On Finite Alphabets and Infinite Bases III: Simulation*

Taolue Chen[1,2] and Wan Fokkink[1,3]

[1] CWI, Department of Software Engineering, PO Box 94079, 1090 GB Amsterdam, The Netherlands
chen@cwi.nl
[2] Nanjing University, State Key Laboratory of Novel Software Technology, Nanjing, Jiangsu, P.R. China, 210093
[3] Vrije Universiteit Amsterdam, Department of Theoretical Computer Science, De Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands
wanf@cs.vu.nl

Abstract. This paper studies the (in)equational theory of simulation preorder and equivalence over the process algebra BCCSP. We prove that in the presence of a finite alphabet with at least two actions, the (in)equational theory of BCCSP modulo simulation preorder or equivalence does not have a finite basis. In contrast, in the presence of an alphabet that is infinite or a singleton, the equational theory for simulation equivalence does have a finite basis.

1 Introduction

Labeled transition systems constitute a fundamental model of concurrent computation which is widely used in light of its flexibility and applicability. They model processes by explicitly describing their states and their transitions from state to state, together with the actions that produce them. Several notions of behavioral equivalence have been proposed, with the aim to identify those states of labeled transition systems that afford the same observations. The lack of consensus on what constitutes an appropriate notion of observable behavior for reactive systems has led to a large number of proposals for behavioral equivalences for concurrent processes.

Van Glabbeek [9] presented the linear time - branching time spectrum of behavioral preorders and equivalences for finitely branching, concrete, sequential processes. In this paper we focus on the *simulation* semantics in this spectrum. A relation R between processes is a simulation if $s_0\ R\ s_1$ and $s_0 \stackrel{a}{\rightarrow} s_0'$ implies $s_1 \stackrel{a}{\rightarrow} s_1'$ with $s_0'\ R\ s_1'$. It was introduced by Milner in his seminal work on CCS [21], and the first branching-time semantics to be used studied in the setting of process algebra (before the formulation of bisimulation by Park [27] appeared). The

* Partially supported by the Dutch Bsik project BRICKS (Basic Research in Informatics for Creating the Knowledge Society), 973 Program of China (No. 2002CB312002), NNSFC (No. 60233010, No. 60273034, No. 60403014).

C. Baier and H. Hermanns (Eds.): CONCUR 2006, LNCS 4137, pp. 421–434, 2006.

notion of simulation is well studied in the literatures, both from the theoretical and from the practical point of view, see e.g. [14,17].

Other semantics in the linear time - branching time spectrum are based on simulation notions or on decorated traces. Figure 1 depicts the linear time - branching time spectrum, where a directed edge from one equivalence to another means that the source of the edge is finer than the target.

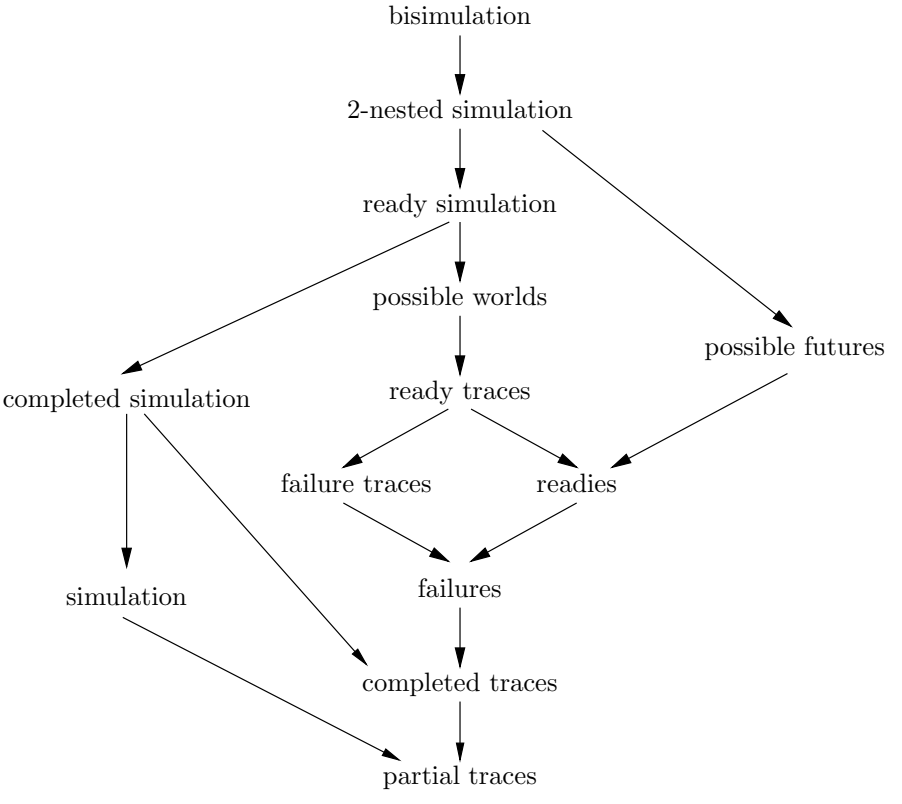

Fig. 1. The linear time - branching time spectrum

Van Glabbeek [9] studied the semantics in his spectrum in the setting of the process algebra BCCSP, which contains only the basic process algebraic operators from CCS and CSP, but is sufficiently powerful to express all finite synchronization trees. Van Glabbeek gave axiomatizations for the semantics in the spectrum, such that two closed BCCSP terms can be equated by the axioms if and only if they are equivalent.

Having defined a model of an axiomatization for a process algebra in terms of labeled transition systems, it is natural to study the connection between the equations that are valid in the chosen model, and those that are derivable from the axioms using the rules of equational logic. A key question here is whether there is a finite axiomatization that is ω-complete. That is, if all closed instances

of an equation can be derived, does this imply that the equation itself can be derived from the axiomatization using the rules of equational logic? (We also refer to an ω-complete axiom system as a *basis* for the equational theory.) An ω-complete axiomatization of a behavioral congruence yields a purely syntactic characterization, independent of labeled transition systems and of the actual details of the definition of the behavioral congruence. This bridge between syntax and semantics plays 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 using general purpose theorem provers or proof checkers, and form the basis of purpose-built axiomatic verification tools like, e.g., PAM [15]. In particular, for theorem proving applications, it is convenient if an axiomatization is ω-complete, because it means that proofs by (structural) induction can be avoided in favor of purely equational reasoning; see [16]. In [12] it was argued that ω-completeness is desirable for the partial evaluation of programs.

The existence of a finite basis for an equational theory is a classic topic of study in universal algebra (see, e.g., [20]), dating back to Lyndon [18]. Murskiĭ [26] proved that "almost all" finite algebras (namely all quasi-primal ones) are finitely based, while in [25] he presented an example of a three-element algebra that has no finite basis. Henkin [13] showed that the algebra of naturals with addition and multiplication is finitely based, while Gurevič [11] showed that after adding exponentiation the algebra is no longer finitely based. McKenzie [19] settled Tarski's Finite Basis Problem in the negative, by showing that the general question whether a finite algebra is finitely based is undecidable.

Notable examples of ω-incomplete axiomatizations in the literature are the $\lambda K\beta\eta$-calculus (see [28]) and the equational theory of CCS [24]. Therefore laws such as commutativity of parallelism, which are valid in the initial model but which cannot be derived, are often added to the latter equational theory. For such extended equational theories, ω-completeness results were presented in the setting of CCS [23,3] and ACP [6].

A number of positive and negative results regarding finite ω-complete axiomatizations for BCCSP occur in the literature. For a comprehensive survey and discussion of open problems, the interested reader is referred to [2].

- *Infinite alphabets*:[1] Moller [23] proved that the ground-complete axiomatization for BCCSP modulo bisimulation equivalence is ω-complete. Groote [10] presented ω-completeness proofs for completed trace equivalence, for trace equivalence (in the presence of an alphabet A with $|A| > 1$), and for readiness and failures equivalence (if $|A| = \infty$). Van Glabbeek [9] noted (without proof) that Groote's technique of inverted substitutions can also be used to prove that the ground-complete axiomatizations for BCCSP modulo simulation, ready simulation and failure trace equivalence are ω-complete if $|A| = \infty$.

[1] In case of an infinite alphabet, occurrences of action names in axioms should be interpreted as variables, as otherwise most of the axiomatizations mentioned in this paragraph would be infinite.

Blom, Fokkink and Nain [4] proved that BCCSP modulo ready trace equivalence does not have a finite sound and ground-complete axiomatization if $|A| = \infty$. Aceto, Fokkink, van Glabbeek and Ingolfsdottir [1] proved such a negative result for 2-nested simulation and possible futures equivalence, independent of the cardinality of A.

– *Finite alphabets*: Fokkink and Nain [8] obtained an ω-complete axiomatization for BCCSP modulo failures equivalence if $|A| < \infty$, by adding one extra axiom that uses the cardinality of A. In [7] they proved that if $1 < |A| < \infty$, BCCSP modulo any semantics in between readiness and possible worlds equivalence does not have a finite basis. In [5], Chen, Fokkink and Nain proved that BCCSP modulo completed simulation equivalence does not have a finite basis if $|A| > 1$, and that BCCSP modulo ready simulation equivalence does not have a finite basis if $1 < |A| < \infty$.

If $|A| = 1$, then the semantics in the linear time - branching time spectrum from completed trace up to ready simulation equivalence all coincide with completed trace equivalence, while simulation equivalence coincides with trace equivalence. And there exists a finite basis for the equational theories of BCCSP modulo completed trace and trace equivalence if $|A| = 1$.

In this paper we consider BCCSP modulo simulation semantics. We prove that if $1 < |A| < \infty$, then no finite sound and ground-complete axiomatization for BCCSP modulo simulation preorder and equivalence is ω-complete. This solves an open question mentioned by van Glabbeek [9, p78] and Aceto et al. [2, p355]. To give some intuition for the infinite family of inequations on which our negative result for simulation preorder is based, we present one of these inequations, for $A = \{a, b\}$:

$$\begin{aligned} a(x + aa\mathbf{0} + ab\mathbf{0} + ba\mathbf{0} + bb\mathbf{0}) \preccurlyeq\ & a(x + aa\mathbf{0} + ab\mathbf{0} + ba\mathbf{0}) \\ & + a(x + aa\mathbf{0} + ab\mathbf{0} + bb\mathbf{0}) \\ & + a(x + aa\mathbf{0} + ba\mathbf{0} + bb\mathbf{0}) \\ & + a(x + ab\mathbf{0} + ba\mathbf{0} + bb\mathbf{0}) \\ & + a(a(a\mathbf{0} + b\mathbf{0}) + b(a\mathbf{0} + b\mathbf{0})) \end{aligned}$$

It is sound modulo simulation preorder. Namely, given a closed substitution ρ, $\rho(x) + aa\mathbf{0} + ab\mathbf{0} + ba\mathbf{0} + bb\mathbf{0}$ is simulated either by $a(a\mathbf{0} + b\mathbf{0}) + b(a\mathbf{0} + b\mathbf{0})$, if $\rho(x)$ cannot perform a trace of length two, or by for instance $\rho(x) + aa\mathbf{0} + ab\mathbf{0} + bb\mathbf{0}$, if $\rho(x)$ can perform the trace ba. The equation above can be generalized to a family of equations of any depth (see Section 3.1) that blocks the existence of a finite basis. Our proof of this fact is based on what in [2, Section 2.3] is called a proof-theoretic technique. Given a finite sound axiomatization E, we give a property of equations that:

– holds true for each instantiation of the axioms in E;
– is preserved by the rules of equational logic; and
– fails for one of the equations in the aforementioned infinite family.

So then this latter sound equation cannot be derived from E.

In contrast, using the technique of inverted substitutions from [10], we present a proof of the claim in [9] that if $|A| = \infty$, then the ground-complete axiomatization of BCCSP modulo simulation equivalence is ω-complete. As remarked above, if $|A| = 1$, then simulation equivalence coincides with trace equivalence, and in that case a finite basis also exists.

We note that only one open question regarding ω-complete axiomatizations for BCCSP modulo the semantics in the linear time - branching time spectrum remains. Namely, it is unknown whether BCCSP modulo failure trace equivalence has a finite basis if $1 < |A| < \infty$.

This paper is set up as follows. Section 2 presents basic definitions regarding simulation semantics, the process algebra BCCSP, and (in)equational logic. Section 3 contains the proofs of the negative results for simulation preorder and equivalence in case $1 < |A| < \infty$. Section 4 contains a short proof of the positive result for simulation equivalence in case $|A| = \infty$.

2 Preliminaries

Simulation semantics: A *labeled transition system* contains a set of states, with typical element s, and a set of transitions $s \xrightarrow{a} s'$, where a ranges over some set A of labels.

Definition 1 (Simulation). *Assume a labeled transition system. A* simulation *is a binary relation R on states such that $s_0\ R\ s_1$ and $s_0 \xrightarrow{a} s_0'$ imply $s_1 \xrightarrow{a} s_1'$ with $s_0'\ R\ s_1'$.*

We write $s_0 \precsim s_1$ if $s_0\ R\ s_1$ with R a simulation. Simulation equivalence*, i.e., $\precsim \cap \precsim^{-1}$, is denoted by $\simeq$. If $s_0 \simeq s_1$, we say that s_0 is* similar *to s_1.*

Syntax of BCCSP: BCCSP(A) is a basic process algebra for expressing finite process behavior. Its syntax consists of closed (process) terms p, q that are constructed from a constant $\mathbf{0}$, a binary operator $\_+\_$ called *alternative composition*, and unary *prefix* operators $a\_$, where a ranges over some nonempty set A of *actions* (with typical elements a, b). Open terms t, u, v, w can moreover contain variables from a countably infinite set V (with typical elements x, y, z). The sets of closed and open terms are denoted by T(BCCSP) and $\mathbb{T}$(BCCSP), respectively. We let $var(t)$ denote the set of variables occurring in term t.

A (closed) substitution maps variables in V to (closed) terms. For every term t and substitution σ, the term $\sigma(t)$ is obtained by replacing every occurrence of a variable x in t by $\sigma(x)$.

Transition rules: Intuitively, closed BCCSP(A)-terms represent finite process behaviors, where $\mathbf{0}$ does not exhibit any behavior, $p + q$ is the nondeterministic choice between the behaviors of p and q, and ap executes action a to transform into p. This intuition is captured, in the style of Plotkin, by the transition rules below, which give rise to A-labeled transitions between closed terms.

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

Simulation preorder $\precsim$ constitutes a *precongruence* for closed BCCSP(A)-terms. That is, $p_1 \precsim q_1$ and $p_2 \precsim q_2$ implies $ap_1 \precsim aq_1$ for $a \in A$ and $p_1 + p_2 \precsim q_1 + q_2$. Likewise, simulation equivalence constitutes a *congruence* for closed BCCSP(A)-terms.

Equations and inequations: An *axiomatization* E is a collection of either inequations $t \preccurlyeq u$ or equations $t \approx u$. We write $E \vdash t \preccurlyeq u$ or $E \vdash t \approx u$ if this (in)equation can be derived from the (in)equations in E using the standard rules of (in)equational logic, where the rule for symmetry can be applied for equational derivations but not for inequational ones. An axiomatization E is *sound* modulo $\precsim$ (or $\simeq$) if for any open terms t, u, from $E \vdash t \preccurlyeq u$ (or $E \vdash t \approx u$) it follows that $\rho(t) \precsim \rho(u)$ (or $\rho(t) \simeq \rho(u)$) for all closed substitutions ρ. E is *ground-complete* modulo $\precsim$ (or $\simeq$) if $p \precsim q$ (or $p \simeq q$) implies $E \vdash p \preccurlyeq q$ (or $E \vdash p \approx q$), for all closed terms p and q. Finally, E is *ω-complete* if for any open terms t, u with $E \vdash \rho(t) \preccurlyeq \rho(u)$ (or $E \vdash \rho(t) \approx \rho(u)$) for all closed substitutions ρ, we have $E \vdash t \preccurlyeq u$ (or $E \vdash t \approx u$).

The core axioms A1-4 [22] for BCCSP(A) below are ω-complete, and sound and ground-complete modulo bisimulation equivalence, which is the finest semantics in the linear time - branching time spectrum (see Figure 1).

$$\begin{array}{ll} \text{A1} & x + y \approx y + x \\ \text{A2} & (x + y) + z \approx x + (y + z) \\ \text{A3} & x + x \approx x \\ \text{A4} & x + \mathbf{0} \approx x \end{array}$$

In the remainder of this paper, process terms are considered modulo A1-4. A term x or at is a *summand* of each term $x + u$ or $at + u$, respectively. We use *summation* $\sum_{i \in \{i_1,\ldots,i_k\}} t_i$ (with $k \geq 0$) to denote $t_{i_1} + \cdots + t_{i_k}$, where the empty sum denotes $\mathbf{0}$. As binding convention, alternative composition and summation bind weaker than prefixing.

Open terms: For open terms t and u, we define $t \precsim u$ (or $t \simeq u$) if $\rho(t) \precsim \rho(u)$ (resp. $\rho(t) \simeq \rho(u)$) for all closed substitutions ρ.

Since we will be interested in ω-completeness, it is useful to extend the operational semantics to open terms, by assuming that variables do not exhibit any behavior.

Definition 2 (Traces). *A sequence $a_1 \cdots a_m \in A^*$, with $m \geq 0$, is a* trace *of a term t_0 if there exists a sequence of transitions $t_0 \stackrel{a_1}{\rightarrow} t_1 \stackrel{a_2}{\rightarrow} \cdots \stackrel{a_m}{\rightarrow} t_m$. We write $t_0 \stackrel{a_1 \cdots a_m}{\rightarrow} t_m$.*

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

We prove some basic facts for relations $t \precsim u$.

Lemma 1

1. *Let $|A| > 1$. If $t \precsim u$, and x is a summand of t, then x is also a summand of u.*
2. *If $t \precsim u$, then $depth(t) \leq depth(u)$.*
3. *If $t \precsim u$, then $var(t) \subseteq var(u)$.*

Proof. 1. Let $m > \mathit{depth}(u)$, $a \neq b$, and ρ the closed substitution with $\rho(x) = a^m b\mathbf{0}$ and $\rho(y) = \mathbf{0}$ for any variable $y \neq x$. By assumption, x is a summand of t, so $\rho(t) \stackrel{a^m b}{\rightarrow} \mathbf{0}$. Since $t \precsim u$, $\rho(t) \precsim \rho(u)$. It follows that $\rho(u) \stackrel{a^m b}{\rightarrow} p$ with $\mathbf{0} \precsim p$. Since $m > \mathit{depth}(u)$, clearly $u \stackrel{a^\ell}{\rightarrow} y + u'$ and $\rho(y) \stackrel{a^{m-\ell} b}{\rightarrow} p$, for some $\ell \leq \mathit{depth}(u)$, variable y and term u'. Since $\ell \leq \mathit{depth}(u) < m$, we have $\rho(y) \neq \mathbf{0}$, and hence $y = x$. Since $\rho(y) \stackrel{a^{m-\ell} b}{\rightarrow} p$ and $a \neq b$, it follows that $\ell = 0$. Concluding, x is also a summand of u.

2. Let ρ be the closed substitution with $\rho(x) = \mathbf{0}$ for all variables x. Since $t \preccurlyeq u$, $\rho(t) \precsim \rho(u)$. From the definition of $\precsim$, it follows that $\mathit{depth}(\rho(t)) \leq \mathit{depth}(\rho(u))$. Hence $\mathit{depth}(t) = \mathit{depth}(\rho(t)) \leq \mathit{depth}(\rho(u)) = \mathit{depth}(u)$.

3. Suppose, towards a contradiction, that there exists some $x \in \mathit{var}(t) \backslash \mathit{var}(u)$. Let $m > \mathit{depth}(u)$ and ρ the closed substitution with $\rho(x) = a^m\mathbf{0}$ and $\rho(y) = \mathbf{0}$ for any variable $y \neq x$. Since $t \precsim u$, $\rho(t) \precsim \rho(u)$. Clearly, $\mathit{depth}(\rho(t)) \geq m > \mathit{depth}(\rho(u))$, which contradicts (2). □

We note that Lemma 1(1) would not hold if $|A| = 1$. For instance, in that case, we have $ax + x \simeq ax$.

3 $1 < |A| < \infty$

In this section we present a proof that the (in)equational theory of BCCSP(A) modulo simulation semantics does not have a finite basis, provided that $1 < |A| < \infty$.

3.1 Simulation Preorder

We start with proving that the inequational theory of BCCSP(A) modulo $\precsim$ does not have a finite basis. The corner stone for this negative result is the infinite family of inequations

$$a(x + \Psi_n) \preccurlyeq \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$$

for $n \geq 0$. Here, the Φ_n are defined inductively as follows:

$$\begin{cases} \Phi_0 & = \mathbf{0} \\ \Phi_{n+1} & = \sum_{b \in A} b\,\Phi_n \end{cases}$$

Moreover, the Ψ_n and Ψ_n^θ are defined by:

$$\Psi_n = \sum_{b_1 \cdots b_n \in A^n} b_1 \cdots b_n \mathbf{0}$$

$$\Psi_n^\theta = \sum_{b_1 \cdots b_n \in A^n \backslash \{\theta\}} b_1 \cdots b_n \mathbf{0} \quad \text{for } \theta \in A^n$$

For any p with $\mathit{depth}(p) \leq n$, clearly $p \precsim \Phi_n$. So in particular, $\Psi_n \precsim \Phi_n$.

It is not hard to see that the inequations above are sound modulo $\precsim$. The idea is that, given a closed substitution ρ, either $depth(\rho(x)) < n$, in which case $a(\rho(x) + \Psi_n)$ is simulated by $a\Phi_n$. Or $\rho(x) \stackrel{b_1 \cdots b_n}{\rightarrow}$, in which case $a(\rho(x) + \Psi_n)$ is simulated by $a(\rho(x) + \Psi_n^{b_1 \cdots b_n})$.

Proposition 1. *Let E be a finite axiomatization over* BCCSP(A) *that is sound modulo $\precsim$. Let $n > 1$ be greater than or equal to the depth of any term in E. Then from E we cannot derive the inequation*

$$a(x + \Psi_n) \preccurlyeq \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$$

The main part of this section is devoted to proving Proposition 1. We start with two key lemmas.

Lemma 2. *If $a(x + \Psi_n) \precsim at \precsim \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$, then $at \simeq a(x + \Psi_n)$.*

Proof. Since $x + \Psi_n \precsim t$, by Lemma 1(1), x is a summand of t. Then (modulo A3) $t = x + t'$ where x is not a summand of t'. We prove that $t' \precsim \Psi_n$.

Since $at \precsim \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$, by Lemma 1(3), $var(t') \subseteq var(t) \subseteq \{x\}$. Assume, towards a contradiction, that x occurs in t'. Consider a substitution σ with $\sigma(x) = a^n\mathbf{0}$. Clearly $depth(\sigma(t')) > depth(\sigma(x))$. By assumption, $a\sigma(t) \precsim \sum_{\theta \in A^n} a(\sigma(x) + \Psi_n^\theta) + a\Phi_n$. However, $depth(a\sigma(t)) = depth(\sigma(t)) + 1 \geq depth(\sigma(t')) + 1 > depth(\sigma(x)) + 1 = n + 1$, while $depth(a(\sigma(x) + \Psi_n^\theta) + a\Phi_n) = n + 1$. This is a contradiction according to Lemma 1(2). In summary, t' is a closed term.

Consider a substitution ρ with $\rho(x) = a^{n+1}\mathbf{0}$. By assumption, $a(\rho(x) + t') \precsim \sum_{\theta \in A^n} a(\rho(x) + \Psi_n^\theta) + a\Phi_n$. Clearly, $\rho(x) + t' \not\precsim \Phi_n$, so $\rho(x) + t' \precsim \rho(x) + \Psi_n^\theta$ for some $\theta \in A^n$. Hence $t' \precsim a^{n+1}\mathbf{0} + \Psi_n^\theta$. Since $at \precsim \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$, by Lemma 1(2), $depth(t') \leq depth(t) \leq n$. So it follows that $t' \precsim a^n\mathbf{0} + \Psi_n^\theta \precsim \Psi_n$.

Then $at = a(x + t') \precsim a(x + \Psi_n)$. By assumption, $a(x + \Psi_n) \precsim at$. Hence $at \simeq a(x + \Psi_n)$. □

Lemma 3. *Assume that:*

- $t \precsim u$;
- $n \geq depth(u)$ *and* $n > 1$;
- $\sigma(t)$ *has a summand similar to* $a(x + \Psi_n)$; *and*
- $\sigma(u) \precsim \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$.

Then $\sigma(u)$ has a summand similar to $a(x + \Psi_n)$.

Proof. We can write $t = \sum_{i \in I} t_i$ and $u = \sum_{j \in J} u_j$ for some finite index sets I and J, where each term t_i and u_j is either a variable or of the form av. According to the third proviso of this lemma, for some $i_0 \in I$, $\sigma(t_{i_0})$ has a summand similar to $a(x + \Psi_n)$. We proceed by a case analysis on the form of t_{i_0}.

1. Let $t_{i_0} \in V$. Since $t \precsim u$ and $t_{i_0} \in V$, by Lemma 1(1), u also has t_{i_0} as a summand. Since $\sigma(t_{i_0})$ has a summand similar to $a(x + \Psi_n)$, the same holds for $\sigma(u)$.

2. Let $t_{i_0} = at'$ for some term t'. Then $a\sigma(t') \simeq a(x + \Psi_n)$. Let $\{y_k \mid k \in K\}$ be the collection of variable summands of t', for some finite index set K. Since $\sigma(t') \simeq x + \Psi_n$, by Lemma 1(1), x is a summand of $\sigma(t')$. So x is a summand of $\sigma(y_{k_0})$ for some $k_0 \in K$. In particular, $K \neq \emptyset$.

   Since V is countable, there exists an injective function $\ulcorner\cdot\urcorner : V \to \mathbb{N}$. Let the closed substitution ρ be defined by

$$\rho(z) = a^{\ulcorner z \urcorner \cdot n} b\mathbf{0} \quad \text{for all } z \in V.$$

   $t \precsim u$ implies $\rho(t) \precsim \rho(u)$. Since $\rho(t) \xrightarrow{a} \rho(t')$, there is a $j_0 \in J$ such that $\rho(u_{j_0}) \xrightarrow{a} p$ with $\rho(t') \precsim p$.

   The term u_{j_0} cannot be a variable. Namely, in that case we would have $p = a^{\ulcorner u_{j_0} \urcorner \cdot n - 1} b\mathbf{0}$. On the other hand, $K \neq \emptyset$ implies that $\rho(t') \xrightarrow{a^{\ulcorner y_k \urcorner \cdot n} b} \mathbf{0}$ for some $k \in K$. Since $a \neq b$ and $n > 1$, this would clearly contradict $\rho(t') \precsim p$. So it follows that $u_{j_0} = au'$ for some term u' with $p = \rho(u')$.

   Consider a trace $t' \xrightarrow{b_1 \cdots b_m} z + t''$ for some $0 \leq m < n$, variable z and term t''. We will now prove that there exists a trace $u' \xrightarrow{b_1 \cdots b_m} z + u''$. Since $\rho(t') \precsim \rho(u')$, there is a trace $\rho(u') \xrightarrow{b_1 \cdots b_m} p'$ with $\rho(z + t'') \precsim p'$. Assume, towards a contradiction, that $u' \xrightarrow{b_1 \cdots b_\ell} y + u_1$ and $\rho(y) \xrightarrow{b_{\ell+1} \cdots b_m} p'$ for some $0 \leq \ell < m$, variable y and term u_1. Since $\rho(y) = a^{\ulcorner y \urcorner \cdot n} b\mathbf{0}$, $0 < m - \ell < n$, and $a \neq b$, it follows that p' cannot simulate the trace $\rho(z + t'') \xrightarrow{a^{\ulcorner z \urcorner \cdot n} b} \mathbf{0}$. This contradicts $\rho(z + t'') \precsim p'$. Hence, since $\rho(u') \xrightarrow{b_1 \cdots b_m} p'$, we have $u' \xrightarrow{b_1 \cdots b_m} u_2$ for some term u_2 with $\rho(u_2) = p'$. By the second proviso of this lemma, $depth(u_2) < n$. Since moreover $\rho(u_2)$ can simulate $\rho(z + t'') \xrightarrow{a^{\ulcorner z \urcorner \cdot n} b} \mathbf{0}$, it follows from the definition of ρ that $u_2 = z + u''$ for some term u''. Concluding, $t' \xrightarrow{b_1 \cdots b_m} z + t''$ implies $u' \xrightarrow{b_1 \cdots b_m} z + u''$.

   Now consider any $b_1 \cdots b_n \in A^n$. Since $\Psi_n \precsim \sigma(t')$ and (by the second proviso of this lemma together with Lemma 1(2)) $depth(t') < n$, we have $t' \xrightarrow{b_1 \cdots b_m} z + t''$ and $\sigma(z) \xrightarrow{b_{m+1} \cdots b_n}$ for some $0 \leq m < n$, variable z and term t''. We proved above that $t' \xrightarrow{b_1 \cdots b_m} z + t''$ implies $u' \xrightarrow{b_1 \cdots b_m} z + u''$ for some term u''. Since $\sigma(z) \xrightarrow{b_{m+1} \cdots b_n}$, this yields $\sigma(u') \xrightarrow{b_1 \cdots b_n}$. This holds for all $b_1 \cdots b_n \in A^n$, so $\Psi_n \precsim \sigma(u')$.

   Furthermore, recall that y_{k_0} is a summand of t', and that x is a summand of $\sigma(y_{k_0})$. Since $t' \xrightarrow{\lambda} t'$ (where λ denotes the empty trace), we proved above that $u' \xrightarrow{\lambda} y_{k_0} + u''$ for some term u''. So y_{k_0} is a summand of u'. Hence x is a summand of $\sigma(u')$.

   Concluding, $x + \Psi_n \precsim \sigma(u')$, so $a(x + \Psi_n) \precsim a\sigma(u')$. By the fourth proviso of this lemma, $a\sigma(u') \precsim \sigma(u) \precsim \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$. So by Lemma 2, $a\sigma(u') \simeq a(x + \Psi_n)$. □

The following lemma paves the way for the proof of Proposition 1.

Lemma 4. *Let E be a finite axiomatization that is sound modulo $\precsim$. Assume that:*

- $E \vdash v \preccurlyeq w$;
- $n > 1$ *is greater than or equal to the depth of any term in* E;
- v *has a summand similar to* $a(x + \Psi_n)$; *and*
- $w \precsim \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$;

Then w *has a summand similar to* $a(x + \Psi_n)$.

Proof. By induction on the depth of the proof of the inequation $v \preccurlyeq w$ from E. We proceed by a case analysis on the last rule used in the derivation of $v \preccurlyeq w$ from E. The case of reflexivity is trivial. Below we consider the other possibilities.

- Case $E \vdash v \preccurlyeq w$ because $\sigma(t) = v$ and $\sigma(u) = w$ for some $t \preccurlyeq u \in E$ and substitution σ. The claim follows by Lemma 3.
- Case $E \vdash v \preccurlyeq w$ because $E \vdash v \preccurlyeq t$ and $E \vdash t \preccurlyeq w$ for some term t. By the soundness of E, $t \precsim w \precsim \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$, so by induction, t has a summand similar to $a(x+\Psi_n)$. Hence, again by induction, w has a summand similar to $a(x + \Psi_n)$.
- Case $E \vdash v \preccurlyeq w$ because $v = v' + v''$ and $w = w' + w''$ with $E \vdash v' \preccurlyeq w'$ and $E \vdash v'' \preccurlyeq w''$. Since v has a summand similar to $a(x + \Psi_n)$, so does either v' or v''. Assume, without loss of generality, that v' has a summand similar to $a(x + \Psi_n)$. Since $w' \precsim w \precsim \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$, by induction, w' has a summand similar to $a(x + \Psi_n)$.
- Case $E \vdash v \preccurlyeq w$ because $v = av'$ and $w = aw'$ with $E \vdash v' \preccurlyeq w'$. Then $av' \simeq a(x + \Psi_n)$. Since $aw' \precsim \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$, by Lemma 2, $aw' \simeq a(x + \Psi_n)$. □

Now we are in a position to prove **Proposition 1**.

Proof. Let E be a finite axiomatization over BCCSP(A) that is sound modulo $\precsim$. Let $n > 1$ be greater than or equal to the depth of any term in E.

$\sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$ does not contain a summand similar to $a(x + \Psi_n)$. So according to Lemma 4, the inequation $a(x + \Psi_n) \preccurlyeq \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$, which is sound modulo $\precsim$, cannot be derived from E. □

Theorem 1. *The inequational theory of* BCCSP(A) *modulo* $\precsim$ *is not finitely based.*

Proof. By Proposition 1, no finite axiomatization over BCCSP(A) that is sound modulo $\precsim$ proves all inequations that are sound modulo $\precsim$. □

3.2 Simulation Equivalence

Following the same line as in Section 3.1, we can prove that the equational theory of BCCSP(A) modulo $\simeq$ does not have a finite basis. The following lemma is the counterpart of Lemma 4 for simulation equivalence.

Lemma 5. *Let* E *be a finite axiomatization that is sound modulo* $\simeq$. *Assume that:*

– $E \vdash v \approx w$;
– $n > 1$ *is greater than or equal to the depth of any term in* E;
– v *has a summand similar to* $a(x + \Psi_n)$; *and*
– $w \simeq \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$;

Then w *has a summand similar to* $a(x + \Psi_n)$.

Proof. Note that Lemma 3 remains true if all occurrences of $\precsim$ are replaced with $\simeq$, owing to the fact that the relation $\simeq$ is included in $\precsim$.

By postulating that for each axiom $t \approx u$ in E also its symmetric counterpart $t \approx u$ is present, one may assume, without loss of generality, that applications of symmetry happen first in equational derivations.

Now the proof proceeds by a case analysis on the last rule used in the derivation of $v \approx w$ from E, similar to the proof of Lemma 4. This case analysis is omitted here. □

Proposition 2. *Let* E *be a finite axiomatization over* BCCSP(A) *that is sound modulo* $\simeq$. *Let* $n > 1$ *be greater than or equal to the depth of any term in* E. *Then from* E *we cannot derive the equation*

$$a(x + \Psi_n) + \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n \approx \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$$

Proof. $\sum_{\theta \in A^n} a(x+\Psi_n^\theta)+a\Phi_n$ does not contain a summand similar to $a(x+\Psi_n)$. So according to Lemma 5, the equation $a(x + \Psi_n) + \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n \approx \sum_{\theta \in A^n} a(x+\Psi_n^\theta)+a\Phi_n$, which is sound modulo $\simeq$, cannot be derived from E. □

Theorem 2. *The equational theory of* BCCSP(A) *modulo* $\simeq$ *is not finitely based.*

Proof. By Proposition 2, no finite axiomatization over BCCSP(A) that is sound modulo $\simeq$ proves all equations that are sound modulo $\simeq$. □

4 Simulation Equivalence with $|A| = \infty$

In [9], van Glabbeek gave a finite axiomatization that is sound and ground-complete for BCCSP(A) modulo $\simeq$. It consists of axioms A1-4 (see Section 2) together with

$$\text{S} \qquad a(x + y) \approx a(x + y) + ax$$

Likewise, a finite sound and ground-complete axiomatization for BCCSP(A) modulo $\precsim$ is obtained by adding $x \preccurlyeq x + y$ to A1-4.

It was stated in [9, p78] and in [2, p355] that if A is infinite, then the axiomatization A1-4 + S is ω-complete. In both articles it was claimed that this could be proved using the technique of inverted substitutions from Groote [10], but the proof itself was never given.

For the sake of completeness, here we present a proof that A1-4 + S is ω-complete, using inverted substitutions. This technique works as follows. Consider

an axiomatization E. For each equation $t \approx u$ of which all closed instances can be derived from E, one must define a closed substitution ρ and a mapping $R : \mathrm{T}(\mathrm{BCCSP}) \to \mathbb{T}(\mathrm{BCCSP})$ such that:

(1) $E \vdash R(\rho(t)) \approx t$ and $E \vdash R(\rho(u)) \approx u$;

(2) for each function symbol f (with arity n), $E \cup \{p_i \approx q_i,\ R(p_i) \approx R(q_i) \mid i = 1, \ldots, n\} \vdash R(f(p_1, \ldots, p_n)) \approx R(f(q_1, \ldots, q_n))$ for all closed terms $p_1, \ldots, p_n, q_1, \ldots, q_n$; and

(3) $E \vdash R(\sigma(v)) \approx R(\sigma(w))$ for each $v \approx w \in E$ and closed substitution σ.

Then, as proved in [10], E is ω-complete.

Theorem 3. *If $|A| = \infty$, then A1-4+S is ω-complete.*

Proof. Consider terms t and u. Define $\rho : V \to \mathrm{T}(\mathrm{BCCSP})$ by $\rho(x) = a_x\mathbf{0}$, where a_x is a unique action for $x \in V$ that occurs in neither t nor u. Such actions exist because A is infinite. We define $R : \mathrm{T}(\mathrm{BCCSP}) \to \mathbb{T}(\mathrm{BCCSP})$ as follows:

$$\begin{cases} R(\mathbf{0}) & = \mathbf{0} \\ R(ap) & = aR(p) \text{ if } a \neq a_x \text{ for all } x \in V \\ R(a_x p) & = x \\ R(p_1 + p_2) & = R(p_1) + R(p_2) \end{cases}$$

We now check the three properties from [10]:

(1) Since t and u do not contain actions of the form a_x, clearly $R(\rho(t)) = t$ and $R(\rho(u)) = u$.

(2) Consider the operator $\_ + \_$. From $R(p_1) \approx R(q_1)$ and $R(p_2) \approx R(q_2)$ we derive $R(p_1 + p_2) = R(p_1) + R(p_2) \approx R(q_1) + R(q_2) = R(q_1 + q_2)$.
Consider the prefix operator $a\_$. We distinguish two cases.
- $a \neq a_y$ for all $y \in V$. Then from $R(p_1) \approx R(q_1)$ we derive $R(ap_1) = aR(p_1) \approx aR(q_1) = R(aq_1)$.
- $a = a_y$ for some $y \in V$. Then $R(a_y p_1) = y = R(a_y q_1)$.

(3) For A1-4, the proof is trivial. We check the remaining case S. Let σ be a closed substitution. We consider two cases.
- $a = a_z$ for some $z \in V$. Then

$$\begin{aligned} R(a(\sigma(x) + \sigma(y))) &= z \\ &\approx z + z \\ &= R(a_z(\sigma(x) + \sigma(y))) + R(a_z\sigma(x)) \end{aligned}$$

- $a \neq a_z$ for all $z \in V$. Then

$$\begin{aligned} R(a(\sigma(x) + \sigma(y))) &= a(R(\sigma(x)) + R(\sigma(y))) \\ &\approx a(R(\sigma(x)) + R(\sigma(y))) + aR(\sigma(x)) \\ &= R(a(\sigma(x) + \sigma(y)) + a\sigma(x)) \end{aligned}$$

This completes the proof. □

Acknowledgement. We thank Bas Luttik for his constructive comments.

References

1. L. Aceto, W. Fokkink, R. van Glabbeek, and A. Ingolfsdottir. Nested semantics over finite trees are equationally hard. *Information and Computation*, 191(2):203–232, 2004.
2. L. Aceto, W. Fokkink, A. Ingolfsdottir and B. Luttik. Finite equational bases in process algebra: Results and open questions. In *Processes, Terms and Cycles: Steps on the Road to Infinity, Essays Dedicated to Jan Willem Klop, on the Occasion of his 60th Birthday*, Amsterdam, LNCS 3838, pp. 338–367. Springer 2005.
3. L. Aceto, W. Fokkink, A. Ingolfsdottir and B. Luttik. A finite equational base for CCS with left merge and communication merge. In *Proceedings 33rd Colloquium on Automata, Languages and Programming (ICALP'06)*, Venice, LNCS. Springer, 2006. To appear.
4. S. Blom, W. Fokkink, and S. Nain. On the axiomatizability of ready traces, ready simulation and failure traces. In *Proceedings 30th Colloquium on Automata, Languages and Programming (ICALP'03)*, Eindhoven, LNCS 2719, pp. 109–118. Springer, 2003.
5. T. Chen, W. Fokkink, and S. Nain. On finite alphabets and infinite bases II: Completed and ready simulation. In *Proceedings 9th Conference on Foundations of Software Science and Computation Structures (FOSSACS'06)*, Vienna, LNCS 3921, pp. 1–15. Springer, 2006.
6. W. Fokkink and B. Luttik. An ω-complete equational specification of interleaving. In *Proceedings 27th Colloquium on Automata, Languages and Programming (ICALP'00)*, Geneva, LNCS 1853, pp. 729–743. Springer, 2000.
7. W. Fokkink and S. Nain. On finite alphabets and infinite bases: From ready pairs to possible worlds. In *Proceedings 7th Conference on Foundations of Software Science and Computation Structures (FOSSACS'04)*, Barcelona, LNCS 2987, pp. 182–194. Springer, 2004.
8. W. Fokkink and S. Nain. A finite basis for failure semantics. In *Proceedings 32nd Colloquium on Automata, Languages and Programming (ICALP'05)*, Lisbon, LNCS 3580, pp. 755–765. Springer, 2005.
9. R. van Glabbeek. The linear time – branching time spectrum I. The semantics of concrete, sequential processes. In J.A. Bergstra, A. Ponse, and S.A. Smolka, eds, *Handbook of Process Algebra*, pp. 3–99. Elsevier, 2001.
10. J.F. Groote. A new strategy for proving ω-completeness with applications in process algebra. In *Proceedings 1st Conference on Concurrency Theory (CONCUR'90)*, Amsterdam, LNCS 458, pp. 314–331. Springer, 1990.
11. R. Gurevič. Equational theory of positive natural numbers with exponentiation is not finitely axiomatizable. *Annals of Pure and Applied Logic*, 49:1–30, 1990.
12. J. Heering. Partial evaluation and ω-completeness of algebraic specifications. *Theoretical Computer Science*, 43:149–167, 1986.
13. L. Henkin. The logic of equality. *American Mathematical Monthly*, 84(8):597–612, 1977.
14. P. Jancar, A. Kucera, and F. Moller. Simulation and bisimulation over one-counter processes. In *Proceedings 17th Symposium on Theoretical Aspects of Computer Science (STACS'2000)*, Lille, LNCS 1770, pp. 334–345. Springer, 2000.
15. H. Lin. PAM: A process algebra manipulator. *Formal Methods in System Design*, 7(3):243–259, 1995.
16. A. Lazrek, P. Lescanne, and J.-J. Thiel. Tools for proving inductive equalities, relative completeness, and ω-completeness. *Information and Computation*, 84(1):47–70, 1990.

17. N. Lynch and M. Tuttle. An introduction to input/output automata. *CWI Quarterly*, 2(3):219–246, 1989.
18. R. Lyndon. Identities in two-valued calculi. *Transactions of the American Mathematical Society*, 71:457–465, 1951.
19. R. McKenzie. Tarski's finite basis problem is undecidable. *Journal of Algebra and Computation*, 6(1):49–104, 1996.
20. R. McKenzie, G. McNulty, and W. Taylor. *Algebras, Varieties, Lattices*. Wadsworth & Brooks/Cole, 1987.
21. R. Milner. *A Calculus of Communicating Systems*. LNCS 92. Springer, 1980.
22. R. Milner. *Communication and Concurrency*. Prentice Hall, 1989.
23. F. Moller. *Axioms for Concurrency*. PhD thesis, University of Edinburgh, 1989.
24. F. Moller. The importance of the left merge operator in process algebras. In *Proceedings 17th Colloquium on Automata, Languages and Programming (ICALP'90)*, Warwick, LNCS 443, pp. 752–764. Springer, 1990.
25. V.L. Murskiĭ. The existence in the three-valued logic of a closed class with a finite basis having no finite complete system of identities. *Doklady Akademii Nauk SSSR*, 163:815–818, 1965. In Russian.
26. V.L. Murskiĭ. The existence of a finite basis of identities, and other properties of "almost all" finite algebras. *Problemy Kibernetiki*, 30:43–56, 1975. In Russian.
27. D.M.R. Park. Concurrency and automata on infinite sequences. In *Proceedings 5th GI Conference*, Karlsruhe, LNCS 104, pp. 167–183. Springer, 1981.
28. G.D. Plotkin. The λ-calculus is ω-incomplete. *Journal of Symbolic Logic*, 39(2):313–317, 1974.