Basic Research in Computer Science

2-Nested Simulation is not Finitely Equationally Axiomatizable

Luca Aceto
Willem Jan Fokkink
Anna Ingólfsdóttir

BRICS Report Series **RS-00-20**

ISSN 0909-0878 **August 2000**

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/00/20/`

2-Nested Simulation is not Finitely Equationally Axiomatizable

Luca Aceto[1], Wan Fokkink[2], and Anna Ingólfsdóttir[1]

[1] **BRICS** (**B**asic **R**esearch in **C**omputer **S**cience), Centre of the Danish National Research Foundation, Department of Computer Science, Aalborg University, Fr. Bajersvej 7E, 9220 Aalborg Ø, Denmark, luca@cs.auc.dk, annai@cs.auc.dk
[2] CWI, Department of Software Engineering, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands, wan@cwi.nl

Abstract. 2-nested simulation was introduced by Groote and Vaandrager [10] as the coarsest equivalence included in completed trace equivalence for which the tyft/tyxt format is a congruence format. In the linear time-branching time spectrum of van Glabbeek [8], 2-nested simulation is one of the few equivalences for which no finite equational axiomatization is presented. In this paper we prove that such an axiomatization does not exist for 2-nested simulation.
Keywords: Concurrency, process algebra, basic CCS, 2-nested simulation, equational logic, complete axiomatizations.

1 Introduction

Labelled transition systems (LTSs) [11] are a fundamental model of concurrent computation, which is widely used in light of its flexibility and applicability. In particular, they are the prime model underlying Plotkin's Structural Operational Semantics [19] and, following Milner's pioneering work on CCS [15], are by now the standard semantic model for various process description languages.

LTSs model processes by explicitly describing their states and their transitions from state to state, together with the actions that produced them. Since this view of process behaviours is very detailed, several notions of behavioural equivalence and preorder have been proposed for LTSs. The aim of such behavioural semantics is to identify those (states of) LTSs that afford the same "observations", in some appropriate technical sense. The lack of consensus on what constitutes an appropriate notion of observable behaviour for reactive systems has led to a large number of proposals for behavioural equivalences for concurrent processes. (Cf. the encyclopaedic study [8], where van Glabbeek presents the linear time-branching time spectrum—a lattice that contains all the known behavioural equivalences and preorders over LTSs, ordered by inclusion.)

One of the criteria that has been put forward for studying the mathematical tractability of the behavioural equivalences in the linear time-branching time spectrum is that they afford elegant, finite equational axiomatizations over fragments of process algebraic languages. Equationally based proof systems play an important role in both the practice and the theory of process algebras. From the

point of view of practice, these proof systems can be used to perform system verifications in a purely syntactic way, and form the basis of axiomatic verification tools like, e.g., PAM [12]. From the theoretical point of view, complete axiomatizations of behavioural equivalences capture the essence of different notions of semantics for processes in terms of a basic collection of identities, and this often allows one to compare semantics which may have been defined in very different styles and frameworks. A review of existing complete equational axiomatizations for many of the behavioral semantics in van Glabbeek's spectrum is offered in [8]. The equational axiomatizations offered *ibidem* are over Milner's Basic CCS (abbreviated to BCCS in what follows), a fragment of CCS suitable for describing finite synchronization trees, and characterize the differences between behavioural semantics in terms of a few revealing axioms.

The main omission in this menagerie of equational axiomatizations for the behavioural semantics in van Glabbeek's spectrum is an axiomatization for 2-nested simulation semantics. 2-nested simulation was introduced by Groote and Vaandrager [10] as the coarsest equivalence included in completed trace equivalence for which the tyft/tyxt format is a congruence format. It thus characterizes the distinctions amongst processes that can be made by observing their termination behaviour in program contexts that can be built using a wide array of operators. (The interested reader is referred to *op. cit.* for motivation and the basic theory of 2-nested simulation.) 2-nested simulation can be decided over finite LTSs in time that is quadratic in their number of transitions [22], and can be characterized by a single parameterised modal logic formula [16]. However, as previously mentioned, no equational axiomatization for it has ever been proposed, even for the language BCCS.

In this paper, we offer a possible mathematical justification for the lack of an equational axiomatization for the 2-nested simulation equivalence and preorder even for the language of finite synchronization trees [14]. More precisely, we show that neither of these two behavioural relations has a finite equational axiomatization over the language of BCCS. These results hold in a very strong form. Indeed, we prove that no finite collection of inequations that are sound with respect to the 2-nested simulation preorder can prove all of the inequalities of the form

$$a^{2m} \lesssim a^{2m} + a^m \qquad (m \geq 0) \ ,$$

which are sound with respect to the 2-nested simulation preorder. Similarly, we establish a result to the effect that no finite collection of equations that are sound with respect to 2-nested simulation equivalence can be used to derive all of the sound equalities of the form

$$a(a^{2m} + a^m) \approx a(a^{2m} + a^m) + a^{2m+1} \qquad (m \geq 0) \ .$$

The import of these two results is that not only the equational theory of 2-nested simulation is not finitely equationally axiomatizable, but neither is the collection of (in)equivalences that hold between BCCS terms over one action and without

occurrences of variables. This state of affairs should be contrasted with the elegant equational axiomatizations over BCCS for most of the other behavioural equivalences in the linear time–branching time spectrum that are reviewed by van Glabbeek in [8]. Only in the case of additional, more complex operators, such as iteration, are these equivalences known to lack a finite equational axiomatization; see, e.g., [3, 6, 7, 20, 21]. Of special relevance for concurrency theory are Moller's results to the effect that the process algebras ACP and CCS (without the auxiliary left merge operator from [5]) do not have a finite equational axiomatization modulo bisimulation equivalence [17, 18]. Aceto, Ésik and Ingólfsdóttir [2] proved that there is no finite equational axiomatization that is ω-complete for the max-plus algebra of the natural numbers, a result whose process algebraic implications are discussed in [1].

The paper is organized as follows. We begin by presenting preliminaries on the language BCCS and (in)equational logic (Sect. 2). We then proceed to define 2-nested simulation, and study some of its basic properties that play a major role in the proof of our main results (Sect. 3). The definition of 2-nested simulation suggests a natural conditional inference system for it. This is presented in Sect. 4. Our main results on the non-existence of finite (in)equational axiomatizations for 2-nested equivalence and preorder are the topic of Sects. 5 and 6. The paper concludes with a result to the effect that the 3-nested simulation preorder has no finite inequational axiomatization, and some open problems (Sect. 7).

2 Preliminaries

The language BCCS The process algebra BCCS [14] is a basic formalism to express finite process behaviour. Its syntax consists of (process) terms that are constructed from a countably infinite set of variables (with typical elements x, y, z), a constant $\mathbf{0}$, a binary operator $+$ called *alternative composition*, and unary *prefixing* operators a, where a ranges over some nonempty set Act of *atomic actions*. We shall use the meta-variables t, u, v to range over process terms, and write $var(t)$ for the collection of variables occurring in the term t.

A process term is *closed* if it does not contain any variables. Closed terms will be typically denoted by p, q, r. Intuitively, closed terms represent completely specified finite process behaviours, where $\mathbf{0}$ does not exhibit any behaviour, $p+q$ combines the behaviours of p and q, and ap can execute action a to transform into p. This intuition for the operators of BCCS is captured, in the style of Plotkin [19], by the transition rules in Table 1. These transition rules give rise to transitions between process terms. The operational semantics for BCCS is thus given by the labelled transition system [11] whose states are terms, and whose Act-labelled transitions are those that are provable using the rules in Table 1.

A (closed) substitution is a mapping from process variables to (closed) BCCS 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 $\sigma(t)$.

Table 1. Transition rules for BCCS

$$\frac{x \xrightarrow{a} x'}{x + y \xrightarrow{a} x'} \qquad \frac{y \xrightarrow{a} y'}{x + y \xrightarrow{a} y'} \qquad ax \xrightarrow{a} x$$

Table 2. Axioms for BCCS

A1	$x + y \approx y + x$
A2	$(x + y) + z \approx x + (y + z)$
A3	$x + x \approx x$
A4	$x + \mathbf{0} \approx x$

In the remainder of this paper, process terms are considered modulo associativity and commutativity of $+$, and modulo absorption of $\mathbf{0}$ summands. In other words, we do not distinguish $t+u$ and $u+t$, nor $(t+u)+v$ and $t+(u+v)$, nor $t+\mathbf{0}$ and t. This is justified because all of the behavioural equivalences we consider satisfy axioms A1, A2 and A4 in Table 2. In what follows, the symbol $=$ will denote syntactic equality modulo axioms A1, A2 and A4. 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 A1, A2 and A4, every BCCS term t has the form $\sum_{i\in I} x_i + \sum_{j\in J} a_j t_j$, for some finite index sets I, J, terms t_j $(j \in J)$ and variables x_i $(i \in I)$.

Equational logic An *axiom system* is a collection of (in)equations over the language BCCS. We say that an equation $t \approx u$ (resp. an inequation $t \lesssim u$) is derivable from an axiom system E if it can be proven from the axioms in E using the standard rules of equational (resp. inequational) logic. It is well-known (cf., e.g., Sect. 2 in [9]) that if an (in)equation relating two closed terms can be proven from an axiom system E, then there is a closed proof for it.

In the proofs of our main results (cf. Thms. 3 and 4), it will be convenient to use a different formulation of the notion of provability of an (in)equation from a set of axioms. This we now proceed to define for the sake of clarity.

A *context* $C[]$ is a closed BCCS term with exactly one occurrence of a hole $[]$ in it. For every context $C[]$ and closed term p, we write $C[p]$ for the closed term that results by placing p in the hole in $C[]$. It is not hard to see that an equation $p \approx q$ is provable from an equational axiom system E iff there is a sequence $p_1 \approx \cdots \approx p_k$ $(k \geq 1)$ such that

- $p = p_1$, $q = p_k$ and
- $p_i = C[\sigma(t)] \approx C[\sigma(u)] = p_{i+1}$ for some closed substitution σ, context $C[]$ and pair of terms t, u with either $t \approx u$ or $u \approx t$ an axiom in E $(1 \leq i < k)$.

The obvious modification of the above observation applies to proofs of inequations from inequational axiom systems. In what follows, we shall refer to se-

quences of the form $p_1 \approx \cdots \approx p_k$ (resp. $p_1 \lesssim \cdots \lesssim p_k$) as *equational* (resp. *inequational*) *derivations.*

For later use, note that, using axioms A1, A2 and A4 in Table 2, every context can be proven equal to either one of the form $C[b([] + p)]$ or to one of the form $[] + p$, for some action b and closed BCCS term p.

3 2-nested simulation

In this paper, we shall study the (in)equational theory of 2-nested simulation semantics over BCCS. This is a behavioural semantics for processes that stems from [10], where it was characterized as the largest congruence with respect to the tyft/tyxt format of transition rules which is included in completed trace semantics.

Definition 1. *A binary relation R between closed terms is a* simulation *iff $p\ R\ q$ together with $p \xrightarrow{a} p'$ implies that there is a transition $q \xrightarrow{a} q'$ with $p'\ R\ q'$.*

For closed terms p, q, we write $p \subseteq^1 q$ iff $p\ R\ q$ with R a simulation. The kernel of $\subseteq^1$ (i.e., the equivalence $\subseteq^1 \cap (\subseteq^1)^{-1}$) is denoted by $\leftrightarrows^1$.

The relation $\subseteq^1$ is the well-known *simulation preorder* [13].

Definition 2. *For closed terms p, q, we write $p \subseteq^2 q$ iff $p\ R\ q$ with R a simulation and R^{-1} included in $\subseteq^1$. The kernel of $\subseteq^2$ (i.e., the equivalence $\subseteq^2 \cap (\subseteq^2)^{-1}$) is denoted by $\leftrightarrows^2$.*

The relations $\subseteq^2$ and $\leftrightarrows^2$ are the *2-nested simulation preorder* and the *2-nested simulation equivalence*, respectively. It is easy to see that $\subseteq^2$ is included in $\leftrightarrows^1$. In the remainder of this paper we will use, instead of Definition 2, the following more descriptive characterization of 2-nested simulation. To the best of our knowledge, this characterization is new.

Theorem 1. *Let p, q be closed BCCS terms. Then $p \subseteq^2 q$ iff*

(1) for all $p \xrightarrow{a} p'$ there is a $q \xrightarrow{a} q'$ with $p' \subseteq^2 q'$, and
(2) $q \subseteq^1 p$.

Proof. We prove the two implications separately.

($\Rightarrow$) Let $p \subseteq^2 q$. By definition, $p\ R\ q$ with R a simulation and R^{-1} included in $\subseteq^1$. So if $p \xrightarrow{a} p'$, then $q \xrightarrow{a} q'$ with $p'\ R\ q'$, which implies $p' \subseteq^2 q'$. Moreover, since R^{-1} is included in $\subseteq^1$, it follows that $q \subseteq^1 p$.

($\Leftarrow$) We define $p\ R\ q$ iff

(1) for all $p \xrightarrow{a} p'$ there is a $q \xrightarrow{a} q'$ with $p' \subseteq^2 q'$, and
(2) $q \subseteq^1 p$.

Suppose $p\ R\ q$. If $p \xrightarrow{a} p'$, then by the definition of R we have $q \xrightarrow{a} q'$ with $p' \subseteq^2 q'$. Since we have already proven the 'only if' implication, $p'\ R\ q'$. So R is a simulation. Furthermore, by (2) R^{-1} is included in $\subseteq^1$. Hence, $p \subseteq^2 q$. □

The transition rules in Table 1 are in tyft/tyxt format, that is a (pre)congruence format for $\subseteq^2$ and $\leftrightarrows^2$ [10]. Hence, we immediately have that:

Lemma 1. *The relations $\subseteq^2$ and $\leftrightarrows^2$ are preserved by the operators of BCCS.*

The relations $\subseteq^2$ and $\leftrightarrows^2$ are extended to arbitrary BCCS terms thus:

Definition 3. *Let t, u be BCCS terms. The inequation $t \lesssim u$ is* sound *with respect to $\subseteq^2$ iff $\sigma(t) \subseteq^2 \sigma(u)$ holds for every closed substitution σ. Similarly, the equation $t \approx u$ is* sound *with respect to $\leftrightarrows^2$ iff $\sigma(t) \leftrightarrows^2 \sigma(u)$ holds for every closed substitution σ.*

Examples of (in)equations that are sound with respect to $\subseteq^2$ are those in Table 2 and

$$a(x+y) \lesssim a(x+y) + ax \ .$$

3.1 Norm and depth

We now present some results on the depth and the norm of BCCS terms that are related in 2-nested simulation semantics. These will find important applications in the proofs of our main results, and shed light on the nature of the identifications made by 2-nested simulation semantics.

Definition 4. *A sequence $a_1 \cdots a_k \in \mathsf{Act}^*$ $(k \geq 0)$ is a* termination trace *of a term t iff there exists a sequence of transitions $t = t_0 \stackrel{a_1}{\to} t_1 \stackrel{a_2}{\to} \cdots \stackrel{a_k}{\to} t_k$ with t_k a term without outgoing transitions.*

Definition 5. *The* depth *and the* norm *of a BCCS term t, denoted by $depth(t)$ and $norm(t)$, are the lengths of the longest and of the shortest termination trace of t, respectively.*

Lemma 2. *If $p \subseteq^2 q$, then*

1. *each termination trace of p is a termination trace of q;*
2. *$depth(p) = depth(q)$; and*
3. *$norm(p) \geq norm(q)$.*

Proof. We prove the three statements separately.

1. By induction on the depth of p.

   [Base case] Let $depth(p) = 0$. Then p cannot perform any transitions, so the empty trace is the only termination trace of p. Since $p \subseteq^2 q$ implies $q \subseteq^1 p$, it follows that q cannot perform any transitions either. Hence, the empty trace is also a termination trace of q.

   [Inductive case] Consider a termination trace $a_1 \cdots a_k$ of p; since $depth(p) > 0$ we have $k > 0$. Then $p \stackrel{a_1}{\to} p'$ where $a_2 \cdots a_k$ is a termination trace of p'. Since $p \subseteq^2 q$, there is a transition $q \stackrel{a_1}{\to} q'$ with $p' \subseteq^2 q'$. By the induction hypothesis $a_2 \cdots a_k$ is a termination trace of q'. So $a_1 \cdots a_k$ is a termination trace of q.

Table 3. Axiom for simulation

S	$x \lesssim_1 x + y$

Table 4. Axiom for 2-nested simulation

2S	$y \lesssim_1 x \;\Rightarrow\; x \lesssim_2 x + y$

2. $p \subseteq^2 q$ implies $p \leftrightarrows^1 q$, so clearly p and q must have equal depth.
3. By statement 1 in the lemma, the shortest termination trace of p is a termination trace of q. □

Remark: If $p \subseteq^2 q$, then q may afford more termination traces than p. As an example, consider the terms $p = aa\mathbf{0}$ and $q = p + a\mathbf{0}$. So if $p \subseteq^2 q$, then $norm(p)$ may be strictly larger than $norm(q)$.

4 A conditional axiomatization

The definition of 2-nested simulation immediately suggests an implicational proof system for the 2-nested simulation preorder. It is folklore that the axioms in Tables 2 and 3 give a complete axiomatization of the simulation preorder over the language BCCS [8]. To obtain a complete inference system for the 2-nested simulation preorder, it is sufficient to add the conditional axiom in Table 4 to the axiom system in Table 2. In axioms S and 2S, the relation symbol $\lesssim_1$ refers to inequations that are provable using the proof system for the simulation preorder, while the relation symbol $\lesssim_2$ refers to inequations that are provable using the proof system for the 2-nested simulation preorder. Not too surprisingly, we have that:

Theorem 2. *A1-4+2S is sound and complete for BCCS modulo the 2-nested simulation preorder.*

Proof. The soundness proof is left to the reader. We prove that A1-4+2S is complete modulo the 2-nested simulation preorder. Suppose $p \subseteq^2 q$. We prove, by induction on the depth of p, that $p \lesssim q$ can be derived from A1-4+2S.

Let $p = \sum_{i\in I} a_i p_i$ and $q = \sum_{j\in J} b_j q_j$. Since $p \subseteq^2 q$, for every $i \in I$ there is a $j_i \in J$ such that $a_i = b_{j_i}$ and $p_i \subseteq^2 q_{j_i}$. By the induction hypothesis, $p_i \lesssim q_{j_i}$ can be derived from A1-4+2S. Hence, $\sum_{i\in I} a_i p_i \lesssim \sum_{i\in I} a_i q_{j_i}$ can be proven from A1-4+2S.

Vice versa, since $q \subseteq^1 p$, for each $l \in J$ there is an $i_l \in I$ such that $b_l = a_{i_l} = b_{j_{i_l}}$ and $q_l \subseteq^1 p_{i_l} \subseteq^2 q_{j_{i_l}}$. By completeness of A1-4+S for the simulation preorder, $b_l q_l \lesssim a_{i_l} q_{j_{i_l}}$ can be derived from A1-4+S. So $a_{i_l} q_{j_{i_l}} \lesssim a_{i_l} q_{j_{i_l}} + b_l q_l$

can be derived using 2S. Hence, $\sum_{l\in J} a_{i_l} q_{j_{i_l}} \lesssim \sum_{j\in J} b_j q_j$ can be proven from A1-4+2S. As the index set $\{j_{i_l} \mid l \in J\}$ is included in the set $\{j_i \mid i \in I\}$, we can derive from A1-4+2S that

$$\sum_{i\in I} a_i q_{j_i} \approx \sum_{i\in I} a_i q_{j_i} + \sum_{l\in J} a_{i_l} q_{j_{i_l}} \lesssim \sum_{i\in I} a_i q_{j_i} + \sum_{j\in J} b_j q_j \approx \sum_{j\in J} b_j q_j = q \ .$$

By transitivity we conclude that $p \lesssim q$ can be derived from A1-4+2S. □

The aforementioned proof system for the 2-nested simulation preorder, albeit very natural, includes the conditional axiom 2S; moreover, the condition of this axiom contains an auxiliary relation symbol that is not defined inductively on the syntax of BCCS. This raises the question of whether there exists a finite purely (in)equational axiomatization of 2-nested simulation preorder and/or equivalence at least over the language BCCS. The remainder of this study is devoted to showing that no finite (in)equational axiomatization of 2-nested simulation exists over BCCS.

5 Inaxiomatizability of the 2-nested simulation preorder

In this section we prove that the 2-nested simulation preorder is not finitely inequationally axiomatizable. The following lemma will play a key role in the proof of this statement. In the lemma, and in the remainder of this paper, we let a^0 denote $\mathbf{0}$, and a^{m+1} denote $a(a^m)$.

Lemma 3. *If $p \subsetneq^2 a^{2m} + a^m$, then either $p \leftrightarrows^2 a^{2m}$ or $p \leftrightarrows^2 a^{2m} + a^m$.*

Proof. The case $m = 0$ is trivial; we focus on the case $m > 0$. We note, first of all, that if $q \subsetneq^2 a^k$ for some $k \geq 0$, then, by Lemma 2(1), q has only the termination trace a^k; clearly, this implies $a^k \subsetneq^2 q$.

Suppose now that $p \xrightarrow{a} p'$. Since $p \subsetneq^2 a^{2m} + a^m$, either $p' \subsetneq^2 a^{2m-1}$ or $p' \subsetneq^2 a^{m-1}$. By Lemma 2(2), p has depth $2m$. So there is at least one transition $p \xrightarrow{a} p'$ with $p' \subsetneq^2 a^{2m-1}$.

If for all transitions $p \xrightarrow{a} p'$ we have $p' \subsetneq^2 a^{2m-1}$ (and so $a^{2m-1} \subsetneq^2 p'$), then it follows that $a^{2m} \subsetneq^2 p$. On the other hand, if there exists a transition $p \xrightarrow{a} p''$ with $p'' \subsetneq^2 a^{m-1}$ (and so $a^{m-1} \subsetneq^2 p''$), then it follows that $a^{2m} + a^m \subsetneq^2 p$. □

The idea behind the proof that the 2-nested simulation preorder is not finitely inequationally axiomatizable is as follows. Assume a finite inequational axiomatization E for BCCS that is sound modulo $\subsetneq^2$. We show that, if m is sufficiently large, then, for all closed inequational derivations $a^{2m} \lesssim p_1 \lesssim \cdots \lesssim p_k$ from E with $p_k \subsetneq^2 a^{2m} + a^m$, we have that $p_k \leftrightarrows^2 a^{2m}$. So $a^{2m} \lesssim a^{2m} + a^m$ cannot be derived from E. Note that $a^{2m} \subsetneq^2 a^{2m} + a^m$.

Lemma 4. *Let $t \lesssim u$ be sound modulo $\subsetneq^2$. Let m be greater than the depth of t. Assume that $C[\sigma(u)] \subsetneq^2 a^{2m} + a^m$. Then $C[\sigma(t)] \leftrightarrows^2 a^{2m}$ implies $C[\sigma(u)] \leftrightarrows^2 a^{2m}$.*

Proof. Let $C[\sigma(t)] \leftrightarrows^2 a^{2m}$; we prove $C[\sigma(u)] \leftrightarrows^2 a^{2m}$. Since $C[\sigma(u)] \subsetneq^2 a^{2m} + a^m$, it is sufficient to show that $a^{2m} + a^m \not\subseteq^2 C[\sigma(u)]$. In fact, if $C[\sigma(u)] \subsetneq^2 a^{2m} + a^m$ and $a^{2m} + a^m \not\subseteq^2 C[\sigma(u)]$, by Lemma 3 it follows that $C[\sigma(u)] \leftrightarrows^2 a^{2m}$, which is to be shown. We prove that $a^{2m} + a^m \not\subseteq^2 C[\sigma(u)]$ holds by distinguishing two cases, depending on the form of the context $C[]$.

- *Case 1*: Suppose $C[]$ is of the form $C'[b([] + r)]$.
  Consider a transition $C[\sigma(u)] \xrightarrow{a} q'$. Since $C[]$ is of the form $C'[b([] + r)]$, clearly there is a transition $C[\sigma(t)] \xrightarrow{a} p'$ where p' can be obtained by replacing at most one subterm $\sigma(u)$ of q' by $\sigma(t)$. Since $\sigma(t) \subsetneq^2 \sigma(u)$, by Lemma 2 $\sigma(t)$ and $\sigma(u)$ have the same depth; so p' and q' have the same depth as well. Since $C[\sigma(t)] \leftrightarrows^2 a^{2m}$, it follows that $p' \subsetneq^2 a^{2m-1}$. So by Lemma 2(2), $\mathit{depth}(p') = \mathit{depth}(q') = 2m - 1$. As $\mathit{depth}(a^{m-1}) \neq 2m - 1$, by Lemma 2(2) $a^{m-1} \not\subseteq^2 q'$. This holds for all transitions $C[\sigma(u)] \xrightarrow{a} q'$, and $a^{2m} + a^m \xrightarrow{a} a^{m-1}$, so $a^{2m} + a^m \not\subseteq^2 C[\sigma(u)]$.
- *Case 2*: Suppose $C[]$ is of the form $[] + r$.
  As $\rho(t) \subsetneq^2 \rho(u)$ for all closed substitutions ρ, by Lemma 2(2) $\rho(t)$ and $\rho(u)$ have the same depth for all ρ. Clearly this implies that $\mathit{depth}(t) = \mathit{depth}(u)$, and moreover that t and u contain exactly the same variables.
  Since $\sigma(t) + r \leftrightarrows^2 a^{2m}$, by Lemma 2(3) $\mathit{norm}(\sigma(t)) \geq 2m$ and $\mathit{norm}(r) \geq 2m$. As $\sigma(u) + r \subsetneq^2 a^{2m} + a^m$, again by Lemma 2(3), we have that $\mathit{norm}(\sigma(u)) \geq m$.
  Since $\mathit{depth}(t) < m$ and $\mathit{norm}(\sigma(t)) \geq 2m$, for each variable $x \in \mathit{var}(t) = \mathit{var}(u)$ we have $\mathit{norm}(\sigma(x)) > m$.
  By the fact that $\mathit{depth}(u) = \mathit{depth}(t) < m$ and $\mathit{norm}(\sigma(u)) \geq m$, each termination trace of $\sigma(u)$ must become, after less than m transitions, a termination trace of a $\sigma(x)$ with $x \in \mathit{var}(u)$. Since for all $x \in \mathit{var}(u) = \mathit{var}(t)$ we have $\mathit{norm}(\sigma(x)) > m$, it follows that $\mathit{norm}(\sigma(u)) > m$. Since moreover $\mathit{norm}(r) \geq 2m$, we have $\mathit{norm}(\sigma(u) + r) > m$. As $a^{2m} + a^m$ has norm m, by Lemma 2(3) we may conclude that $a^{2m} + a^m \not\subseteq^2 \sigma(u) + r$. □

Remark: The inequation $ax \lesssim ax + a^1$ is sound modulo $\subsetneq^2$. However, $a^4 \not\leftrightarrows^2 a^4 + a^1$. So the side condition in the statement of Lemma 4 that $C[\sigma(u)] \subsetneq^2 a^{2m} + a^m$ cannot be omitted. (Note that $a^4 + a^1 \not\subseteq^2 a^4 + a^2$.)

Theorem 3. *BCCS modulo the 2-nested simulation preorder is not finitely inequationally axiomatizable.*

Proof. Let E be a finite, non-empty inequational axiomatization for BCCS that is sound modulo $\subsetneq^2$. Let $m > \max\{\mathit{depth}(t) \mid t \lesssim u \in E\}$.

By Lemma 4, and using induction on the length of derivations, it follows that if the closed inequation $a^{2m} \lesssim r$ can be derived from E and $r \subsetneq^2 a^{2m} + a^m$, then $r \leftrightarrows^2 a^{2m}$. As $a^{2m} + a^m \not\subseteq^2 a^{2m}$ (Lemma 2(3)), it follows that $a^{2m} \lesssim a^{2m} + a^m$ cannot be derived from E. Since $a^{2m} \subsetneq^2 a^{2m} + a^m$, we may conclude that E is not complete modulo $\subsetneq^2$. □

6 Inaxiomatizability of 2-nested simulation equivalence

We now proceed to prove that the 2-nested simulation equivalence is not finitely equationally axiomatizable. The following lemma will play a key role in the proof of this statement.

Lemma 5. *Let the inequational axiom $u \lesssim t$ be sound modulo $\subsetneq^2$. If t is of the form $\sum_{i\in I} x_i + \sum_{j\in J} a_j t_j$ and u is of the form $\sum_{k\in K} y_k + \sum_{\ell\in L} b_\ell u_\ell$, then*

- *$\{y_k \mid k \in K\} \subseteq \{x_i \mid i \in I\}$, and*
- *for each $\ell \in L$ there is a $j \in J$ such that $var(t_j) \subseteq var(u_\ell)$.*

Proof. Let m be greater than the depth of u.

Assume, towards a contradiction, that $y_k \notin \{x_i \mid i \in I\}$ for some $k \in K$. Let $\sigma(y_k) = a^m$ and let $\sigma(z) = \mathbf{0}$ for $z \neq y_k$. As $\sigma(y_k) \stackrel{a}{\to} a^{m-1}$, it follows that $\sigma(u) \stackrel{a}{\to} a^{m-1}$; so $\sigma(u)$ has a termination trace of length m. On the other hand, $\sigma(x_i) \leftrightarrows^2 \mathbf{0}$ for $i \in I$, and it is easy to see that no $\sigma(a_j t_j)$ for $j \in J$ has a termination trace of length m; so $\sigma(t)$ does not have a termination trace of length m. As $\sigma(u) \subsetneq^2 \sigma(t)$ by the soundness of $u \lesssim t$, this contradicts Lemma 2(1).

Assume, towards a contradiction, that there is an $\ell \in L$ such that $var(t_j) \not\subseteq var(u_\ell)$ for all $j \in J$. Let $\rho(z) = \mathbf{0}$ for $z \in var(u_\ell)$ and let $\rho(z) = a^m$ for $z \notin var(u_\ell)$. Since $\rho(z) = \mathbf{0}$ for $z \in var(u_\ell)$, clearly $depth(\rho(u_\ell)) \leq depth(u)-1 < m-1$. On the other hand, for all transitions $\rho(t) \stackrel{c}{\to} p'$ we have $depth(p') \geq m-1$. Namely, each transition of $\rho(t)$ is of the form $\rho(t) \stackrel{a}{\to} a^{m-1}$ or $\rho(t) \stackrel{a_j}{\to} \rho(t_j)$; by assumption, for every $j \in J$, the term t_j contains a variable $z \notin var(u_\ell)$, implying that $depth(\rho(t_j)) \geq m$. Since $\rho(u) \subsetneq^2 \rho(t)$ and $\rho(u) \stackrel{b_\ell}{\to} \rho(u_\ell)$, it follows that there is a transition $\rho(t) \stackrel{b_\ell}{\to} q'$ with $\rho(u_\ell) \subsetneq^2 q'$. Since $depth(\rho(u_\ell)) < m-1$ and $depth(q') \geq m-1$, this contradicts Lemma 2(2). □

Assume a finite equational axiomatization E for BCCS that is sound modulo $\leftrightarrows^2$. The idea behind the proof that E cannot be complete modulo $\leftrightarrows^2$ is as follows. We show that, if m is sufficiently large, then, for all closed derivations $a(a^{2m} + a^m) \approx p_1 \approx \cdots \approx p_k$ from E, $p_k \stackrel{a}{\to} p'_k$ implies $norm(p'_k) = m$. Clearly, $a(a^{2m} + a^m) + a^{2m+1}$ does not satisfy the latter property, so $a(a^{2m} + a^m) \approx a(a^{2m} + a^m) + a^{2m+1}$ cannot be derived from E. Note that $a(a^{2m} + a^m) \leftrightarrows^2 a(a^{2m} + a^m) + a^{2m+1}$.

Theorem 4. *BCCS modulo 2-nested simulation equivalence is not finitely equationally axiomatizable.*

Proof. Let E be a finite, non-empty equational axiomatization for BCCS that is sound modulo $\leftrightarrows^2$. Let $m > \max\{depth(t) \mid t \approx u \in E\}$.

First we prove the following fact:

Claim: Let $t \approx u \in E$ and let σ be a closed substitution such that $C[\sigma(t)]$ only has termination traces of lengths $m+1$ and $2m+1$. Suppose moreover that for every transition $C[\sigma(t)] \stackrel{b}{\to} p'$ we have $norm(p') = m$. Then, for every transition $C[\sigma(u)] \stackrel{c}{\to} q'$ we have $norm(q') = m$.

Proof of the claim. First of all, note that, as $C[\sigma(t)] \leftrightarrows^2 C[\sigma(u)]$, by Lemma 2(1) we know that $C[\sigma(u)]$ only has termination traces of lengths $m+1$ and $2m+1$. We now proceed with the proof by distinguishing two cases, depending on the form of the context $C[]$.

- *Case 1*: Suppose $C[]$ is of the form $C'[d([]+r)]$.
  Consider a transition $C[\sigma(u)] \xrightarrow{c} q'$. Since $C[]$ is of the form $C'[d([]+r)]$, clearly there is a transition $C[\sigma(t)] \xrightarrow{c} p'$ where p' can be obtained by replacing at most one subterm $\sigma(u)$ of q' by $\sigma(t)$. Since $\sigma(t) \leftrightarrows^2 \sigma(u)$, by Lemma 2(3) $\sigma(t)$ and $\sigma(u)$ have the same norm; so p' and q' have the same norm as well. By assumption $norm(p') = m$, so $norm(q') = m$.
- *Case 2*: Suppose $C[]$ is of the form $[]+r$.
  Let t be of the form $\sum_{i\in I} x_i + \sum_{j\in J} a_j t_j$ and let u be of the form $\sum_{k\in K} y_k + \sum_{\ell\in L} b_\ell u_\ell$. Consider a transition $\sigma(u)+r \xrightarrow{c} q'$. We distinguish three possible cases.
- *Case 2.1*: Let $r \xrightarrow{c} q'$. Then $\sigma(t)+r \xrightarrow{c} q'$, which implies $norm(q') = m$.
- *Case 2.2*: Let $\sigma(y_k) \xrightarrow{c} q'$ for some $k \in K$. By Lemma 5, $y_k = x_i$ for some $i \in I$, so $\sigma(x_i) \xrightarrow{c} q'$. Then $\sigma(t)+r \xrightarrow{c} q'$, which implies $norm(q') = m$.
- *Case 2.3*: Let $q' = \sigma(u_\ell)$ for some $\ell \in L$. By Lemma 5, $var(t_j) \subseteq var(u_\ell)$ for some $j \in J$. Since $depth(t) < m$, we have $depth(t_j) < m$. On the other hand, $\sigma(t)+r \xrightarrow{a_j} \sigma(t_j)$ implies $norm(\sigma(t_j)) = m$. Hence, each termination trace of $\sigma(t_j)$ (so in particular its shortest one) must become, after less than m transitions, a termination trace of a $\sigma(x)$ with $x \in var(t_j)$. So $norm(\sigma(t_j)) = m$ implies $norm(\sigma(x)) \leq m$ for some $x \in var(t_j)$. Since $x \in var(u_\ell)$ and $depth(u_\ell) < m$, we have $norm(\sigma(u_\ell)) < 2m$. Since $\sigma(u)$ only has termination traces of lengths $m+1$ and $2m+1$, and moreover $\sigma(u) \xrightarrow{b_\ell} \sigma(u_\ell)$, it follows that $\sigma(u_\ell)$ can only have termination traces of lengths m and $2m$. Hence, $norm(\sigma(u_\ell)) = m$. (*End of the proof of the claim*)

Suppose now that p only has termination traces of lengths $m+1$ and $2m+1$. Suppose moreover that for every transition $p \xrightarrow{b} p'$ we have $norm(p') = m$. By induction on the length of equational derivations from E, using the claim that we have just proven, it is easy to show that if $p \approx q$ can be derived from E, then for every transition $q \xrightarrow{c} q'$ we have $norm(q') = m$.

Concluding, $a(a^{2m}+a^m)$ only has termination traces of lengths $m+1$ and $2m+1$. Moreover, its only transition is $a(a^{2m}+a^m) \xrightarrow{a} a^{2m}+a^m$, and $a^{2m}+a^m$ has norm m. Finally, $a(a^{2m}+a^m)+a^{2m+1} \xrightarrow{a} a^{2m}$, and a^{2m} does not have norm m. So $a(a^{2m}+a^m) \approx a(a^{2m}+a^m)+a^{2m+1}$ cannot be derived from E. Since $a(a^{2m}+a^m) \leftrightarrows^2 a(a^{2m}+a^m)+a^{2m+1}$, we may conclude that E is not complete modulo $\leftrightarrows^2$. □

7 The 3-nested simulation preorder and beyond

Groote and Vaandrager [10] actually introduced a hierarchy of n-nested simulation preorders for $n \geq 2$. The following definition generalizes Definition 2.

Definition 6. *For $n \geq 1$, $p \subseteq^{n+1} q$ iff p R q with R a simulation and R^{-1} included in $\subseteq^n$. The kernel of $\subseteq^{n+1}$ is denoted by $\leftrightarrows^{n+1}$.*

It is easy to see that $\subseteq^{n+1}$ is included in $\leftrightarrows^n$, for $n \geq 1$. The characterization of the 2-nested simulation preorder in Theorem 1 generalizes to the n-nested simulation preorders for $n \geq 3$. Also, the idea behind the conditional axiomatization for the 2-nested preorder (see Theorem 2) generalizes to the n-nested simulation preorders for $n \geq 3$. The proofs of these results are omitted.

Theorem 5. *For $n \geq 1$, and for closed process terms p and q over BCCS, $p \subseteq^{n+1} q$ iff*

(1) for all $p \xrightarrow{a} p'$ there is a $q \xrightarrow{a} q'$ with $p' \subseteq^{n+1} q'$, and
(2) $q \subseteq^n p$.

Definition 7. *For $n \geq 1$, let $\lesssim_{n+1}$ be the preorder generated by the equational axioms A1-4 together with $y \lesssim_n x \Rightarrow x \lesssim_{n+1} x + y$.*

Theorem 6. *For $n \geq 1$, and for closed process terms p and q over BCCS, $p \lesssim_n q$ iff $p \subseteq^n q$.*

It follows from the proof of Theorem 4 that there does not exist a finite inequational axiomatization for the 3-nested simulation preorder.

Theorem 7. *BCCS modulo the 3-nested simulation preorder is not finitely inequationally axiomatizable.*

Proof. Let E be a finite inequational axiomatization for BCCS that is sound modulo $\subseteq^3$. Since $\subseteq^3$ is included in $\leftrightarrows^2$, clearly the equational axiomatization $E' = \{t \approx u \mid t \lesssim u \in E\}$ is sound modulo $\leftrightarrows^2$. Let $m > \max\{depth(t) \mid t \approx u \in E'\}$. In the proof of Theorem 4 it was shown that $a(a^{2m} + a^m) \approx a(a^{2m} + a^m) + a^{2m+1}$ cannot be derived from E'. Hence, $a(a^{2m} + a^m) \lesssim a(a^{2m} + a^m) + a^{2m+1}$ cannot be derived from E. Since $a(a^{2m} + a^m) \subseteq^3 a(a^{2m} + a^m) + a^{2m+1}$, it follows that E is not complete modulo $\subseteq^3$. □

We leave it as an open question whether there exist finite equational axiomatizations for n-nested simulation equivalence if $n \geq 3$, and finite inequational axiomatizations for the n-nested simulation preorder if $n \geq 4$.

References

1. L. Aceto, Z. Ésik, and A. Ingólfsdóttir, *On the two-variable fragment of the equational theory of the max-sum algebra of the natural numbers*, in Proceedings of the 17th STACS, H. Reichel and S. Tison, eds., vol. 1770 of Lecture Notes in Computer Science, Springer-Verlag, Feb. 2000, pp. 267–278.
2. L. Aceto, Z. Ésik, and A. Ingólfsdóttir, *The max-plus algebra of the natural numbers has no finite equational basis*, research report, BRICS, Department of Computer Science, Aalborg University, October 1999. Pp. 25. To appear in *Theoretical Computer Science*.

3. L. Aceto, W. Fokkink, and A. Ingólfsdóttir, *A menagerie of non-finitely based process semantics over BPA*—from ready simulation to completed traces*, Mathematical Structures in Computer Science, 8 (1998), pp. 193–230.
4. J. Baeten and J. Klop, eds., *Proceedings CONCUR 90,* Amsterdam, vol. 458 of Lecture Notes in Computer Science, Springer-Verlag, 1990.
5. J. Bergstra and J. W. Klop, *Fixed point semantics in process algebras*, Report IW 206, Mathematisch Centrum, Amsterdam, 1982.
6. J. H. Conway, *Regular Algebra and Finite Machines*, Mathematics Series (R. Brown and J. De Wet eds.), Chapman and Hall, London, United Kingdom, 1971.
7. J. L. Gischer, *The equational theory of pomsets*, Theoretical Comput. Sci., 61 (1988), pp. 199–224.
8. R. van Glabbeek, *The linear time – branching time spectrum*, in Baeten and Klop [4], pp. 278–297.
9. J. F. Groote, *A new strategy for proving ω–completeness with applications in process algebra*, in Baeten and Klop [4], pp. 314–331.
10. J. F. Groote and F. Vaandrager, *Structured operational semantics and bisimulation as a congruence*, Information and Computation, 100 (1992), pp. 202–260.
11. R. Keller, *Formal verification of parallel programs*, Comm. ACM, 19 (1976), pp. 371–384.
12. H. Lin, *An interactive proof tool for process algebras*, in 9th Annual Symposium on Theoretical Aspects of Computer Science, vol. 577 of Lecture Notes in Computer Science, Cachan, France, 13–15 Feb. 1992, Springer, pp. 617–618.
13. R. Milner, *An algebraic definition of simulation between programs*, in Proceedings 2nd Joint Conference on Artificial Intelligence, William Kaufmann, 1971, pp. 481–489.
14. ———, *A Calculus of Communicating Systems*, vol. 92 of Lecture Notes in Computer Science, Springer-Verlag, 1980.
15. ———, *Communication and Concurrency*, Prentice-Hall International, Englewood Cliffs, 1989.
16. W. Mitchell and D. Carlisle, *Modal observation equivalence of processes*, Technical Report UMCS-96-1-1, Manchester University, Computer Science, 1996.
17. F. Moller, *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. G. Plotkin, *A structural approach to operational semantics*, Report DAIMI FN-19, Computer Science Department, Aarhus University, 1981.
20. V. Redko, *On defining relations for the algebra of regular events*, Ukrainskii Matematicheskii Zhurnal, 16 (1964), pp. 120–126. In Russian.
21. P. Sewell, *Nonaxiomatisability of equivalences over finite state processes*, Annals of Pure and Applied Logic, 90 (1997), pp. 163–191.
22. S. K. Shukla, D. J. Rosenkrantz, H. B. Hunt III, and R. E. Stearns, *A HORNSAT based approach to the polynomial time decidability of simulation relations for finite state processes*, in DIMACS Workshop on Satisfiability Problem: Theory and Applications, D. Du, J. Gu, and P. M. Pardalos, eds., vol. 35 of DIMACS Series in Discrete Mathematics and Computer Science, 1996, pp. 603–642.

Recent BRICS Report Series Publications

RS-00-20 **Luca Aceto, Willem Jan Fokkink, and Anna Ingólfsdóttir.** ***2-Nested Simulation is not Finitely Equationally Axiomatizable*****. August 2000. 13 pp.**

RS-00-19 **Vinodchandran N. Variyam.** ***A Note on*** $\mathrm{NP} \cap \mathrm{coNP/poly}$**. August 2000. 7 pp.**

RS-00-18 **Federico Crazzolara and Glynn Winskel.** ***Language, Semantics, and Methods for Cryptographic Protocols*****. August 2000. ii+42 pp.**

RS-00-17 **Thomas S. Hune.** ***Modeling a Language for Embedded Systems in Timed Automata*****. August 2000. 26 pp. Earlier version entitled** ***Modelling a Real-Time Language*** **appeared in Gnesi and Latella, editors,** ***Fourth International ERCIM Workshop on Formal Methods for Industrial Critical Systems,*** **FMICS '99 Proceedings of the FLoC Workshop, 1999, pages 259–282.**

RS-00-16 **Jiří Srba.** ***Complexity of Weak Bisimilarity and Regularity for BPA and BPP*****. June 2000. 20 pp. To appear in Aceto and Victor, editors,** ***Expressiveness in Concurrency: Fifth International Workshop EXPRESS '00 Proceedings,*** **ENTCS, 2000.**

RS-00-15 **Daniel Damian and Olivier Danvy.** ***Syntactic Accidents in Program Analysis: On the Impact of the CPS Transformation*****. June 2000. Extended version of an article to appear in** ***Proceedings of the fifth ACM SIGPLAN International Conference on Functional Programming,*** **2000.**

RS-00-14 **Ronald Cramer, Ivan B. Damgård, and Jesper Buus Nielsen.** ***Multiparty Computation from Threshold Homomorphic Encryption*****. June 2000. ii+38 pp.**

RS-00-13 **Ondřej Klíma and Jiří Srba.** ***Matching Modulo Associativity and Idempotency is NP-Complete*****. June 2000. 19 pp. To appear in** ***Mathematical Foundations of Computer Science: 25th International Symposium,*** **MFCS '00 Proceedings, LNCS, 2000.**

RS-00-12 **Ulrich Kohlenbach.** ***Intuitionistic Choice and Restricted Classical Logic*****. May 2000. 9 pp.**

RS-00-11 **Jakob Pagter.** ***On Ajtai's Lower Bound Technique for R-way Branching Programs and the Hamming Distance Problem*****. May 2000. 18 pp.**