BRICS

Basic Research in Computer Science

BRICS RS-04-1 Aceto et al.: Split-2 Bisimilarity has a Finite Axiomatization over CCS with Hennessy's Me

Split-2 Bisimilarity has a Finite Axiomatization over CCS with Hennessy's Merge

Luca Aceto
Willem Jan Fokkink
Anna Ingólfsdóttir
Bas Luttik

BRICS Report Series RS-04-1

ISSN 0909-0878 January 2004

See back inner page for a list of recent BRICS Report Series publications. Copies may be obtained by contacting:

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK–8000 Aarhus C
Denmark

Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk

BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:

`http://www.brics.dk`
`ftp://ftp.brics.dk`
This document in subdirectory `RS/04/1/`

Split-2 Bisimilarity has a Finite Axiomatization over CCS with Hennessy's Merge

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 note shows that split-2 bisimulation equivalence (also known as timed equivalence) affords a finite equational axiomatization over the process algebra obtained by adding an auxiliary operation proposed by Hennessy in 1981 to the recursion free fragment of Milner's Calculus of Communicating Systems. Thus the addition of a single binary operation, viz. Hennessy's merge, is sufficient for the finite equational axiomatization of parallel composition modulo this non-interleaving equivalence. This result is in sharp

*Partially supported by the Statens Naturvidenskabelige Forskningsråd (Danish Natural Science Research Council), project "The Equational Logic of Parallel Processes", nr. 21-03-0342.

contrast to a theorem previously obtained by the same authors to the effect that the same language is not finitely based modulo bisimulation equivalence.

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, split-2 bisimulation, non-interleaving equivalences, Hennessy's merge, left merge, communication merge, parallel composition, equational logic, complete axiomatizations, finitely based algebras.

1 Introduction

This note offers a contribution to the fascinating study of equational characterizations of the parallel composition operation modulo (variations on) the classic notion of bisimulation equivalence [14, 19]. In particular, we provide a finite equational axiomatization of *split-2 bisimulation equivalence*—a notion of bisimulation equivalence based on the assumption that actions have observable beginnings and endings [9, 10, 11]—over the recursion, relabelling and restriction free fragment of Milner's CCS [14] enriched with an auxiliary operator proposed by Hennessy in a 1981 preprint entitled *"On the relationship between time and interleaving"* and its published version [11]. To put this contribution, and its significance, in its research context, we find it appropriate to recall briefly some of the key results in the history of the study of equational axiomatizations of parallel composition in process algebra.

Research on equational axiomatizations of behavioural equivalences over process algebras incorporating a notion of parallel composition can be traced at least as far back as the seminal paper [12], where Hennessy and Milner offered, amongst a wealth of other classic results, a complete equational axiomatization of bisimulation equivalence over the recursion free fragment of CCS. (See the paper [5] for a more detailed historical account highlighting, e.g., Hans Bekić's early contributions to this field of research.) The axiomatization given by Hennessy and Milner in that paper dealt with parallel composition using the so-called *expansion law*—an axiom schema with a countably infinite number of instances that is essentially an equational formulation of the Plotkin-style rules describing the operational semantics of parallel composition. 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 clarified the key role played by the expansion law in the axiomatization of parallel composition over CCS by showing in [16, 17, 18] that strong bisimulation equivalence is *not* finitely based over CCS and PA without the left merge operator. Thus auxiliary operators like the ones used by Bergstra and Klop are indeed necessary to obtain a finite axiomatization of parallel composition. Moreover, Moller proved in [16, 17] that his negative result holds true for each "reasonable congruence" that is included in standard bisimulation equivalence. In particular, this theorem of Moller's applies to split-2 bisimulation equivalence since that equivalence is "reasonable" in Moller's technical sense.

In his paper [11], Hennessy proposed an axiomatization of observation congruence [12] (also known as rooted weak bisimulation equivalence) and timed congruence (essentially rooted weak split-2 bisimulation equivalence) over a CCS-like recursion free process language. Those axiomatizations used an auxiliary operator, denoted $|\!/$ by Hennessy, that is essentially a combination of Bergstra and Klop's left and communication merge operators. 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 [12]. Confirming a conjecture by Bergstra and Klop in [8, page 118], and answering problem 8 in [2], we showed in [3] that the language obtained by adding Hennessy's merge to CCS does *not* afford a finite equational axiomatization modulo bisimulation equivalence. This is due to the fact that, in strong bisimulation semantics, no finite collection of equations can express the interplay between interleaving and communication that underlies the semantics of Hennessy's merge. Technically, this is captured in our proof of the main result in [3] by showing that no finite collection of axioms that are valid in bisimulation semantics can prove all of the equations in the following family:

$$a\mathbf{0} \,|\!/\, \sum_{i=0}^{n} \bar{a}a^i \quad \approx \quad a\sum_{i=0}^{n} \bar{a}a^i + \sum_{i=0}^{n} \tau a^i \quad (n \geq 0) \ .$$

In split-2 semantics, however, these equations are not sound, since they express some form of interleaving. Indeed, we prove that, in sharp contrast to the situation in standard bisimulation semantics, Hennessy's merge *can be finitely axiomatized* modulo split-2 bisimulation equivalence, and its use suffices to yield a finite axiomatization of the parallel composition operation. This shows that "reasonable congruences" finer than standard bisimulation equivalence can be finitely axiomatized over CCS using Hennessy's merge as the single auxiliary operation—compare with the non-finite axiomatizability results for these congruences offered in [16, 17].

The paper is organized as follows. We begin by presenting preliminaries on the language CCS_H—the extension of CCS with Hennessy's merge operator—and split-2 bisimulation equivalence in Sect. 2. We then offer a finite equational axiom system for split-2 bisimulation equivalence over CCS_H, and prove that it is sound and complete (Sect. 3).

This is a companion paper to [3], where the interested readers may find further motivation and more references to related literature. However, we have striven to make it readable independently of that paper. Some familiarity with [1, 11] and the basic notions on process algebras and bisimulation equivalence will be helpful, but is not necessary, in reading this study. The uninitiated reader is referred to the textbooks [6, 14] for extensive motivation and background on process algebras. Precise pointers to material in [1, 11] will be given whenever necessary.

2 The language $\mathbf{CCS}_H$

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 [11] to the recursion, restriction and relabelling free subset of Milner's CCS [14]. This language is given by the following grammar:

$$p ::= \mathbf{0} \quad | \quad \mu p \quad | \quad p + p \quad | \quad p \,|\, p \quad | \quad p \not| \; p \ ,$$

where μ ranges over a set of *actions* A. We assume that A has the form $\{\tau\} \cup \Lambda \cup \bar{\Lambda}$, where Λ is a given set of *names*, $\bar{\Lambda} = \{\bar{a} \mid a \in \Lambda\}$ is the set of *complement names*, and τ is a distinguished action. Following Milner [14], the action symbol τ will result from the synchronized occurrence of the complementary actions a and $\bar{a}$. We let a, b range over the set of *visible actions* $\Lambda \cup \bar{\Lambda}$. As usual, we postulate that $\bar{\bar{a}} = a$ for each name $a \in \Lambda$. We shall use p, q, r to range over process terms. The *size* of a term is the number of operation symbols in it. Following standard practice in the literature on CCS and related languages, trailing $\mathbf{0}$'s will often be omitted from terms.

The structural operational semantics for the language CCS_H given by Hennessy in [11, Sect. 2.1] is based upon the idea that visible actions have a beginning and an ending. Moreover, for each visible action a, these distinct events may be observed, and are denoted by $S(a)$ and $F(a)$, respectively. We define

$$E = A \cup \{S(a), F(a) \mid a \in \Lambda \cup \bar{\Lambda}\} \ .$$

In the terminology of [11], this is the set of *events*, and we shall use e to range over it. As usual, we write E^* for the collection of finite sequences of events.

Table 1: SOS Rules for S ($\mu \in A$, $a \in \Lambda \cup \bar{\Lambda}$ and $e \in E$)

$$\frac{}{ap \xrightarrow{S(a)} a_S p} \qquad \frac{}{a_S p \xrightarrow{F(a)} p} \qquad \frac{}{\mu p \xrightarrow{\mu} p}$$

$$\frac{p \xrightarrow{e} s}{p + q \xrightarrow{e} s} \qquad \frac{q \xrightarrow{e} s}{p + q \xrightarrow{e} s}$$

$$\frac{s \xrightarrow{e} s'}{s \mid t \xrightarrow{e} s' \mid t} \qquad \frac{t \xrightarrow{e} t'}{s \mid t \xrightarrow{e} s \mid t'} \qquad \frac{s \xrightarrow{a} s',\ t \xrightarrow{\bar{a}} t'}{s \mid t \xrightarrow{\tau} s' \mid t'}$$

$$\frac{p \xrightarrow{e} s}{p \not| \, q \xrightarrow{e} s \mid q} \qquad \frac{p \xrightarrow{a} p',\ q \xrightarrow{\bar{a}} q'}{p \not| \, q \xrightarrow{\tau} p' \mid q'}$$

The operational semantics for the language CCS_H is given in terms of binary next-state relations $\xrightarrow{e}$, one for each event $e \in E$. As explained in [11], the relations $\xrightarrow{e}$ are defined over the set of *states* S, an extension of CCS_H obtained by adding new prefixing operations a_S ($a \in \Lambda \cup \bar{\Lambda}$) to the signature for CCS_H. More formally, the set of states is given by the following grammar:

$$s ::= p \quad | \quad a_S p \quad | \quad s \mid s \ ,$$

where p ranges over CCS_H. Intuitively, a state of the form $a_S p$ is one in which the execution of action a has started, but has not terminated yet. We shall use s, t to range over the set of states S.

The Plotkin style rules for the language S are given in Table 1; comments on these rules may be found in [11, Sect. 2.1].

Definition 2.1 For a sequence of events $\sigma = e_1 \cdots e_k$ ($k \geq 0$), and states s, s', we write $s \xrightarrow{\sigma} s'$ iff there exists a sequence of transitions

$$s = s_0 \xrightarrow{e_1} s_1 \xrightarrow{e_2} \cdots \xrightarrow{e_k} s_k = s' \ .$$

If $s \xrightarrow{\sigma} s'$ holds for some state s', then σ is a *trace* of s.

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

In this paper, we shall consider the language CCS_H, and more generally the set of states S, modulo split-2 bisimulation equivalence [4, 9, 11]. (The weak variant of this relation is called *t-observational equivalence* by Hennessy in [11]. Later on, this relation has been called *timed equivalence* in [4]. Here we adopt the terminology introduced by van Glabbeek and Vaandrager in [9].)

Definition 2.2 *Split-2 bisimulation equivalence*, denoted by $\underline{\leftrightarrow}_{2S}$, is the largest symmetric relation over S such that whenever $s \underline{\leftrightarrow}_{2S} t$ and $s \xrightarrow{e} s'$, then there is a transition $t \xrightarrow{e} t'$ with $s' \underline{\leftrightarrow}_{2S} t'$.

We shall also sometimes refer to $\underline{\leftrightarrow}_{2S}$ as *split-2 bisimilarity*. If $s \underline{\leftrightarrow}_{2S} t$, then we say that s and t are *split-2 bisimilar*.

In what follows, we shall mainly be interested in $\underline{\leftrightarrow}_{2S}$ as it applies to the language CCS_H. The interested reader is referred to [11, Sect. 2.1] for examples of (in)equivalent terms with respect to $\underline{\leftrightarrow}_{2S}$. Here, we limit ourselves to remarking that $\underline{\leftrightarrow}_{2S}$ is a non-interleaving equivalence. For example, the reader can easily check that

$$a \mid b \not\underline{\leftrightarrow}_{2S} a \mid b + ab \not\underline{\leftrightarrow}_{2S} ab + ba \ \ .$$

It is well-known that split-2 bisimulation equivalence is indeed an equivalence relation. Moreover, two split-2 bisimulation equivalent states afford the same finite non-empty set of traces, and have therefore the same depth.

The following result can be shown following standard lines—see, e.g., [4].

Fact 2.1 Split-2 bisimilarity is a congruence over the language CCS_H. Moreover, for all states s, s', t, t', if $s \underline{\leftrightarrow}_{2S} s'$ and $t \underline{\leftrightarrow}_{2S} t'$, then $s \mid t \underline{\leftrightarrow}_{2S} s' \mid t'$.

A standard question a process algebraist would ask at this point, and the one that we shall address in the remainder of this paper, is whether split-2 bisimulation equivalence affords a finite equational axiomatization over the language CCS_H. As we showed in [3], standard bisimulation equivalence is not finitely based over the language CCS_H. In particular, we argued *ibidem* that no finite collection of equations over CCS_H that is sound with respect to bisimulation equivalence can prove all of the equations

$$e_n: \quad a\mathbf{0} \not\mid p_n \quad \approx \quad ap_n + \sum_{i=0}^{n} \tau a^i \quad (n \geq 0) \ \ , \tag{1}$$

where a^0 denotes $\mathbf{0}$, a^{m+1} denotes $a(a^m)$, and the terms p_n are defined thus:

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

Note, however, that none of the equations e_n holds with respect to $\underline{\leftrightarrow}_{2S}$. In fact, for each $n \geq 0$, the transition

$$ap_n + \sum_{i=0}^{n} \tau a^i \xrightarrow{S(a)} a_S p_n$$

Table 2: The Axiom System $\mathcal{E}$ for CCS$_H$ Modulo $\underline{\leftrightarrow}_{2S}$

A1	$x + y$	$\approx$	$y + x$
A2	$(x + y) + z$	$\approx$	$x + (y + z)$
A3	$x + x$	$\approx$	x
A4	$x + \mathbf{0}$	$\approx$	x
HM1	$(x + y) \mathbin{\vert\!/} z$	$\approx$	$x \mathbin{\vert\!/} z + y \mathbin{\vert\!/} z$
HM2	$(x \mathbin{\vert\!/} y) \mathbin{\vert\!/} z$	$\approx$	$x \mathbin{\vert\!/} (y \mid z)$
HM3	$x \mathbin{\vert\!/} \mathbf{0}$	$\approx$	x
HM4	$\mathbf{0} \mathbin{\vert\!/} x$	$\approx$	$\mathbf{0}$
HM5	$(\tau x) \mathbin{\vert\!/} y$	$\approx$	$\tau(x \mid y)$
HM6	$ax \mathbin{\vert\!/} ((\bar{a}y \mathbin{\vert\!/} w) + z)$	$\approx$	$ax \mathbin{\vert\!/} ((\bar{a}y \mathbin{\vert\!/} w) + z) + \tau(x \mid y \mid w)$
M	$x \mid y$	$\approx$	$(x \mathbin{\vert\!/} y) + (y \mathbin{\vert\!/} x)$

cannot be matched, modulo $\underline{\leftrightarrow}_{2S}$, by the term $a\mathbf{0} \mathbin{|\!/} p_n$. Indeed, the only state reachable from $a\mathbf{0} \mathbin{|\!/} p_n$ via an $S(a)$-labelled transition is $a_S\mathbf{0} \mid p_n$. This state is not split-2 bisimilar to $a_S p_n$ because it can perform the transition

$$a_S\mathbf{0} \mid p_n \xrightarrow{S(\bar{a})} a_S\mathbf{0} \mid \bar{a}_S\mathbf{0} \ ,$$

whereas the only initial event $a_S p_n$ can embark in is $F(a)$. Thus the family of equations on which our proof of the main result from [3] was based is unsound with respect to split-2 bisimilarity. Indeed, as we shall show in what follows, split-2 bisimilarity affords a finite equational axiomatization over the language CCS$_H$, if the set of actions A is finite. Hence it is possible to finitely axiomatize split-2 bisimilarity over CCS using a single auxiliary binary operation, viz. Hennessy's merge.

3 An Axiomatization of Split-2 Bisimilarity over CCS$_H$

Let $\mathcal{E}$ denote the collection of equations in Table 2. In those equations the symbols x, y, w, z are variables. Equation HM6 is an axiom schema describing one equation per visible action a. Note that $\mathcal{E}$ is finite, if so is A.

We write $\mathcal{E} \vdash p \approx q$, where p, q are terms in the language CCS$_H$ that may possibly contain occurrences of variables, if the equation $p \approx q$ can be proven from those in $\mathcal{E}$ using the standard rules of equational logic. For example, using axioms A1, A2, A3, M, HM1 and HM2, it is possible to derive the equations:

$$x \mid \mathbf{0} \approx x \tag{2}$$

$$\mathbf{0} \mid x \approx x \tag{3}$$

$$x \mid y \approx y \mid x \quad \text{and} \tag{4}$$

$$(x \mid y) \mid z \approx x \mid (y \mid z) \tag{5}$$

that state that, modulo $\underline{\leftrightarrow}_{2S}$, the language CCS_H is a commutative monoid with respect to parallel composition with **0** as unit element. (In light of the provability of (5), we have taken the liberty of omitting parentheses in the second summand of the term at the right-hand side of equation HM6 in Table 2.) Moreover, it is easy to see that:

Fact 3.1 For each CCS_H term p, if $p \underline{\leftrightarrow}_{2S} \mathbf{0}$, then the equation $p \approx \mathbf{0}$ is provable using A4, HM4 and M.

All of the equations in the axiom system $\mathcal{E}$ may be found in the axiomatization of t-observational congruence proposed by Hennessy in [11]. However, the abstraction from τ-labelled transitions underlying t-observational congruence renders axiom HM2 above unsound. (See the discussion in [1, Page 854 and Sect. 3].) Indeed, to the best of our knowledge, it is yet unknown whether (t-)observational congruence affords a finite equational axiomatization over CCS, with or without Hennessy's merge.

Our aim, in the remainder of this note, will be to show that, in the presence of a finite collection of actions A, split-2 bisimilarity (that is strong t-bisimulation) *is* finitely axiomatizable over the language CCS_H. This is the import of the following:

Theorem 3.1 For all CCS_H terms p, q not containing occurrences of variables, $p \underline{\leftrightarrow}_{2S} q$ if, and only if, $\mathcal{E} \vdash p \approx q$.

We now proceed to prove the above theorem by establishing separately that the axiom system $\mathcal{E}$ is sound and complete.

Proposition 3.1 [Soundness] For all CCS_H terms p, q, if $\mathcal{E} \vdash p \approx q$, then $p \underline{\leftrightarrow}_{2S} q$.

Proof: Since $\underline{\leftrightarrow}_{2S}$ is a congruence over the language CCS_H (Fact 2.1), it suffices only to check that each of the equations in $\mathcal{E}$ is sound. The verification is tedious, but not hard, and we omit the details. □

Remark 3.1 For later use in the proof of Proposition 3.3, we note that equations (2)–(5) also hold modulo $\underline{\leftrightarrow}_{2S}$ when the variables x, y, z are allowed to range over the set of states S.

The proof of the completeness of the equations in $\mathcal{E}$ with respect to $\underline{\leftrightarrow}_{2S}$ follows the general outline of that of [11, Theorem 2.1.2]. As usual, we rely upon the existence of normal forms for CCS_H terms. In the remainder of this paper, process terms are considered modulo associativity and commutativity of +. In other words, we do not distinguish $p+q$ and $q+p$, nor $(p+q)+r$ and $p+(q+r)$. This is justified because, as previously observed, split-2 bisimulation equivalence satisfies axioms A1, A2 in Table 2. In what follows, the symbol $=$ will denote equality modulo axioms A1, A2. We use a *summation* $\sum_{i\in\{1,\ldots,k\}} p_i$ to denote $p_1 + \cdots + p_k$, where the empty sum represents **0**.

Definition 3.1 The set NF of *normal forms* is the least subset of CCS_H such that

$$\sum_{i\in I}(a_i p_i \not| \; p'_i) + \sum_{j\in J} \tau q_j \in \mathrm{NF} \ ,$$

where I, J are finite index sets, if the following conditions hold:

1. the terms p_i, p'_i $(i \in I)$ and q_j $(j \in J)$ are contained in NF and
2. if $a_i p_i \not| \; p'_i \xrightarrow{\tau} q$ for some q, then $q = q_j$ for some $j \in J$.

Proposition 3.2 [Normalization] For each CCS_H term p, there is a term $\hat{p} \in \mathrm{NF}$ such that $\mathcal{E} \vdash p \approx \hat{p}$.

Proof: Define the relation $\prec$ on CCS_H terms thus:

$p \prec q$ if, and only if,

- $depth(p) < depth(q)$ or
- $depth(p) = depth(q)$ and the size of p is smaller than that of q.

Note that $\prec$ is a well-founded relation, so we may use $\prec$-induction. The remainder of the proof consists of a case analysis on the syntactic form of p.

We only provide the details for the case $p = q \not| \; r$. (The cases $p = \mathbf{0}$, $p = q+r$ and $p = \mu q$ are trivial—the last owing to the fact that $\mu q \approx \mu q \not| \; \mathbf{0}$ is an instance of axiom HM3—, and the case $p = q \mid r$ follows from the case that is treated in detail using axiom M.)

Assume therefore that $p = q \not| \; r$. Then $depth(q) \leq depth(p)$ and the size of q is smaller than that of p, so $q \prec p$. Hence, by the induction hypothesis there exists $\hat{q} \in \mathrm{NF}$ such that $\mathcal{E} \vdash q \approx \hat{q}$, say

$$\hat{q} = \sum_{i\in I}(a_i q_i \not| \; q'_i) + \sum_{j\in J} \tau q''_j \ .$$

By axioms HM1, HM2, HM4 and HM5 it follows that

$$p \approx \sum_{i \in I} a_i q_i \not{|}\, (q_i' \mid r) + \sum_{j \in J} \tau (q_j'' \mid r) \ .$$

Since $depth(q_i'), depth(q_j'') < depth(\hat{q}) = depth(q)$ for each $i \in I$ and $j \in J$, it follows that

$$depth(q_i' \mid r), depth(q_j'' \mid r) < depth(\hat{q} \not{|}\, r) = depth(q \not{|}\, r) = depth(p) \ ,$$

and hence $q_i' \mid r \prec p$ and $q_j'' \mid r \prec p$. By the induction hypothesis there are normal forms $\widehat{q_i' \mid r}$, $\widehat{q_j'' \mid r}$ such that $\mathcal{E} \vdash q_i' \mid r \approx \widehat{q_i' \mid r}$, $q_j'' \mid r \approx \widehat{q_j'' \mid r}$. So $\mathcal{E}$ proves the equation

$$p \approx \sum_{i \in I} a_i q_i \not{|}\, (\widehat{q_i' \mid r}) + \sum_{j \in J} \tau (\widehat{q_j'' \mid r}) \ . \tag{6}$$

Finally, using equation HM6, it is now a simple matter to add summands to the right-hand side of the above equation in order to meet requirement 2 in Definition 3.1. In fact, let $i \in I$ and

$$\widehat{q_i' \mid r} = \sum_{h \in H} (a_h r_h \not{|}\, r_h') + \sum_{k \in K} \tau r_k'' \ .$$

Using A4, we have that

$$\widehat{q_i' \mid r} \approx \sum_{h \in H, a_h = \bar{a}_i} (a_h r_h \not{|}\, r_h') + \sum_{h \in H, a_h \neq \bar{a}_i} (a_h r_h \not{|}\, r_h') + \sum_{k \in K} \tau r_k''$$

is provable from $\mathcal{E}$. Then, using HM6 and the induction hypothesis repeatedly, we can prove the equation

$$a_i q_i \not{|}\, (\widehat{q_i' \mid r}) \quad \approx \quad a_i q_i \not{|}\, (\widehat{q_i' \mid r}) + \sum_{h \in H, a_h = \bar{a}_i} \tau (\widehat{q_i \mid r_h \mid r_h'}) \ .$$

Using this equation as a rewrite rule from left to right in (6) for each $i \in I$ produces a term meeting requirement 2 in Definition 3.1 that is the desired normal form for $p = q \not{|}\, r$. □

The key to the proof of the promised completeness theorem is an important cancellation result that has its roots in one proven by Hennessy for his t-observational equivalence in [11].

Theorem 3.2 Let p, p', q, q' be CCS_H terms, and let a be a visible action. Assume that $a_S p \mid p' \underline{\leftrightarrow}_{2S}\, a_S q \mid q'$. Then $p \underline{\leftrightarrow}_{2S}\, q$ and $p' \underline{\leftrightarrow}_{2S}\, q'$.

For the moment, we postpone the proof of this result, and use it to establish the following statement, to the effect that the axiom system $\mathcal{E}$ is complete with respect to $\underline{\leftrightarrow}_{2S}$ over CCS$_H$.

Theorem 3.3 [Completeness] Let p, q be CCS$_H$ terms such that $p \underline{\leftrightarrow}_{2S}\, q$. Then $\mathcal{E} \vdash p \approx q$.

Proof: By induction on the depth of p and q. (Recall that, since $p \underline{\leftrightarrow}_{2S}\, q$, the terms p and q have the same depth.) In light of Propositions 3.1 and 3.2, we may assume without loss of generality that p and q are contained in NF. Let

$$\begin{aligned} p &= \sum_{i\in I}(a_i p_i \not| \; p'_i) + \sum_{j\in J}\tau p''_j \quad \text{and} \\ q &= \sum_{h\in H}(b_h q_h \not| \; q'_h) + \sum_{k\in K}\tau q''_k \ . \end{aligned}$$

We prove that $\mathcal{E} \vdash p \approx p + q$, from which the statement of the theorem follows by symmetry and transitivity. To this end, we argue that each summand of q can be absorbed by p using the equations in $\mathcal{E}$, i.e., that

1. $\mathcal{E} \vdash p \approx p + \tau q''_k$ for each $k \in K$, and
2. $\mathcal{E} \vdash p \approx p + (b_h q_h \not| \; q'_h)$ for each $h \in H$.

We prove these two statements in turn.

- PROOF OF STATEMENT 1. Let $k \in K$. Then $q \xrightarrow{\tau} q''_k$. Since $p \underline{\leftrightarrow}_{2S}\, q$, there is a term r such that $p \xrightarrow{\tau} r$ and $r \underline{\leftrightarrow}_{2S}\, q''_k$. Since $p \in$ NF, condition 2 in Definition 3.1 yields that $r = p''_j$ for some $j \in J$. The induction hypothesis together with closure with respect to τ-prefixing now yields that

  $$\mathcal{E} \vdash \tau p''_j \approx \tau q''_k \ .$$

  Therefore, using A1–A3, we have that

  $$\mathcal{E} \vdash p \approx p + \tau p''_j \approx p + \tau q''_k \ ,$$

  which was to be shown.

- PROOF OF STATEMENT 2. Let $h \in H$. Then $q \xrightarrow{S(b_h)} b_{hS} q_h \mid q'_h$. Since $p \underline{\leftrightarrow}_{2S}\, q$, there is a state s such that $p \xrightarrow{S(b_h)} s$ and $s \underline{\leftrightarrow}_{2S}\, b_{hS} q_h \mid q'_h$. Because of the form of p, it follows that $s = a_{iS} p_i \mid p'_i$ for some $i \in I$ such that $a_i = b_h$. By Theorem 3.2, we have that

  $$p_i \underline{\leftrightarrow}_{2S}\, q_h \text{ and } p'_i \underline{\leftrightarrow}_{2S}\, q'_h \ .$$

Since the depth of all of these terms is smaller than that of p, we may apply the induction hypothesis twice to obtain that

$$\mathcal{E} \vdash p_i \approx q_h \text{ and } \mathcal{E} \vdash p'_i \approx q'_h \ .$$

Therefore, using A1–A3 and $a_i = b_h$, we have that

$$\mathcal{E} \vdash p \approx p + (a_i p_i \not| \ p'_i) \approx p + (b_h q_h \not| \ q'_h) \ ,$$

which was to be shown.

The proof of the theorem is now complete. □

To finish the proof of the completeness theorem, and therefore of Theorem 3.1, we are left to show Theorem 3.2. Our proof of that result relies on a unique decomposition property with respect to parallel composition for states modulo $\underline{\leftrightarrow}_{2S}$. In order to formulate this decomposition property, we shall make use of some notions from [15, 16]. These we now proceed to introduce for the sake of completeness and readability.

Definition 3.2 A state s is *irreducible* if $s \underline{\leftrightarrow}_{2S} s_1 \mid s_2$ implies $s_1 \underline{\leftrightarrow}_{2S} \mathbf{0}$ or $s_2 \underline{\leftrightarrow}_{2S} \mathbf{0}$, for all states s_1, s_2.

We say that s is *prime* if it is irreducible and is not split-2 bisimilar to $\mathbf{0}$.

For example, each state s of depth 1 is prime because every state of the form $s_1 \mid s_2$, where s_1 and s_2 are not split-2 bisimilar to $\mathbf{0}$, has depth at least 2, and thus cannot be split-2 bisimilar to s.

Fact 3.2 The state $a_S p$ is prime, for each CCS$_H$ term p and action a.

Proof: Since $a_S p$ is not split-2 bisimilar to $\mathbf{0}$, it suffices only to show that it is irreducible. To this end, assume, towards a contradiction, that $a_S p \underline{\leftrightarrow}_{2S} s_1 \mid s_2$ for some states s_1, s_2 that are not split-2 bisimilar to $\mathbf{0}$. Then, since $a_S p \underline{\leftrightarrow}_{2S} s_1 \mid s_2$, we have that $s_1 \xrightarrow{F(a)} s'_1$ and $s_2 \xrightarrow{F(a)} s'_2$, for some s'_1, s'_2. But then it follows that

$$s_1 \mid s_2 \xrightarrow{F(a)} s'_1 \mid s_2 \xrightarrow{F(a)} s'_1 \mid s'_2 \ ,$$

whereas the term $a_S p$ cannot perform two subsequent $F(a)$-transitions. We may therefore conclude that such s_1 and s_2 cannot exist, and hence that the term $a_S p$ is irreducible, which was to be shown. □

The following result is the counterpart for the language CCS$_H$ of the unique decomposition theorems presented for various languages in, e.g., [4, 13, 15, 16].

Proposition 3.3 Each state is split-2 bisimilar to a parallel composition of primes, uniquely determined up to split-2 bisimilarity and the order of the primes. (We adopt the convention that $\mathbf{0}$ denotes the empty parallel composition.)

Proof: We shall obtain this result as a consequence of a general unique decomposition result, obtained by the fourth author in [13].

Let $[S]$ denote the set of states modulo split-2 bisimilarity, and, for a state $s \in S$, denote by $[s]$ the equivalence class in $[S]$ that contains s. By Fact 2.1 we can define on $[S]$ a binary operation $|$ by

$$[s] \mid [t] = [s \mid t] \ .$$

By Remark 3.1, the set $[S]$ with the binary operation $|$ and the distinguished element $[\mathbf{0}]$ is a commutative monoid.

Next, we define on $[S]$ a partial order $\preccurlyeq$ by

$$[s'] \preccurlyeq [s] \text{ iff there exist } s'' \in S \text{ and } \sigma \in E^* \text{ such that } s \xrightarrow{\sigma} s'' \underline{\leftrightarrow}_{2S}\, s'.$$

Note that $\preccurlyeq$ is indeed a partial order (to establish antisymmetry use that transitions decrease depth, and that split-2 bisimilar states have the same depth).

For each state s, there are a sequence of events σ and a state s' such that

$$s \xrightarrow{\sigma} s' \underline{\leftrightarrow}_{2S}\, \mathbf{0} \ .$$

So $[\mathbf{0}]$ is the least element of $[S]$ with respect to $\preccurlyeq$. Furthermore, if $[s'] \preccurlyeq [s]$, then $s \xrightarrow{\sigma} s'' \underline{\leftrightarrow}_{2S}\, s'$, for some $\sigma \in E^*$ and state s''. So, using the SOS rules for S and Fact 2.1, it follows that $s \mid t \xrightarrow{\sigma} s'' \mid t \underline{\leftrightarrow}_{2S}\, s' \mid t$, and hence

$$[s'] \mid [t] = [s' \mid t] \preccurlyeq [s \mid t] = [s] \mid [t] \ .$$

Thereby, we have now established that $[S]$ with $|$, $[\mathbf{0}]$ and $\preccurlyeq$ is a positively ordered commutative monoid in the sense of [13].

From the SOS rules for S it easily follows that this positively ordered commutative monoid is *precompositional* (see [13]), i.e., that

$$\text{if } [s] \preccurlyeq [s_1] \mid [s_2], \text{ then there are } [s_1'] \preccurlyeq [s_1],\, [s_2'] \preccurlyeq [s_2] \text{ s.t. } [s] = [s_1'] \mid [s_2'].$$

Consider the mapping $|\_| : [S] \to \mathbf{N}$ into the positively ordered monoid of natural numbers with addition, 0 and the standard less-than-or-equal relation, defined by

$$[s] \mapsto depth(s) \ .$$

It is straightforward to verify that $|\_|$ is a *stratification* (see [13]), i.e., that

(i) $|[s] \mid [t]| = |[s]| + |[t]|$; and

(ii) if $[s] \prec [t]$, then $|[s]| < |[t]|$.

We conclude that $[S]$ with $|$, $[\mathbf{0}]$ and $\preccurlyeq$ is a stratified and precompositional positively ordered commutative monoid, and hence, by Theorem 13 in [13], it has unique decomposition. This completes the proof of the proposition. $\Box$

Using the above unique decomposition result, we are now in a position to complete the proof of Theorem 3.2.

Proof of Theorem 3.2: Assume that $a_S p \mid p' \underline{\leftrightarrow}_{2S} a_S q \mid q'$. Using Proposition 3.3, we have that p' and q' can be expressed uniquely as parallel compositions of primes. Say that

$$\begin{array}{lll} p' & \underline{\leftrightarrow}_{2S} & p_1 \mid p_2 \mid \cdots \mid p_m \quad \text{and} \\ q' & \underline{\leftrightarrow}_{2S} & q_1 \mid q_2 \mid \cdots \mid q_n \end{array}$$

for some $m, n \geq 0$ and primes p_i ($1 \leq i \leq m$) and q_j ($1 \leq j \leq n$) in the language CCS$_H$. Since $a_S p$ and $a_S q$ are prime (Fact 3.2) and $\underline{\leftrightarrow}_{2S}$ is a congruence (Fact 2.1), the unique prime decompositions of $a_S p \mid p'$ and $a_S q \mid q'$ given by Proposition 3.3 are

$$\begin{array}{lll} a_S p \mid p & \underline{\leftrightarrow}_{2S} & a_S p \mid p_1 \mid p_2 \mid \cdots \mid p_m \quad \text{and} \\ a_S q \mid q' & \underline{\leftrightarrow}_{2S} & a_S q \mid q_1 \mid q_2 \mid \cdots \mid q_n \ , \end{array}$$

respectively. In light of our assumption that $a_S p \mid p' \underline{\leftrightarrow}_{2S} a_S q \mid q'$, these two prime decompositions coincide by Proposition 3.3. Hence, as $a_S p \not\underline{\leftrightarrow}_{2S} q_j$ for each $1 \leq j \leq n$, we have that

1. $a_S p \underline{\leftrightarrow}_{2S} a_S q$,
2. $m = n$ and, without loss of generality,
3. $p_i \underline{\leftrightarrow}_{2S} q_i$ for each $1 \leq i \leq m$.

It is now immediate to see that $p \underline{\leftrightarrow}_{2S} q$ and $p' \underline{\leftrightarrow}_{2S} q'$, which was to be shown. $\Box$

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.

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*, Note NS-03-2, BRICS, Department of Computer Science, Aalborg University, September 2003.

[3] L. ACETO, W. FOKKINK, A. INGÓLFSDÓTTIR, AND B. LUTTIK, *CCS with Hennessy's merge has no finite equational axiomatization*, Research report RS-03-34, BRICS, November 2003.

[4] L. ACETO AND M. HENNESSY, *Towards action refinement in process algebras*, Information and Computation, 103 (1993), pp. 204–269.

[5] J. BAETEN, *A brief history of process algebra*, Report CSR 04-02, Eindhoven University of Technology, 2004.

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

[7] J. BERGSTRA AND J. W. KLOP, *The algebra of recursively defined processes and the algebra of regular processes*, in Proceedings 11^{th} ICALP, Antwerpen, J. Paredaens, ed., vol. 172 of Lecture Notes in Computer Science, Springer-Verlag, 1984, pp. 82–95.

[8] ——, *Process algebra for synchronous communication*, Information and Control, 60 (1984), pp. 109–137.

[9] R. VAN GLABBEEK AND F. VAANDRAGER, *Petri net models for algebraic theories of concurrency*, in Proceedings PARLE conference, Eindhoven, Vol. II (Parallel Languages), J. de Bakker, A. Nijman, and P. Treleaven, eds., vol. 259 of Lecture Notes in Computer Science, Springer-Verlag, 1987, pp. 224–242.

[10] R. GORRIERI AND C. LANEVE, *Split and ST bisimulation semantics*, Information and Computation, 118 (1995), pp. 272–288.

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

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

[13] B. LUTTIK, *A unique decomposition theorem for ordered monoids with applications in process theory*, in Proceedings of Mathematical Foundations of Computer Science 2003, 28th International Symposium, MFCS 2003, Bratislava, Slovakia, August 25–29, 2003, B. Rovan and P. Vojtás, eds., vol. 2747 of Lecture Notes in Computer Science, Springer-Verlag, 2003, pp. 562–571.

[14] R. MILNER, *Communication and Concurrency*, Prentice-Hall International, Englewood Cliffs, 1989.

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

[16] 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.

[17] ——, *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.

[18] ——, *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.

[19] 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.

Recent BRICS Report Series Publications

RS-04-1 **Luca Aceto, Willem Jan Fokkink, Anna Ingólfsdóttir, and Bas Luttik.** ***Split-2 Bisimilarity has a Finite Axiomatization over CCS with Hennessy's Merge*****. January 2004. 16 pp.**

RS-03-53 **Kyung-Goo Doh and Peter D. Mosses.** ***Composing Programming Languages by Combining Action-Semantics Modules*****. December 2003. 39 pp. Appears in** ***Science of Computer Programming*****, 47(1):2–36, 2003.**

RS-03-52 **Peter D. Mosses.** ***Pragmatics of Modular SOS*****. December 2003. 22 pp. Invited paper, published in Kirchner and Ringeissen, editors,** ***Algebraic Methodology and Software Technology: 9th International Conference*****, AMAST '02 Proceedings, LNCS 2422, 2002, pages 21–40.**

RS-03-51 **Ulrich Kohlenbach and Branimir Lambov.** ***Bounds on Iterations of Asymptotically Quasi-Nonexpansive Mappings*****. December 2003. 24 pp.**

RS-03-50 **Branimir Lambov.** ***A Two-Layer Approach to the Computability and Complexity of Real Numbers*****. December 2003. 16 pp.**

RS-03-49 **Marius Mikucionis, Kim G. Larsen, and Brian Nielsen.** ***Online On-the-Fly Testing of Real-time Systems*****. December 2003. 14 pp.**

RS-03-48 **Kim G. Larsen, Ulrik Larsen, Brian Nielsen, Arne Skou, and Andrzej Wasowski.** ***Danfoss EKC Trial Project Deliverables*****. December 2003. 53 pp.**

RS-03-47 **Hans Hüttel and Jiří Srba.** ***Recursive Ping-Pong Protocols*****. December 2003. 21 pp. To appear in the proceedings of 2004 IFIP WG 1.7, ACM SIGPLAN and GI FoMSESS Workshop on Issues in the Theory of Security (WITS'04).**

RS-03-46 **Philipp Gerhardy.** ***The Role of Quantifier Alternations in Cut Elimination*****. December 2003. 10 pp. Extends paper appearing in Baaz and Makowsky, editors,** ***European Association for Computer Science Logic: 17th International Workshop*****, CSL '03 Proceedings, LNCS 2803, 2003, pages 212-225.**