On Finite Alphabets and Infinite Bases: From Ready Pairs to Possible Worlds

Wan Fokkink[1,2] and Sumit Nain[3]

[1] CWI, Department of Software Engineering, PO Box 94079, 1090 GB Amsterdam,
The Netherlands, wan@cwi.nl
[2] Vrije Universiteit Amsterdam, Department of Theoretical Computer Science,
De Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands, wanf@cs.vu.nl
[3] IIT Delhi, Department of Computer Science and Engineering, Hauz Khas,
New Delhi-110 016, India, nain@cse.iitd.ernet.in

Abstract. We prove that if a finite alphabet of actions contains at least two elements, then the equational theory for the process algebra BCCSP modulo any semantics no coarser than readiness equivalence and no finer than possible worlds equivalence does not have a finite basis. This semantic range includes ready trace equivalence.

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 [8] presented the linear time - branching time spectrum of behavioral equivalences for finitely branching, concrete, sequential processes. In this paper we focus on three equivalence relations in this spectrum. *Readiness semantics* [22,27] distinguishes a process by its finite traces, where each finite trace is decorated with the set of initial actions at its ultimate state. In *ready trace semantics* [4,26], each finite trace is decorated with the set of initial actions at all its states. *Possible worlds semantics* [28] distinguishes a process by the deterministic processes that can be "ready simulated" by the original process. In a *ready simulation*, the sets of initial actions at a simulated and its simulating state must always be the same. Readiness semantics is coarser than ready trace semantics (meaning that it distinguishes fewer processes), which in turn is coarser than possible worlds semantics. Other semantics in the spectrum are based on (bi)simulation, failures, failure traces, and (completed) 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.

I. Walukiewicz (Ed.): FOSSACS 2004, LNCS 2987, pp. 182–194, 2004.

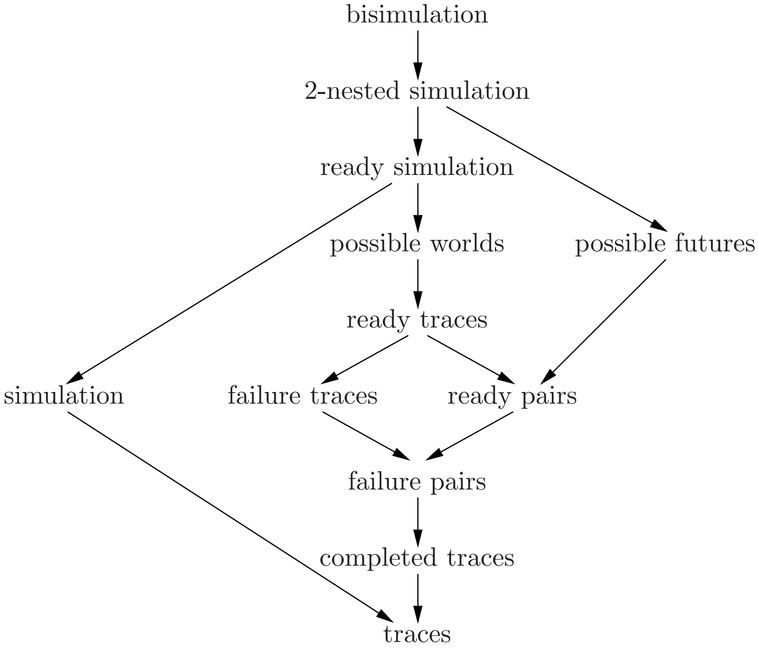

Fig. 1. The linear time - branching time spectrum

Van Glabbeek [8] studied the semantics in his spectrum in the setting of the process algebra BCCSP, which contains only basic process algebraic operators from CCS and CSP, but is sufficiently powerful to express all finite synchronization trees. Van Glabbeek gave (sound and complete) axiomatizations for semantics in the spectrum, meaning that two closed BCCSP terms can be equated if and only if they are equivalent.

An axiomatization E is *ω-complete* when an equation can be derived from E if (and only if) all its closed instantiations can be derived from E. In applications dealing with theorem proving, ω-completeness of the underlying equational theory often facilitates the production of equational derivations; see [13]. In [11] it was argued that ω-completeness is desirable for the partial evaluation of programs.

In universal algebra, ω-completeness is referred to as a *basis* for the equational theory. The existence of finite bases for algebras is a classic topic of study in universal algebra (see, e.g., [16]), dating back to Lyndon [14]. Murskiĭ [21] proved that "almost all" finite algebras (namely all quasi-primal ones) are finitely based, while in [20] he presented an example of a three-element algebra that has no finite basis. Henkin [12] showed that the algebra of naturals with addition and multiplication is finitely based, while Gurevič [10] showed that after adding exponentiation the algebra is no longer finitely based. McKenzie [15] settled Tarski's Finite Basis Problem in the negative, by showing that the general question whether a finite algebra is finitely based is undecidable.

Other notable examples of ω-incomplete axiomatizations in the literature are the $\lambda K\beta\eta$-calculus (see [25]) and the equational theory of CCS [17]. 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 [19] and ACP [6]. Another negative result, for basic process algebra with the binary Kleene star, was reported in [2]: semantics no coarser than completed trace equivalence and no finer than ready simulation equivalence have no finite (sound and complete) axiomatization, so by default no finite ω-complete axiomatization.

A number of positive and negative results regarding finite ω-complete axiomatizations for BCCSP occur in the literature. Moller [19] proved that the finite axiomatization for BCCSP modulo bisimulation equivalence is ω-complete. Groote [9] presented a similar result for completed trace equivalence, for trace equivalence (in case of an alphabet with more than one element), and for readiness and failures equivalence (in case of an infinite alphabet). Blom, Fokkink and Nain [5] proved that in case of an infinite alphabet, BCCSP modulo ready trace equivalence does not have a finite (sound and complete) axiomatization. Aceto, Fokkink and Ingólfsdóttir [3] proved a similar negative result for 2-nested simulation equivalence, independent of the cardinality of the alphabet.[1]

Groote [9] explicitly left open the question of ω-complete axiomatizations for BCCSP modulo readiness and ready trace equivalence in case of a *finite* (non-empty) alphabet. The same question for possible worlds equivalence, irrespective of the cardinality of the alphabet, was posed by van Glabbeek [8].

In case of a *singleton* alphabet, readiness, ready trace and possible worlds equivalence coincide with completed trace equivalence. As mentioned before, there exists a finite ω-complete axiomatization for BCCSP modulo completed trace equivalence, independent of the cardinality of the alphabet.

In this paper we consider BCCSP with a finite alphabet *with more than one element.* We prove for any semantics $\sim$ no coarser than readiness equivalence and no finer than possible worlds equivalence, that there is *no* finite ω-complete axiomatization for BCCSP modulo $\sim$. Ready trace semantics is included in this range (see Figure 1).

The proof of the main theorem of this paper only concerns equations of depth one. Pivotal for this proof is a special kind of "cover equation" (see Definition 3), from which all sound equations of depth one for BCCSP modulo readiness equivalence can be derived. For the soundness of the cover equations, modulo possible worlds semantics, it is essential that the alphabet is finite. Thus we not only obtain a negative result, but we gain some insight into the equational theory of readiness, ready trace and possible worlds semantics in the presence of a finite alphabet.

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

Finally, we prove that if the alphabet is infinite, then the (sound and complete) axiomatization for possible worlds semantics is ω-complete. So there is a striking incompatibility of a finite alphabet and a finite basis. Namely, in case of an infinite alphabet BCCSP modulo readiness semantics or possible worlds semantics has a finite basis, while in case of a finite alphabet it only has an infinite basis.

Groote [9] also asked whether in case of a finite alphabet, BCCSP modulo failures or failure trace semantics has a finite ω-complete axiomatization. These questions remain open, for alphabets with more than one element. We note that the aforementioned cover equations can be derived from the standard axioms for failures semantics and failure trace equivalence. So there is hope that finite ω-complete axiomatizations for these semantics do exist.

2 Preliminaries

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*. Open terms t, u can moreover contain variables from a countably infinite set V (with typical elements w, x, y, z). As binding convention, alternative composition and summation bind weaker than prefixing. 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 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 [24], by the transition rules below, which give rise to A-labeled transitions between closed terms.

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

The *depth* of a term t, denoted by $\mathit{depth}(t)$, is the maximal number of transitions in sequence that t can exhibit. It is defined by: $\mathit{depth}(\mathbf{0}) = 0$, $\mathit{depth}(x) = 0$, $\mathit{depth}(t + u) = \max\{\mathit{depth}(t), \mathit{depth}(u)\}$, and $\mathit{depth}(at) = \mathit{depth}(t) + 1$.

For a closed term p, $\mathcal{I}(p)$ denotes the set of actions a for which there exists a transition $p \xrightarrow{a} p'$. A closed term p is *deterministic* if for each $a \in \mathcal{I}(p)$ there is exactly one closed term p' such that $p \xrightarrow{a} p'$, and moreover p' is deterministic.

Definition 1. *A closed term p_1 is a* possible world *of a closed term p_0 if $\mathcal{I}(p_1) = \mathcal{I}(p_0)$, p_1 is deterministic, and for each transition $p_1 \xrightarrow{a} p_1'$ there is a transition $p_0 \xrightarrow{a} p_0'$ such that p_1' is a possible world of p_0'. Two closed terms p and q are* possible worlds equivalent, *denoted by $p \sim_{\mathrm{PW}} q$, if they have exactly the same possible worlds.*

Definition 2. *A pair* $(a_1 \cdots a_k, B)$ *with* $B \subseteq A$ *and* $k \geq 0$ *is a* ready pair *of* p_0 *if* $p_0 \xrightarrow{a_1} p_1 \cdots \xrightarrow{a_k} p_k$ *with* $\mathcal{I}(p_k) = B$. *Two closed terms* p *and* q *are* readiness equivalent, *denoted by* $p \sim_{\mathrm{R}} q$, *if they have exactly the same ready pairs.*

Axiomatization. An *(equational) axiomatization* E for BCCSP(A) is a collection of equations $t \approx u$. We write $E \vdash t \approx u$ if this equation can be derived from the equations in E using the standard rules of equational logic, and $E \vdash F$ if $E \vdash t \approx u$ for all $t \approx u \in F$. An axiomatization E is *sound* modulo an equivalence $\sim$ on closed terms if $(E \vdash p \approx q) \Rightarrow p \sim q$, and it is *complete* modulo $\sim$ if $p \sim q \Rightarrow (E \vdash p \approx q)$, for all closed terms p and q. An axiomatization E is ω*-complete* if for each equation $t \approx u$ with $E \vdash \sigma(t) \approx \sigma(u)$ for all closed substitutions σ, we have $E \vdash t \approx u$.

The core axioms A1-4 [17] for BCCSP(A) below are sound and complete modulo bisimulation equivalence [23], which is the finest semantics in van Glabbeek's 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 A1-2. A term x or at is a *summand* of each term $x + u$ or $at + u$, respectively. We use *summation* $\sum_{i=1}^{k} t_i$ or $\sum_{i \in \{1,\dots,k\}} t_i$, with $k \geq 0$, to denote $t_1 + \cdots + t_k$, where the empty sum denotes $\mathbf{0}$.

Lemma 1. *If* $t \approx u$ *is sound modulo* $\sim_{\mathrm{R}}$, *then* t *and* u *have the same depth.*

Proof. Let σ map each variable in V to $\mathbf{0}$. Since $\sigma(t) \sim_{\mathrm{R}} \sigma(u)$, clearly $\sigma(t)$ and $\sigma(u)$ have the same depth. So $depth(t) = depth(\sigma(t)) = depth(\sigma(u)) = depth(u)$. □

3 On Finite Alphabets and Infinite Bases

In this section, we assume that $1 < |A| < \infty$.

Let $\sim$ denote a semantics no coarser than readiness semantics and no finer than possible worlds semantics. We prove that no finite sound and complete axiomatization for BCCSP(A) modulo $\sim$ is ω-complete.

3.1 How the Proof Was Construed

To prove the result mentioned above, we started out with the following infinite family of equations e_n for $n > |A|$:

$$\begin{aligned}
&a(x_1 + \cdots + x_n) + \textstyle\sum_{i=1}^{n} a(x_1 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_n) \\
\approx\ &\textstyle\sum_{i=1}^{n} a(x_1 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_n).
\end{aligned}$$

These equations are sound modulo $\sim_{\mathrm{PW}}$. Namely, it is not hard to see that for each closed substitution σ, the possible worlds of the summand $\sigma(a(x_1+\cdots+x_n))$ at the left-hand side of $\sigma(e_n)$ are included in the possible worlds of the right-hand side of $\sigma(e_n)$.

However, our expectation that the equations e_n for $n > |A|$ would obstruct a finite ω-complete axiomatization turned out to be false. Namely, e_n can be obtained by (1) applying to e_{n-1} a substitution σ with $\sigma(x_i) = x_i + x_n$ for $i = 1, \ldots, n-1$, and (2) adding the summand $a(x_1 + \cdots + x_{n-1})$ at the left- and right-hand side of the resulting equation. Hence, from $e_{|A|+1}$ (together with A1-3) we can derive the e_n for $n > |A|$.

Therefore we moved to a more complicated family of equations (see Definition 7), similar in spirit to the equations e_n. However, while cancellation of the summand $a(x_1 + \cdots + x_{n-1})$ from e_n for $n > |A| + 1$ leads to an equation that is again sound modulo $\sim_{\mathrm{PW}}$, such a cancellation is not possible for the new family of equations (see Proposition 3). We prove that they do obstruct a finite ω-complete axiomatization (see Corollary 1).

3.2 Cover Equations

We introduce the class of *cover equations* (see Definition 3), and show that they are sound modulo $\sim_{\mathrm{PW}}$. We prove that each equation that involves terms of depth ≤ 1 and that is sound modulo $\sim_{\mathrm{R}}$ can be derived from the cover equations. Moreover, if such an equation contains no more than k summands at its left- and right-hand side, then it can be derived from cover equations containing no more than k summands at their left- and right-hand sides (see Theorem 1).

In the remainder of this section, terms are considered not only modulo A1,2, but also modulo A3,4. By abuse of notation, we let a finite set $X \subset V$ denote the term $\sum_{x \in X} x$. From now on, X, Y, Z (possibly subscripted) denote finite subsets of V.

Definition 3. *A term $\sum_{i\in I} aY_i$ is a* cover *of aX if:*

1. *$\forall Z \subseteq X$ with $|Z| < |A|$, $\exists i{\in}I\ (Z \subseteq Y_i \subseteq X)$; and*
2. *$\forall Z \subseteq X$ with $|Z| = |A|$, $\exists i{\in}I\ (Z \subseteq Y_i)$.*

This is denoted by $\sum_{i\in I} aY_i \trianglerighteq aX$. We say that $aX + \sum_{i\in I} aY_i \approx \sum_{i\in I} aY_i$ is a cover equation*.*

Example 1. $\sum_{i=1}^{n} a(x_1 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_n) \trianglerighteq a(x_1 + \cdots + x_n)$ for $n > |A|$. Hence the equations in Section 3.1 are cover equations.

If $|X| < |A|$, then by Definition 3.1, $t \trianglerighteq aX$ implies that aX is a summand of t. So the only interesting cover equations are the ones where $|X| \geq |A|$ (cf. Definition 7).

We proceed to prove that the cover equations are sound modulo $\sim_{\mathrm{PW}}$.

Proposition 1. *If $t \trianglerighteq aX$, then $aX + t \approx t$ is sound modulo $\sim_{\mathrm{PW}}$.*

Proof. Let σ be an arbitrary closed substitution. It suffices to show that the possible worlds of $\sigma(aX)$ are also possible worlds of $\sigma(t)$. Let $t = \sum_{i\in I} aY_i$, and let ap be a possible world of $\sigma(aX)$. Then p is a possible world of $\sigma(X)$. So by Definition 1: $\mathcal{I}(p) = \mathcal{I}(\sigma(X))$; p has exactly $|\mathcal{I}(\sigma(X))|$ summands, one summand bp_b for each $b \in \mathcal{I}(\sigma(X))$; and for each $b \in \mathcal{I}(\sigma(X))$ there is an $x_b \in X$ such that $\sigma(x_b) \xrightarrow{b} q_b$ and p_b is a possible world of q_b. Let $Z = \{x_b \mid b \in \mathcal{I}(\sigma(X))\}$. Then $\mathcal{I}(\sigma(Z)) = \mathcal{I}(\sigma(X))$. Clearly p is a possible world of $\sigma(Z)$. Note that $|Z| \leq |\mathcal{I}(\sigma(X))|$. We consider two cases.

1. $|\mathcal{I}(\sigma(X))| < |A|$.
   By Definition 3.1, $Z \subseteq Y_i \subseteq X$ for some $i \in I$. Then $\mathcal{I}(\sigma(Y_i)) = \mathcal{I}(\sigma(X))$, so p is a possible world of $\sigma(Y_i)$. Thus ap is a possible world of $\sigma(t)$.
2. $|\mathcal{I}(\sigma(X))| = |A|$.
   By Definition 3, $Z \subseteq Y_i$ for some $i \in I$. Then $\mathcal{I}(\sigma(Y_i)) = A = \mathcal{I}(\sigma(X))$, so p is a possible world of $\sigma(Y_i)$. Thus ap is a possible world of $\sigma(t)$.

Concluding, the possible worlds of $\sigma(aX)$ are also possible worlds of $\sigma(t)$. □

We proceed to prove that each sound equation $t \approx u$ modulo $\sim_{\mathrm{R}}$ where t and u have depth 1 and contain no more than k summands, can be derived from the cover equations with $|I| \leq k$ (see Theorem 1). First we present some notations.

Definition 4. *$C^k = \{aX + \sum_{i\in I} aY_i \approx \sum_{i\in I} aY_i \mid \sum_{i\in I} aY_i \trianglerighteq aX \wedge |I| \leq k\}$ for $k \geq 0$.*

Definition 5. *R_1 denotes the set of equations $t \approx u$ with $depth(t) = depth(u) \leq 1$ that are sound modulo $\sim_{\mathrm{R}}$.*

Notation. $S(t)$ denotes the number of distinct summands of term t.

Definition 6. *$R_1^k = \{t \approx u \in R_1 \mid S(t) \leq k \wedge S(u) \leq k\}$ for $k \geq 0$.*

Notation. $A = \{a_1, \ldots, a_{|A|}\}$.

We present part of the proof of Theorem 1 as a separate lemma, as this lemma will be re-used in the proof of Proposition 4.

Lemma 2. *If $t \approx u \in R_1$, then t and u contain exactly the same summands $x \in V$ and aX with $|X| < |A|$.*

Proof. Let $x \in V$ be a summand of t. We define $\sigma(x) = a_1a_1\mathbf{0}$ and $\sigma(y) = \mathbf{0}$ for $y \neq x$. Then $(a_1a_1, \emptyset)$ is a ready pair of $\sigma(t)$, so it must be a ready pair of $\sigma(u)$. Since $depth(u) \leq 1$, this implies that x is a summand of u.

Let aX be a summand of t where $X = \{x_1, \ldots, x_k\}$ with $k < |A|$. We define $\sigma(x_i) = a_i\mathbf{0}$ for $i = 1, \ldots, k$ and $\sigma(y) = a_{k+1}\mathbf{0}$ for $y \notin X$. Then $(a, \{a_1, \ldots, a_k\})$ is a ready pair of $\sigma(t)$, so it must be a ready pair of $\sigma(u)$. Since $depth(u) \leq 1$, this implies that aX is a summand of u.

By symmetry, each summand $x \in V$ and aX with $|X| < |A|$ of u is also a summand of t. □

Theorem 1. *$C^k \vdash R_1^k$ for $k \geq 0$.*

Proof. Let $t \approx u \in R_1^k$. Consider a summand aX of t with $|X| \geq |A|$. We prove that a subset of the summands of u form a cover of aX.

1. Let $Z = \{z_1, \ldots, z_k\} \subseteq X$ with $k < |A|$.
   We define $\sigma(z_i) = a_i\mathbf{0}$ for $i = 1, \ldots, k$, $\sigma(x) = \mathbf{0}$ for $x \in X \backslash Z$ and $\sigma(y) = a_{|A|}\mathbf{0}$ for $y \notin X$. The ready pairs of $\sigma(aX)$ must also be ready pairs of $\sigma(u)$. Since $depth(u) \leq 1$, this implies that there is a summand aY of u with $Z \subseteq Y \subseteq X$.
2. Let $Z = \{z_1, \ldots, z_{|A|}\} \subseteq X$.
   We define $\sigma(z_i) = a_i\mathbf{0}$ for $i = 1, \ldots, |A|$ and $\sigma(y) = \mathbf{0}$ for $y \notin Z$. The ready pairs of $\sigma(aX)$ must also be ready pairs of $\sigma(u)$. Since $depth(u) \leq 1$, this implies that there is a summand aY of u with $Z \subseteq Y$.

Concluding, in view of Definition 3, $u = u' + u''$ with $u' \trianglerighteq aX$. Since $S(u') \leq S(u) \leq k$, we have $aX + u' \approx u' \in C^k$. So $C^k \vdash aX + u \approx u$.

By Lemma 2, each summand $x \in V$ and aX with $|X| < |A|$ of t is a summand of u. Moreover, $C^k \vdash aX + u \approx u$ for each summand aX of t with $|X| \geq |A|$. Hence, $C^k \vdash t + u \approx u$.

By symmetry, also $C^k \vdash t + u \approx t$. So $C^k \vdash t \approx t + u \approx u$. □

3.3 Cover Equations $a_1X_n + t_n \approx t_n$ for $n \geq |A|$

We now turn our attention to a special kind of cover equation $a_1X_n + t_n \approx t_n$ for $n \geq |A|$, where t_n contains $n+1$ summands (see Definition 7 and Proposition 2). If a term u is obtained by eliminating one or more summands from t_n, then $a_1X_n + u \approx u$ is not sound modulo $\sim_R$ (see Proposition 3); moreover, if a summand of a term v is not a summand of $a_1X_n + t_n$, then $t_n \approx v$ is not sound modulo $\sim_R$ (see Proposition 4). These two facts together imply that $a_1X_n + t_n \approx t_n$ cannot be derived from C^n (see Theorem 2). Theorems 1 and 2 form the corner stones of the proof of Corollary 1, which contains the main result of this paper.

Definition 7. *Let $n \geq |A|$. Let $x_1, \ldots, x_n, w_{|A|}, \ldots, w_n$ be distinct variables in V. Let $X_{|A|-1}$ and X_n denote $\{x_1, \ldots, x_{|A|-1}\}$ and $\{x_1, \ldots, x_n\}$, respectively. We define that t_n denotes the term*

$$a_1X_{|A|-1} + \sum_{i=1}^{|A|-1} a_1(X_n \backslash \{x_i\}) + \sum_{i=|A|}^{n} a_1(X_{|A|-1} \cup \{x_i, w_i\}).$$

Proposition 2. *$t_n \trianglerighteq a_1X_n$ for $n \geq |A|$.*

Proof. Let $Z \subseteq X_n$ with $|Z| < |A|$. We need to find a summand a_1Y of t_n with $Z \subseteq Y \subseteq X_n$. We distinguish two cases.

1. $Z \subseteq X_{|A|-1}$. Then $Z \subseteq X_{|A|-1} \subseteq X_n$.

2. $Z \not\subseteq X_{|A|-1}$. Then $Z \subseteq X_n \backslash \{x_i\} \subseteq X_n$ for some $1 \leq i < |A|$.

Let $Z \subseteq X_n$ with $|Z| = |A|$. We need to find a summand $a_1 Y$ of t_n with $Z \subseteq Y$. We distinguish two cases.

1. $X_{|A|-1} \subset Z$. Then $Z \subseteq X_{|A|-1} \cup \{x_i, w_i\}$ for some $|A| \leq i \leq n$.
2. $X_{|A|-1} \not\subset Z$. Then $Z \subseteq X_n \backslash \{x_i\}$ for some $1 \leq i < |A|$. □

Proposition 3. *Let $n \geq |A|$. If the summands of u are a proper subset of the summands of t_n, then $a_1 X_n + u \approx u$ is not sound modulo $\sim_{\mathrm{R}}$.*

Proof. Suppose that all summands of u are summands of t_n, but that some summand $a_1 Y$ of t_n is not a summand of u. We consider the three possible forms of Y, and for each case give a closed substitution σ such that some ready pair of $\sigma(a_1 X_n)$ is not a ready pair of $\sigma(u)$.

1. $Y = X_{|A|-1}$.
   We define $\sigma(x_i) = a_i \mathbf{0}$ for $i = 1, \ldots, |A| - 1$, $\sigma(x_i) = \mathbf{0}$ for $i = |A|, \ldots, n$, and $\sigma(y) = a_{|A|}\mathbf{0}$ for $y \notin X_n$. Then the ready pair $(a_1, \{a_1, \ldots, a_{|A|-1}\})$ of $\sigma(a_1 X_n)$ is not a ready pair of $\sigma(u)$.
2. $Y = X_n \backslash \{x_j\}$ for some $1 \leq j < |A|$.
   We define $\sigma(x_i) = a_i \mathbf{0}$ for $i = 1, \ldots, j-1, j+1, \ldots, |A|$, $\sigma(x_i) = \mathbf{0}$ for $i = j$ and $i = |A| + 1, \ldots, n$, and $\sigma(y) = a_j \mathbf{0}$ for $y \notin X_n$. Then the ready pair $(a_1, \{a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_{|A|}\})$ of $\sigma(a_1 X_n)$ is not a ready pair of $\sigma(u)$.
3. $Y = X_{|A|-1} \cup \{x_j, w_j\}$ for some $|A| \leq j \leq n$.
   We define $\sigma(x_i) = a_i \mathbf{0}$ for $i = 1, \ldots, |A| - 1$, $\sigma(x_j) = a_{|A|}\mathbf{0}$, and $\sigma(y) = \mathbf{0}$ for $y \notin X_{|A|-1} \cup \{x_j\}$. Then the ready pair $(a_1, \{a_1, \ldots, a_{|A|}\})$ of $\sigma(a_1 X_n)$ is not a ready pair of $\sigma(u)$. □

Proposition 4. *Let $n \geq |A|$. If $t_n \approx u$ is sound modulo $\sim_{\mathrm{R}}$, then each summand of u is a summand of $a_1 X_n + t_n$.*

Proof. Let $t_n \approx u$ be sound modulo $\sim_{\mathrm{R}}$. By Lemma 1, *depth*$(u) = 1$. By Lemma 2, u does not have summands $x \in V$, so clearly each summand of u is of the form $a_1 Y$. If $|Y| < |A|$, then by Lemma 2, $a_1 Y$ is a summand of t_n. Let $|Y| \geq |A|$; we prove that $a_1 Y$ is a summand of $a_1 X_n + t_n$.

First we prove that $Y \subseteq X_n \cup \{w_i \mid i{=}|A|, \ldots, n\}$. Suppose, towards a contradiction, that there is a $y \in Y \backslash (X_n \cup \{w_i \mid i{=}|A|, \ldots, n\})$. We define $\sigma(y) = a_1 \mathbf{0}$, and $\sigma(z) = \mathbf{0}$ for $z \neq y$. The ready pair $(a_1, \{a_1\})$ of $\sigma(a_1 Y)$ is not a ready pair of $\sigma(t_n)$, contradicting that $t_n \approx u$ is sound modulo $\sim_{\mathrm{R}}$. Hence, $Y \subseteq X_n \cup \{w_i \mid i = |A|, \ldots, n\}$.

To prove that $a_1 Y$ is a summand of $a_1 X_n + t_n$, we consider two cases.

1. $w_i \in Y$ for some $|A| \leq i \leq n$.
   Suppose, towards a contradiction, that there is a $y \in Y \backslash (X_{|A|-1} \cup \{x_i, w_i\})$. We define $\sigma(y) = a_1 \mathbf{0}$, $\sigma(w_i) = a_2 \mathbf{0}$, and $\sigma(z) = \mathbf{0}$ for $z \notin \{y, w_i\}$. The ready

pair $(a_1, \{a_1, a_2\})$ of $\sigma(a_1Y)$ is not a ready pair of $\sigma(t_n)$, contradicting that $t_n \approx u$ is sound modulo $\sim_{\mathrm{R}}$.
Suppose, towards a contradiction, that there is an $x \in (X_{|A|-1} \cup \{x_i, w_i\}) \backslash Y$. Note that $w_i \in Y$ implies $x \neq w_i$. We define $\sigma(x) = a_1\mathbf{0}$, $\sigma(w_i) = a_2\mathbf{0}$, and $\sigma(z) = \mathbf{0}$ if $z \notin \{x, w_i\}$. The ready pair $(a_1, \{a_2\})$ of $\sigma(a_1Y)$ is not a ready pair of $\sigma(t_n)$, contradicting that $t_n \approx u$ is sound modulo $\sim_{\mathrm{R}}$.
Hence, $Y = X_{|A|-1} \cup \{x_i, w_i\}$.

2. $Y \subseteq X_n$.
Since $|Y| \geq |A|$, there is a $Z = \{z_1, \ldots, z_{|A|-1}\} \subseteq Y$ with $Z \neq X_{|A|-1}$. We define $\sigma(z_i) = a_i\mathbf{0}$ for $i = 1, \ldots, |A| - 1$, $\sigma(y) = \mathbf{0}$ for $y \in Y \backslash Z$, and $\sigma(z) = a_{|A|}\mathbf{0}$ for $z \notin Y$. The ready pair $(a_1, \{a_1, \ldots, a_{|A|-1}\})$ of $\sigma(a_1Y)$ must be a ready pair of $\sigma(t_n)$, which implies that there is a summand a_1Y' of t_n with $Z \subseteq Y' \subseteq Y \subseteq X_n$. Since $Z \neq X_{|A|-1}$, it follows that $Y' = X_n \backslash \{x_i\}$ for some $1 \leq i < |A|$. Hence, either $Y = X_n$ or $Y = X_n \backslash \{x_i\}$ for some $1 \leq i < |A|$.

Concluding, each summand of u is a summand of $a_1X_n + t_n$. □

The following example shows that Proposition 4 would fail if $|A| = 1$.

Example 2. Let $|A| = 1$ and $n = 1$. Note that $t_1 = a_1\mathbf{0} + a_1(x_1 + w_1)$ and $a_1X_1 = a_1x_1$. Since $|A| = 1$, $a_1\mathbf{0} + a_1(x_1 + w_1) \approx a_1w_1 + a_1\mathbf{0} + a_1(x_1 + w_1)$ is sound modulo $\sim_{\mathrm{R}}$. However, a_1w_1 is not a summand of $a_1x_1 + a_1\mathbf{0} + a_1(x_1 + w_1)$.

Theorem 2. *$C^n \nvdash a_1X_n + t_n \approx t_n$ for $n \geq |A|$.*

Proof. Suppose, towards a contradiction, that there is a derivation of $a_1X_n + t_n \approx t_n$ using only equations in C^n: $a_1X_n + t_n = u_0 \approx u_1 \approx \cdots \approx u_j = t_n$ for some $j \geq 1$. By Lemma 1, $u_1, \ldots, u_j$ have depth 1. Since $u_0 = a_1X_n + t_n$, $u_j = t_n$, and the equations in C^n are of the form $aY + v \approx v$, there must be a $1 \leq i \leq j$ such that $u_{i-1} = a_1X_n + u_i$ and a_1X_n is not a summand of u_i. Since $t_n \approx u_i$ is sound modulo $\sim_{\mathrm{R}}$, Proposition 4 implies that all summands of u_i are summands of t_n. Since $a_1X_n + u_i \approx u_i$ is sound modulo $\sim_{\mathrm{R}}$, Proposition 3 implies that $u_i = t_n$. Hence, $a_1X_n + t_n \approx t_n$ can be derived using a single application of an equation $a_1Y + v \approx v \in C^n$. Then $\sigma(Y) = X_n$ and $\sigma(v) + w = t_n$ for some substitution σ and term w. Since $a_1X_n + \sigma(v) \approx \sigma(v)$ is sound modulo $\sim_{\mathrm{R}}$ and $\sigma(v) + w = t_n$, Proposition 3 implies that $\sigma(v) = t_n$. However, $a_1Y + v \approx v \in C^n$ implies $S(v) \leq n$, and v does not contain summands from V, so clearly $S(\sigma(v)) \leq n$. This contradicts the fact that $S(\sigma(v)) = S(t_n) = n + 1$.

Concluding, $C^n \nvdash a_1X_n + t_n \approx t_n$. □

3.4 The Main Result

Corollary 1. *Let E be a finite axiomatization that is sound and complete for* BCCSP(A) *modulo an equivalence $\sim$ that is no coarser than readiness semantics and no finer than possible worlds semantics. If $1 < |A| < \infty$, then E is not ω-complete.*

Proof. Suppose, towards a contradiction, that E is ω-complete. By Propositions 2 and 1, $a_1 X_n + t_n \approx t_n$ for $n \geq |A|$ is sound modulo $\sim_{\mathrm{PW}}$, so also modulo $\sim$. Then these equations can be derived from E. Let E_1 denote the equations in E of depth ≤ 1. Clearly, $E_1 \vdash a_1 X_n + t_n \approx t_n$ for $n \geq |A|$ (cf. Lemma 1).

Choose an $n \geq |A|$ such that $S(t) \leq n$ and $S(u) \leq n$ for each $t \approx u \in E_1$. Since E_1 is sound modulo $\sim$, so also modulo $\sim_{\mathrm{R}}$, it follows that $E_1 \subseteq R_1^n$. By Theorem 1, $C^n \vdash E_1$. This implies that $C^n \vdash a_1 X_n + t_n \approx t_n$, which contradicts Theorem 2.

Concluding, E is not ω-complete. □

4 On Infinite Alphabets and Finite Bases: Possible Worlds

In case of an infinite alphabet, the equational theory of BCCSP modulo readiness semantics has a finite basis [9], while the equational theory of BCCSP modulo ready trace semantics does not have a finite basis [5]. In this section we prove that, in case of an infinite alphabet, the equational theory of BCCSP modulo possible worlds semantics has a finite basis.

Let $|A| = \infty$. From now on, we interpret occurrences of action names in axioms as variables (of type action), as else axiom A5 for BCCSP modulo possible worlds semantics given below would actually denote infinitely many axioms. To emphasize this interpretation, action names in axioms are written as α, β instead of a, b.

The axiomatization consisting of A1-4 together with

$$\text{A5} \quad \alpha(\beta x + \beta y + z) \approx \alpha(\beta x + z) + \alpha(\beta y + z)$$

is sound and complete for BCCSP modulo possible worlds semantics (see [28]).

We prove that A1-5 are ω-complete. The proof strategy, which is based on giving semantics to open terms, is rather standard (cf. [1,7,18]), so we only provide a sketch of the proof.

Theorem 3. *If $|A| = \infty$, then the axiomatization A1-5 is ω-complete.*

Proof. Terms are considered modulo A1,2 (so no longer modulo A3,4). The operational semantics for closed terms in Section 2 is extended to open terms by adding a transition rule for variables:

$$\frac{}{x \xrightarrow{x} \mathbf{0}}$$

Furthermore, possible worlds semantics (see Definition 1) is extended to open terms. First we define $\mathcal{I}(t)$ for open terms t: it denotes the set of actions a and variables x for which there exists a transition $t \xrightarrow{a} t'$ or $t \xrightarrow{x} t'$, respectively. A term t_1 is a *possible world* of a term t_0 if $\mathcal{I}(t_1) = \mathcal{I}(t_0)$, t_1 is deterministic, and for each transition $t_1 \xrightarrow{a} t_1'$ or $t_1 \xrightarrow{x} t_1'$, respectively, there is a transition $t_0 \xrightarrow{a} t_0'$ or $t_0 \xrightarrow{x} t_0'$, respectively, such that t_1' is a possible world of t_0'. We write $t \sim_{\mathrm{PW}}^{o} u$, if t and u have exactly the same possible worlds. Without proof we observe the following three facts.

(A) $t \sim^o_{\mathrm{PW}} u$ if and only if $\sigma(t) \sim_{\mathrm{PW}} \sigma(u)$ for all closed substitutions σ.[2]

(B) The term rewriting system

$$\begin{aligned}\alpha(\beta x + \beta y + z) &\to \alpha(\beta x + z) + a(\beta y + z)\\ x + x &\to x\\ x + 0 &\to x\end{aligned}$$

is *terminating*, meaning that it does not give rise to infinite reductions of BCCSP terms.

(C) If $t \sim^o_{\mathrm{PW}} u$, then the *normal forms* of t and u, with respect to the term rewriting system above, can all be equated by A1,2.

Finally, suppose $\sigma(t) = \sigma(u)$ can be derived from A1-5 for all closed substitutions σ. By the soundness of A1-5 modulo $\sim_{\mathrm{PW}}$, $\sigma(t) \sim_{\mathrm{PW}} \sigma(u)$ for all closed substitutions σ. By (A), $t \sim^o_{\mathrm{PW}} u$. By (B), t and u can be reduced to normal forms t' and u', respectively, using the rewrite rules. By (C), $t' \approx u'$ can be derived from A1,2. Hence, $t \approx t' \approx u' \approx u$ can be derived from A1-5. □

References

1. L. Aceto, W.J. Fokkink, R.J. van Glabbeek, and A. Ingólfsdóttir. Axiomatizing prefix iteration with silent steps. *Information Computation*, 127(1):26–40, 1996.
2. L. Aceto, W.J. 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(3):193–230, 1998.
3. L. Aceto, W.J. Fokkink, and A. Ingólfsdóttir. 2-nested simulation is not finitely equationally axiomatizable. In *Proceedings 18th Symposium on Theoretical Aspects of Computer Science (STACS'01)*, Dresden, LNCS 2010, pp. 39–50. Springer, 2001.
4. J.C.M. Baeten, J.A. Bergstra, and J.W. Klop. Ready-trace semantics for concrete process algebra with the priority operator. *The Computer Journal*, 30(6):498–506, 1987.
5. S.C.C. Blom, W.J. 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. Springer, 2003. To appear.
6. W.J. Fokkink and S.P. 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. R.J. van Glabbeek. A complete axiomatization for branching bisimulation congruence of finite-state behaviours. In *Proceedings 18th Symposium on Mathematical Foundations of Computer Science (MFCS'93)*, Gdansk, LNCS 711, pp. 473–484. Springer, 1993.
8. R.J. 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.

[2] The infinite alphabet is crucial for the validity of (A). The cover equations provide a counter-example in case of a finite alphabet.

9. 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.
10. R. Gurevič. Equational theory of positive natural numbers with exponentiation is not finitely axiomatizable. *Annals of Pure and Applied Logic*, 49:1–30, 1990.
11. J. Heering. Partial evaluation and ω-completeness of algebraic specifications. *Theoretical Computer Science*, 43:149–167, 1986.
12. L. Henkin. The logic of equality. *American Mathematical Monthly*, 84(8):597–612, 1977.
13. 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.
14. R.C. Lyndon. Identities in two-valued calculi. *Transactions of the American Mathematical Society*, 71:457–465, 1951.
15. R.N. McKenzie. Tarski's finite basis problem is undecidable. *International Journal of Algebra and Computation*, 6(1):49–104, 1996.
16. R.N. McKenzie, G. McNulty, and W. Taylor. *Algebras, Varieties, Lattices.* Wadsworth & Brooks/Cole, 1987.
17. R. Milner. *Communication and Concurrency.* Prentice Hall, 1989.
18. R. Milner. A complete axiomatisation for observational congruence of finite-state behaviours. *Information and Computation*, 81(2):227–247, 1989.
19. F. Moller. *Axioms for Concurrency.* PhD thesis, University of Edinburgh, 1989.
20. 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.
21. 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.
22. E.-R. Olderog and C.A.R. Hoare. Specification-oriented semantics for communicating processes. *Acta Informatica*, 23(1):9–66, 1986.
23. D.M.R. Park. Concurrency and automata on infinite sequences. In *Proceedings 5th GI (Gesellschaft für Informatik) Conference*, Karlsruhe, LNCS 104, pp. 167–183. Springer, 1981.
24. G.D. Plotkin. A structural approach to operational semantics. Report DAIMI FN-19, Aarhus University, 1981.
25. G.D. Plotkin. The λ-calculus is ω-incomplete. *Journal of Symbolic Logic*, 39:313–317, 1974.
26. A. Pnueli. Linear and branching structures in the semantics and logics of reactive systems. In W. Brauer, ed., *Proceedings 12th Colloquium on Automata, Languages and Programming (ICALP'85)*, Nafplion, LNCS 194, pp. 15–32. Springer, 1985.
27. W.C. Rounds and S.D. Brookes. Possible futures, acceptances, refusals, and communicating processes. In *Proceedings 22nd IEEE Symposium on Foundations of Comper Science (FOCS'81)*, Nashville, pp. 140-149. IEEE Computer Society Press, 1981.
28. S. Veglioni and R. De Nicola. Possible worlds for process algebras. In *Proceedings 9th Conference on Concurrency Theory (CONCUR'98)*, Nice, LNCS 1466, pp. 179–193. Springer, 1998.