence and neither t nor u have $\mathbf{0}$ summands or factors, it follows that u also has x as a summand (Lemma 4.4). Thus there is an index $j \in J$ such that $u_j = x$, and, modulo bisimulation, $\sigma(u)$ has $a\mathbf{0} \between p_n$ as a summand, which was to be shown.

2. CASE $t_i = \mu t'$ FOR SOME TERM t'. This case is vacuous because, since

   $$\sigma(t_i) = \mu\sigma(t') \stackrel{\mu}{\rightarrow} \sigma(t')$$

   is the only transition afforded by $\sigma(t_i)$, this term cannot be bisimilar to $a\mathbf{0} \between p_n$.

3. CASE $t_i = t' \between t''$ FOR SOME TERMS t', t''. The analysis of this case is the crux of the proof, and we present the argument in considerable detail.

   Since $t_i = t' \between t''$, we have that

   $$\sigma(t_i) = \sigma(t') \between \sigma(t'') \leftrightarrow a\mathbf{0} \between p_n \ .$$

   As σ is a substantial substitution, it follows that $\sigma(t') \not\leftrightarrow \mathbf{0}$ and $\sigma(t'') \not\leftrightarrow \mathbf{0}$ (Lemma 4.1(1)). Thus $\sigma(t') \leftrightarrow a\mathbf{0}$ and $\sigma(t'') \leftrightarrow p_n$ (Lemma 4.3). Now, t'' can be written thus:

   $$t'' = v_1 + \cdots + v_\ell \quad (\ell > 0) \ ,$$

   where none of the summands v_i is $\mathbf{0}$ or a sum. Observe that, since n is larger than the size of t, we have that $\ell < n$. Hence, since

   $$\sigma(t'') \leftrightarrow p_n = \sum_{i=0}^{n} \bar{a}a^i \ ,$$

there must be some $h \in \{1, \ldots, \ell\}$ such that

$$\sigma(v_h) \leftrightarrow \bar{a}.a^{i_1} + \cdots + \bar{a}.a^{i_m}$$

for some $m > 1$ and $0 \leq i_1 < \ldots < i_m \leq n$. By Lemma 4.2, it follows that v_h can only be a variable x and thus that

$$\sigma(x) \quad \leftrightarrow \quad \bar{a}.a^{i_1} + \cdots + \bar{a}.a^{i_m} \ . \tag{8}$$

Since t' has no $\mathbf{0}$ factors, the above equation yields that $x \notin var(t')$—or else $\sigma(t') \not\leftrightarrow a\mathbf{0}$ (Lemma 4.1(2)). Thus, since σ is substantial, modulo bisimulation equivalence,

$$t' = y_1 + \cdots + y_k[+a\mathbf{0}] \tag{9}$$

for some $k \geq 0$ and some variables $y_1, \ldots, y_k$ different from x with

$$\sigma(y_1) \leftrightarrow \cdots \sigma(y_k) \leftrightarrow a\mathbf{0} \ .$$

(The notation $[+a\mathbf{0}]$ in (9) denotes an optional $a\mathbf{0}$ summand. Moreover, if $k = 0$, then $t' = a\mathbf{0}$.) So, modulo bisimulation equivalence, t_i has the form $t' \between (x + t''')$, for some term t'''.

Our order of business will now be to use the information collected so far in this case of the proof to argue that $\sigma(u)$ has a summand bisimilar to $a\mathbf{0} \between p_n$. To this end, consider the substitution

$$\sigma' = \sigma[x \mapsto \bar{a}(a\mathbf{0} \between p_n)] \ .$$

We have that

$$\begin{array}{lcl} \sigma'(t_i) & = & \sigma'(t') \between \sigma'(t'') \\ & = & \sigma(t') \between \sigma'(t'') \quad (\text{As } x \notin var(t')) \\ & \leftrightarrow & a\mathbf{0} \between (\bar{a}(a\mathbf{0} \between p_n) + \sigma'(t''')) \ . \end{array}$$

Thus, $\sigma'(t_i) \stackrel{\tau}{\rightarrow} p' \leftrightarrow a\mathbf{0} \between p_n$ for some p'. By (6), we have that $\sigma'(t) \stackrel{\tau}{\rightarrow} p'$ also holds. Since $t \approx u$ is sound with respect to $\leftrightarrow$, it follows that $\sigma'(t) \leftrightarrow \sigma'(u)$. Hence, by (7), there are a $j \in J$ and a q' such that

$$\sigma'(u_j) \stackrel{\tau}{\rightarrow} q' \leftrightarrow a\mathbf{0} \between p_n \ . \tag{10}$$

Recall that, by one of the assumptions of the proposition, $\sigma(u) \leftrightarrow a\mathbf{0} \between p_n$, and thus $\sigma(u)$ has depth $n+2$. On the other hand, by (10), $depth(\sigma'(u_j)) \geq n+3$. Since σ and σ' differ only in the closed term they map variable x to, it follows that

$$x \in var(u_j) \ . \tag{11}$$

We now proceed to show that $\sigma(u_j) \leftrightarrow a\mathbf{0} \between p_n$ by a further case analysis on the form a term u_j satisfying (10) and (11) may have.

(a) CASE $u_j = x$. This case is vacuous because $\sigma'(x) = \bar{a}(a\mathbf{0} \between p_n) \stackrel{\tau}{\not\to}$, and thus this possible form for u_j does not meet (10).

(b) CASE $u_j = \mu u'$ FOR SOME TERM u'. In light of (10), we have that $\mu = \tau$ and $q' = \sigma'(u') \underline{\leftrightarrow} (a\mathbf{0} \between p_n)$. Using (11) and the fact that u' has no $\mathbf{0}$ factors, we have that $depth(\sigma'(u')) \geq n + 3$ (Lemma 4.1(2)). Since $a\mathbf{0} \between p_n$ has depth $n+2$, this contradicts the fact that $\sigma'(u') \underline{\leftrightarrow} a\mathbf{0} \between p_n$.

(c) CASE $u_j = u' \between u''$ FOR SOME TERMS u', u''. This is the lengthiest sub-case of case 3 of the proof, and its analysis will occupy us for the next couple of pages.

Our assumption that u has no $\mathbf{0}$ factors yields that neither u' nor u'' is bisimilar to $\mathbf{0}$. Moreover, by (11), either $x \in var(u')$ or $x \in var(u'')$. Since $\sigma'(u_j) = \sigma'(u') \between \sigma'(u'')$ affords transition (10), we have that $q' = q_1 \mid q_2$ for some q_1, q_2. Since $a\mathbf{0} \between p_n$ is prime (Proposition 4.1(2)), it follows that either $q_1 \underline{\leftrightarrow} \mathbf{0}$ or $q_2 \underline{\leftrightarrow} \mathbf{0}$. We now continue our proof by examining the two possible origins for transition (10). These are

i. $\sigma'(u') \stackrel{\tau}{\to} q_1$ and $q_2 = \sigma'(u'')$ and

ii. $\sigma'(u') \stackrel{\alpha}{\to} q_1$ and $\sigma'(u'') \stackrel{\bar{\alpha}}{\to} q_2$, with $\alpha \in \{a, \bar{a}\}$.

We examine these two cases in turn.

i. Assume that $\sigma'(u') \stackrel{\tau}{\to} q_1$ and $q_2 = \sigma'(u'')$. We now proceed to argue that this case produces a contradiction. To this end, note first of all that, as σ' is substantial and u'' is not bisimilar to $\mathbf{0}$, it must be the case that $q_1 \underline{\leftrightarrow} \mathbf{0}$ and $q_2 = \sigma'(u'') \underline{\leftrightarrow} a\mathbf{0} \between p_n$. In light of the definition of σ', it follows that x occurs in u', but not in u'' (Lemma 4.1(2)). Therefore, since σ and σ' only differ at the variable x,

$$\sigma(u'') = \sigma'(u'') \underline{\leftrightarrow} a\mathbf{0} \between p_n \ .$$

Since $\underline{\leftrightarrow}$ is a congruence, we derive that

$$\sigma(u_j) = \sigma(u') \between \sigma(u'') \underline{\leftrightarrow} \sigma(u') \between (a\mathbf{0} \between p_n) \ . \qquad (12)$$

Since σ is substantial, x occurs in u', and u' has no $\mathbf{0}$ factors, we may infer that

$$\begin{array}{rcl} n+2 & = & depth(a\mathbf{0} \between p_n) \\ & = & depth(\sigma(u)) \quad (\text{As } \sigma(u) \underline{\leftrightarrow} a\mathbf{0} \between p_n) \\ & \geq & depth(\sigma(u_j)) \quad (\text{By (7)}) \\ & = & depth(\sigma(u')) + n + 2 \quad (\text{By (12)}) \\ & > & n+2 \quad (\text{As } depth(\sigma(u')) > 0 \text{ by Lemma 4.1(2)}) \ , \end{array}$$

which is the desired contradiction.

ii. Assume now that $\sigma'(u') \stackrel{\alpha}{\rightarrow} q_1$ and $\sigma'(u'') \stackrel{\bar{\alpha}}{\rightarrow} q_2$, with $\alpha \in \{a, \bar{a}\}$. Recall that exactly one of q_1, q_2 is bisimilar to $\mathbf{0}$. We proceed with the proof by considering these two possible cases in turn.

CASE $q_1 \leftrightarrow \mathbf{0}$. Our order of business will be to argue that, in this case, $\sigma(u_j) \leftrightarrow a\mathbf{0} \between p_n$, and thus that $q = \sigma(u)$ has a summand bisimilar to $a\mathbf{0} \between p_n$.
To this end, observe, first of all, that $q_2 \leftrightarrow a\mathbf{0} \between p_n$ by (10). It follows that $x \in var(u'')$, for otherwise we could derive a contradiction thus:

$$\begin{array}{rcl} depth(a\mathbf{0} \between p_n) & = & depth(\sigma(u)) \quad (\text{As } \sigma(u) \leftrightarrow a\mathbf{0} \between p_n) \\ & \geq & depth(\sigma(u_j)) \quad (\text{By (7)}) \\ & > & depth(\sigma(u'')) \quad (\text{As } depth(\sigma(u')) > 0) \\ & = & depth(\sigma'(u'')) \quad (\text{As } x \notin var(u'')) \\ & > & depth(a\mathbf{0} \between p_n) \\ & & \quad (\text{As } \sigma'(u'') \stackrel{\bar{\alpha}}{\rightarrow} q_2 \leftrightarrow a\mathbf{0} \between p_n) \ . \end{array}$$

Moreover, we claim that $x \notin var(u')$. Indeed, if x also occurred in u', then, since u' has no $\mathbf{0}$ factors, the term $\sigma(x)$ would contribute to the behaviour of $\sigma(u_j)$. Therefore, by (8), the term $\sigma(u_j)$ would afford a sequence of actions containing two occurrences of $\bar{a}$, contradicting our assumption that $\sigma(u) \leftrightarrow a\mathbf{0} \between p_n$. It follows that $\alpha = a$, because

$$\sigma'(u') = \sigma(u') \stackrel{\bar{a}}{\nrightarrow} \ ,$$

since $\sigma(u) \leftrightarrow a\mathbf{0} \between p_n$.
Observe now that, as $\sigma'(u'') \stackrel{\bar{a}}{\rightarrow} q_2 \leftrightarrow a\mathbf{0} \between p_n$, it must be the case that u'' has a summand x. To see that this does hold, we examine the other possible forms a summand w of u'' responsible for the transition

$$\sigma'(u'') \stackrel{\bar{a}}{\rightarrow} q_2 \leftrightarrow a\mathbf{0} \between p_n$$

may have, and argue that each of them leads to a contradiction.

A. CASE $w = \bar{a}w'$, FOR SOME TERM w'. In this case, $q_2 = \sigma'(w')$. However, the depth of such a q_2 is either smaller than $n+2$ (if $x \notin var(w')$), or larger than $n+2$ (if $x \in var(w')$). This contradicts the fact that q_2 is bisimilar to $a\mathbf{0} \between p_n$, because the latter term has depth $n+2$.

B. CASE $w = w_1 \between w_2$, FOR SOME TERMS w_1 AND w_2. Since

$$\sigma'(w) = \sigma'(w_1) \between \sigma'(w_2) \stackrel{\bar{a}}{\rightarrow} q_2 \ ,$$

there is a closed term q_3 such that $\sigma'(w_2) \stackrel{\bar{a}}{\rightarrow} q_3$ and $q_2 = q_3 \mid \sigma'(w_2) \leftrightarrow a\mathbf{0} \between p_n$. As the term $a\mathbf{0} \between p_n$ is prime, σ'

is substantial, and w_2 is not bisimilar to $\mathbf{0}$, we may infer that $q_3 \underline{\leftrightarrow} \mathbf{0}$ and

$$\sigma'(w_2) \underline{\leftrightarrow} a\mathbf{0} \between p_n \ .$$

It follows that $x \notin var(w_2)$—or else the depth of $\sigma'(w_2)$ would be at least $n+3$—, and therefore that

$$\sigma'(w_2) = \sigma(w_2) \underline{\leftrightarrow} a\mathbf{0} \between p_n \ .$$

However, this contradicts our assumption that $\sigma(u) \underline{\leftrightarrow} a\mathbf{0} \between p_n$.

Summing up, we have argued that u'' has a summand x. Therefore, by (8),

$$\sigma(u'') \underline{\leftrightarrow} \bar{a}.a^{i_1} + \cdots + \bar{a}.a^{i_m} + r'' \ ,$$

for some closed term r''. We have already noted that

$$\sigma(u') = \sigma'(u') \xrightarrow{a} q_1 \underline{\leftrightarrow} \mathbf{0} \ .$$

Therefore, we have that

$$\sigma(u') \underline{\leftrightarrow} a\mathbf{0} + r' \ ,$$

for some closed term r'. Using the congruence properties of bisimulation equivalence, we may infer that

$$\sigma(u_j) = \sigma(u') \between \sigma(u'') \underline{\leftrightarrow} (a\mathbf{0}+r') \between (\bar{a}.a^{i_1}+\cdots+\bar{a}.a^{i_m}+r'') \ .$$

In light of this equivalence, we have that

$$\sigma(u_j) \xrightarrow{a} r \underline{\leftrightarrow} \bar{a}.a^{i_1} + \cdots + \bar{a}.a^{i_m} + r'' \underline{\leftrightarrow} \sigma(u'') \ ,$$

for some closed term r. By (7),

$$q = \sigma(u) \xrightarrow{a} r \ .$$

Since $q = \sigma(u) \underline{\leftrightarrow} a\mathbf{0} \between p_n$ by our assumption, it must be the case that $r \underline{\leftrightarrow} \sigma(u'') \underline{\leftrightarrow} p_n$. So, again using the congruence properties of $\underline{\leftrightarrow}$, we have that

$$\sigma(u_j) = \sigma(u') \between \sigma(u'') \underline{\leftrightarrow} (a\mathbf{0} + r') \between p_n \ .$$

As $\sigma(u) \underline{\leftrightarrow} a\mathbf{0} \between p_n$, using Lemma 4.3 it is now a simple matter to infer that

$$\sigma(u') \underline{\leftrightarrow} a\mathbf{0} \ .$$

Hence $\sigma(u_j) \underline{\leftrightarrow} a\mathbf{0} \between p_n$. Note that $\sigma(u_j)$ is a summand of $q = \sigma(u)$. Therefore q has a summand bisimilar to $a\mathbf{0} \between p_n$, which was to be shown.

CASE $q_2 \leftrightarrow \mathbf{0}$. We now proceed to argue that this case produces a contradiction. To this end, observe, first of all, that $q_1 \leftrightarrow a\mathbf{0} \not| \ p_n$. Reasoning as in the analysis of the previous case, we may infer that $\alpha = a$, x occurs in u', but x does not occur in u''. Moreover, since $\sigma'(u') \stackrel{a}{\rightarrow} q_1 \leftrightarrow a\mathbf{0} \not| \ p_n$, it must be the case that $u' \stackrel{a}{\rightarrow} u'''$ for some u''' such that

$$\sigma'(u''') = q_1 \leftrightarrow a\mathbf{0} \not| \ p_n \ .$$

(For, otherwise, using Lemma 2.1(3), we would have that

$$\sigma'(u') \stackrel{a}{\rightarrow} q_1$$

because $u' \stackrel{y}{\rightarrow} c$, $\sigma(y) \stackrel{a}{\rightarrow} q_1'$ and $q_1 = \sigma'[y_d \mapsto q_1'](c)$, for some variable y, configuration c and closed term q_1'. Note that $y \neq x$. In fact, if $y = x$, then we would have that $a = \bar{a}$ by the definition of σ', contradicting the distinctness of these two complementary actions. Observe now that, again in light of the definition of σ', the variable x cannot occur in c, or else the depth of $q_1 = \sigma'[y_d \mapsto q_1'](c)$ would be at least $n + 3$, contradicting our assumption that $q_1 \leftrightarrow a\mathbf{0} \not| \ p_n$. Hence, since the variable y is different from x, it is not hard to see that $\sigma(u') \stackrel{a}{\rightarrow} q_1$ also holds, and thus that $depth(q_1) < depth(\sigma(u)) = n + 2$, contradicting our assumption that $q_1 \leftrightarrow a\mathbf{0} \not| \ p_n$.) Since u contains no $\mathbf{0}$ factors, in light of the definition of σ', this u''' cannot contain occurrences of the variable x. (For, otherwise, Lemma 4.1(2) would yield that

$$depth(\sigma'(u''')) = depth(q_1) \geq n + 3 \ ,$$

contradicting our assumption that $q_1 \leftrightarrow a\mathbf{0} \not| \ p_n$.) So

$$\sigma(u''') = q_1 \leftrightarrow a\mathbf{0} \not| \ p_n$$

also holds. Thus

$$\begin{array}{rcl} n+2 & = & depth(a\mathbf{0} \not| \ p_n) \\ & = & depth(\sigma(u)) \quad \text{(As } \sigma(u) \leftrightarrow a\mathbf{0} \not| \ p_n\text{)} \\ & \geq & depth(\sigma(u_j)) \quad \text{(By (7))} \\ & = & depth(\sigma(u') \not| \ \sigma(u'')) \\ & > & depth(\sigma(u''')) + depth(\sigma(u'')) \\ & & \text{(As } \sigma(u') \stackrel{a}{\rightarrow} \sigma(u''')\text{)} \\ & > & n+2 \\ & & \text{(As } depth(\sigma(u'')) > 0 \text{ and } depth(\sigma(u''')) = n+2\text{)} \end{array}$$

which is the desired contradiction.

This completes the proof for the case $u_j = u' \between u''$ for some terms u', u''.

The proof is now complete. □

We are now ready to prove Proposition 3.2, thus completing the proof of Theorem 3.2 and of our main result (Theorem 3.1).

Proof of Proposition 3.2: Assume that E is a finite axiom system over the language CCS_H^- that is sound with respect to bisimulation equivalence, and that the following hold, for some closed terms p and q and positive integer n larger than the size of each term in the equations in E:

1. $E \vdash p \approx q$,
2. $p \underline{\leftrightarrow} q \underline{\leftrightarrow} a\mathbf{0} \between p_n$,
3. p and q contain no occurrences of $\mathbf{0}$ as a summand or factor, and
4. p has a summand bisimilar to $a\mathbf{0} \between p_n$.

We prove that q also has a summand bisimilar to $a\mathbf{0} \between p_n$ by induction on the depth of the closed proof of the equation $p \approx q$ from E. Recall that, without loss of generality, we may assume that the closed terms involved in the proof of the equation $p \approx q$ have no $\mathbf{0}$ summands or factors (by Proposition 2.1, as E may be assumed to be saturated), that applications of symmetry happen first in equational proofs (that is, E is closed with respect to symmetry), and that only closed substantial substitutions are used (E is closed with respect to $\mathbf{0}$-substititions).

We proceed by a case analysis on the last rule used in the proof of $p \approx q$ from E. The case of reflexivity is trivial, and that of transitivity follows immediately by using the inductive hypothesis twice. Below we only consider the other possibilities.

- CASE $E \vdash p \approx q$, BECAUSE $\sigma(t) = p$ AND $\sigma(u) = q$ FOR SOME EQUATION $(t \approx u) \in E$ AND CLOSED SUBSTANTIAL SUBSTITUTION σ. Observe, first of all, that since $\sigma(t) = p$ and $\sigma(u) = q$ have no $\mathbf{0}$ summands or factors, then neither do t and u. Therefore, as n is larger than the size of each term mentioned in equations in E, the claim follows by Proposition 5.1.

- CASE $E \vdash p \approx q$, BECAUSE $p = \mu p'$ AND $q = \mu q'$ FOR SOME p', q' SUCH THAT $E \vdash p' \approx q'$. This case is vacuous because $p = \mu p' \not\underline{\leftrightarrow} a\mathbf{0} \between p_n$, and thus p does not have a summand bisimilar to $a\mathbf{0} \between p_n$.

- CASE $E \vdash p \approx q$, BECAUSE $p = p' + p''$ AND $q = q' + q''$ FOR SOME p', q', p'', q'' SUCH THAT $E \vdash p' \approx q'$ AND $E \vdash p'' \approx q''$. Since p has a summand bisimilar to $a\mathbf{0} \between p_n$, we have that so does either p' or p''. Assume, without loss of generality, that p' has a summand bisimilar to $a\mathbf{0} \between p_n$.

Since p is bisimilar to $a\mathbf{0} \between p_n$, so is p'. Using the soundness of E modulo bisimulation, it follows that $q' \leftrightarrow a\mathbf{0} \between p_n$. The inductive hypothesis now yields that q' has a summand bisimilar to $a\mathbf{0} \between p_n$. Hence, q has a summand bisimilar to $a\mathbf{0} \between p_n$, which was to be shown.

- CASE $E \vdash p \approx q$, BECAUSE $p = p' \between p''$ AND $q = q' \between q''$ FOR SOME p', q', p'', q'' SUCH THAT $E \vdash p' \approx q'$ AND $E \vdash p'' \approx q''$. Since the proof involves no uses of $\mathbf{0}$ as a summand or a factor, we have that $p', p'' \not\leftrightarrow \mathbf{0}$ and $q', q'' \not\leftrightarrow \mathbf{0}$. It follows that q is a summand of itself. By our assumptions,

  $$a\mathbf{0} \between p_n \leftrightarrow q \ .$$

  Therefore we have that q has a summand bisimilar to $a\mathbf{0} \between p_n$, and we are done.

This completes the proof. □

6 Concluding Remarks

In their seminal paper [8], Bergstra and Klop showed that the parallel composition operator can be finitely axiomatized modulo bisimulation equivalence with the use of two auxiliary operators, viz. the by now classic left merge and communication merge. Independently, and at roughly the same time, Hennessy proposed the auxiliary operator $\between$, and used it in [21] to give equational axiomatizations of Milner's observation congruence [26] and timed congruence. The axiomatization of observation congruence offered by Hennessy using the $\between$ operator relies, however, on a variation on the classic expansion law [26], and is therefore infinite. This led Bergstra and Klop to conjecture in [8, page 118] that Hennessy's $\between$ operator does not have a finite equational axiomatization. The main result in this paper confirms this conjecture of Bergstra and Klop's, and answers one of the questions in [2, Problem 8], by showing that, in the presence of two distinct complementary actions, it is impossible to provide a finite axiomatization of the recursion free fragment of CCS modulo bisimulation equivalence using $\between$. This result further reinforces the status of the left merge and the communication merge operators as auxiliary operators in the finite equational characterization of parallel composition in bisimulation semantics.

A natural question to ask at this point is whether there is a single *binary* operator that preserves bisimulation equivalence, and whose addition to the recursion free fragment of CCS allows for the finite equational axiomatization of parallel composition—see [2, Problem 8]. (As was recently pointed out to us by Jos Baeten and Rob van Glabbeek, it is certainly possible to obtain a finite axiomatization of bisimulation equivalence by adding one *ternary* operator to the signature of CCS.) We conjecture that no such operator exists, and that the use of *two* auxiliary operators is therefore necessary to achieve a finite axiomatization of parallel composition in bisimulation semantics. This result would offer the definitive justification

we seek for the canonical standing of the operators proposed by Bergstra and Klop. Work on the confirmation of this conjecture is under way, and we hope to report on it elsewhere in the near future.

Acknowledgments The work reported in this paper was carried out while Luca Aceto was on leave at Reykjavík University, and Anna Ingólfsdóttir was at deCODE Genetics. They thank these institutions for their hospitality and excellent working conditions. The authors thank Zoltán Ésik for pointing out useful references on the study of the equational theory of shuffle in formal language theory.

References

[1] L. ACETO, *On "Axiomatising finite concurrent processes"*, SIAM J. Comput., 23 (1994), pp. 852–863.

[2] ——, *Some of my favourite results in classic process algebra*, BRICS Report NS-03-2, BRICS, Department of Computer Science, Aalborg University, September 2003.

[3] L. ACETO, B. BLOOM, AND F. VAANDRAGER, *Turning SOS rules into equations*, Information and Computation, 111 (1994), pp. 1–52.

[4] L. ACETO, W. FOKKINK, AND C. VERHOEF, *Structural operational semantics*, in Handbook of Process Algebra, North-Holland, 2001, pp. 197–292.

[5] D. AUSTRY AND G. BOUDOL, *Algèbre de processus et synchronisations*, Theoretical Comput. Sci., 30 (1984), pp. 91–131.

[6] J. BAETEN AND E. DE VINK, *Axiomatizing GSOS with termination*, in Proceedings of STACS 2002, 19th Annual Symposium on Theoretical Aspects of Computer Science, Antibes-Juan les Pins, France, March 14–16, 2002, H. Alt and A. Ferreira, eds., vol. 2285 of Lecture Notes in Computer Science, Springer-Verlag, 2002, pp. 583–595.

[7] J. BAETEN AND P. WEIJLAND, *Process Algebra*, Cambridge Tracts in Theoretical Computer Science 18, Cambridge University Press, 1990.

[8] J. BERGSTRA AND J. W. KLOP, *Process algebra for synchronous communication*, Information and Control, 60 (1984), pp. 109–137.

[9] S. L. BLOOM AND Z. ÉSIK, *Nonfinite axiomatizability of shuffle inequalities*, in Proceedings of TAPSOFT'95: Theory and Practice of Software Development, 6th International Joint Conference CAAP/FASE, Aarhus, Denmark, May 22–26, 1995, P. D. Mosses, M. Nielsen, and M. I. Schwartzbach, eds., vol. 915 of Lecture Notes in Computer Science, Springer-Verlag, 1995, pp. 318–333.

[10] ——, *Free shuffle algebras in language varieties*, Theoret. Comput. Sci., 163 (1996), pp. 55–98.

[11] ——, *Axiomatizing shuffle and concatenation in languages*, Inform. and Comput., 139 (1997), pp. 62–91.

[12] ——, *Varieties generated by languages with poset operations*, Math. Structures Comput. Sci., 7 (1997), pp. 701–713.

[13] ——, *Shuffle binoids*, RAIRO Inform. Théor. Appl., 32 (1998), pp. 175–198.

[14] Z. ÉSIK, *Axiomatizing the subsumption and subword preorders on finite and infinite partial words*, Theoret. Comput. Sci., 273 (2002), pp. 225–248. WORDS (Rouen, 1999).

[15] Z. ÉSIK AND M. BERTOL, *Nonfinite axiomatizability of the equational theory of shuffle*, Acta Inform., 35 (1998), pp. 505–539.

[16] Z. ÉSIK AND S. OKAWA, *Series and parallel operations on pomsets*, in Proceedings of Foundations of Software Technology and Theoretical Computer Science (Chennai, 1999), vol. 1738 of Lecture Notes in Comput. Sci., Springer-Verlag, Berlin, 1999, pp. 316–328.

[17] W. FOKKINK AND B. LUTTIK, *An omega-complete equational specification of interleaving*, in Proceedings 27th Colloquium on Automata, Languages and Programming—ICALP'00, Geneva, U. Montanari, J. Rolinn, and E. Welzl, eds., vol. 1853 of Lecture Notes in Computer Science, Springer-Verlag, July 2000, pp. 729–743.

[18] J. L. GISCHER, *The equational theory of pomsets*, Theoretical Comput. Sci., 61 (1988), pp. 199–224.

[19] J. F. GROOTE, *A new strategy for proving ω–completeness with applications in process algebra*, in Proceedings CONCUR 90, Amsterdam, J. Baeten and J. Klop, eds., vol. 458 of Lecture Notes in Computer Science, Springer-Verlag, 1990, pp. 314–331.

[20] M. HENNESSY, *Algebraic Theory of Processes*, MIT Press, Cambridge, Massachusetts, 1988.

[21] ——, *Axiomatising finite concurrent processes*, SIAM J. Comput., 17 (1988), pp. 997–1017.

[22] M. HENNESSY AND R. MILNER, *Algebraic laws for nondeterminism and concurrency*, J. Assoc. Comput. Mach., 32 (1985), pp. 137–161.

[23] C. HOARE, *Communicating Sequential Processes*, Prentice-Hall International, Englewood Cliffs, 1985.

[24] R. KELLER, *Formal verification of parallel programs*, Comm. ACM, 19 (1976), pp. 371–384.

[25] R. MILNER, *Flowgraphs and flow algebras*, J. Assoc. Comput. Mach., 26 (1979), pp. 794–818.

[26] ——, *Communication and Concurrency*, Prentice-Hall International, Englewood Cliffs, 1989.

[27] R. MILNER AND F. MOLLER, *Unique decomposition of processes (note)*, Theoretical Comput. Sci., 107 (1993), pp. 357–363.

[28] F. MOLLER, *Axioms for Concurrency*, PhD thesis, Department of Computer Science, University of Edinburgh, July 1989. Report CST-59-89. Also published as ECS-LFCS-89-84.

[29] ——, *The importance of the left merge operator in process algebras*, in Proceedings 17^{th} ICALP, Warwick, M. Paterson, ed., vol. 443 of Lecture Notes in Computer Science, Springer-Verlag, July 1990, pp. 752–764.

[30] ——, *The nonexistence of finite axiomatisations for CCS congruences*, in Proceedings 5^{th} Annual Symposium on Logic in Computer Science, Philadelphia, USA, IEEE Computer Society Press, 1990, pp. 142–153.

[31] D. PARK, *Concurrency and automata on infinite sequences*, in 5^{th} GI Conference, Karlsruhe, Germany, P. Deussen, ed., vol. 104 of Lecture Notes in Computer Science, Springer-Verlag, 1981, pp. 167–183.

[32] G. PLOTKIN, *A structural approach to operational semantics*, Report DAIMI FN-19, Computer Science Department, Aarhus University, 1981.

[33] V. PRATT, *Modeling concurrency with partial orders*, International Journal of Parallel Programming, 15 (1986), pp. 33–71.

[34] R. DE SIMONE, *Higher-level synchronising devices in* MEIJE–*SCCS*, Theoretical Comput. Sci., 37 (1985), pp. 245–267.

[35] S. T. TSCHANTZ, *Languages under concatenation and shuffling*, Mathematical Structures in Computer Science, 4 (1994), pp. 505–511.