On Finite Alphabets and Infinite Bases

Taolue Chen [a,1] Wan Fokkink [a,b,*] Bas Luttik [a,c] Sumit Nain [d]

[a] *CWI, Department of Software Engineering, PO Box 94079, 1090 GB Amsterdam, The Netherlands*

[b] *Vrije Universiteit Amsterdam, Department of Computer Science, De Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands*

[c] *Eindhoven University of Technology, Department of Computer Science, PO Box 513, 5600 MB Eindhoven, The Netherlands*

[d] *Rice University, Department of Computer Science, 6100 S. Main Street, Houston, TX 77005-1892, USA*

Abstract

Van Glabbeek (1990) presented the linear time – branching time spectrum of behavioral semantics. He studied these semantics in the setting of the basic process algebra BCCSP, and gave finite, sound and ground-complete, axiomatizations for most of these semantics. Groote (1990) proved for some of van Glabbeek's axiomatizations that they are *ω-complete*, meaning that an equation can be derived if (and only if) all of its closed instantiations can be derived. In this paper we settle the remaining open questions for all the semantics in the linear time – branching time spectrum, either positively by giving a finite sound and ground-complete axiomatization that is ω-complete, or negatively by proving that such a finite basis for the equational theory does not exist. We prove that in case of a finite alphabet with at least two actions, failure semantics affords a finite basis, while for ready simulation, completed simulation, simulation, possible worlds, ready trace, failure trace and ready semantics, such a finite basis does not exist. Completed simulation semantics also lacks a finite basis in case of an infinite alphabet of actions.

Key words: Concurrency, Process Algebra, Equational Theory, ω-Completeness.

* Corresponding author.
Email addresses: chen@cwi.nl (Taolue Chen), wanf@cs.vu.nl (Wan Fokkink), s.p.luttik@tue.nl (Bas Luttik), sumitnain@yahoo.com (Sumit Nain).

[1] Supported by the Dutch Bsik project BRICKS (Basic Research in Informatics for Creating the Knowledge Society).

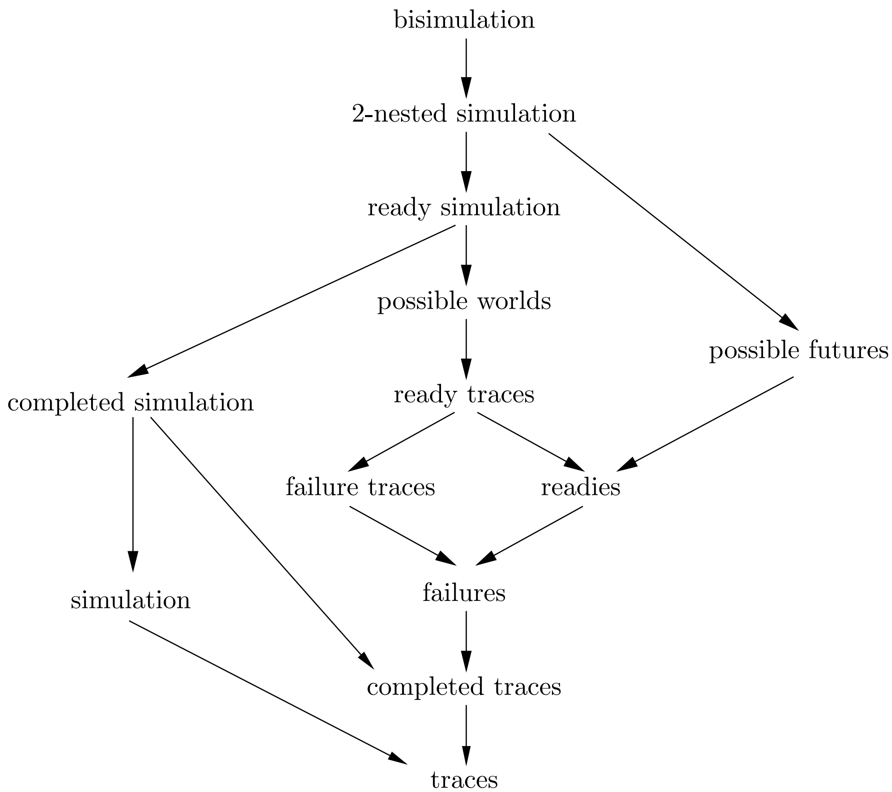

Fig. 1. The linear time – branching time spectrum

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 semantics 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 semantics for concurrent processes.

Van Glabbeek [11,12] presented the linear time – branching time spectrum of behavioral semantics for finitely branching, concrete, sequential processes. These semantics are based on simulation notions or on decorated traces. Figure 1 depicts the linear time – branching time spectrum, where an arrow from one semantics to another means that the source of the arrow is finer than the target.

To give further insight into the identifications made by the respective behavioral equivalences in his spectrum, van Glabbeek [11,12] studied them 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. In particular, he associated with every behavioral equivalence in his spectrum a sound equational axiomatization, a collection of equations of behaviorally equivalent BCCSP terms. Most of the axiomatizations were also shown to be complete in the sense that whenever two *closed* BCCSP terms are behaviorally equivalent, then the axiomatization admits a derivation in equational logic of the corresponding equation.

In this paper, we shall consider a more general form of completeness. We call an axiomatization *complete* if any two behaviorally equivalent BCCSP terms (not just the closed ones) can be equated; completeness for closed terms only we shall henceforth refer to as *ground-completeness*. A complete axiomatization of a behavioral semantics yields a purely syntactic characterization, independent of the underlying labeled transition system and of the actual details of the definition of the behavioral semantics. Such a bridge between syntax and semantics plays an important role in both the theory and practice of process algebras. From the point of view of theory, it gives insight in the semantic relationships between the syntactic constructions. From the point of view of practice, a complete axiomatization can be used to perform system verifications in a purely syntactic way using general purpose theorem provers or proof checkers, and form the foundation of purpose-built axiomatic verification tools like, e.g., PAM [17].

A complete axiomatization enjoys the property that whenever all closed instances of an equation can be derived from it, then the equation itself can also be derived from it; this property is generally referred to as *ω-completeness*. For theorem proving applications, it is particularly 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 [18]. In [15] it was argued that ω-completeness is desirable for the partial evaluation of programs. Notable examples of ω-incomplete axiomatizations in the literature are the $\lambda K\beta\eta$-calculus (see [28]) and the equational theory of CCS [25]. 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 [24,4] and ACP [8].

In universal algebra, a complete axiomatization is referred to as a *basis* for the equational theory of the algebra it axiomatizes. The existence of a finite basis for an equational theory is a classic topic of study in universal algebra (see, e.g., [21]), dating back to Lyndon [19]. Murskiĭ [27] proved that “almost all” finite algebras (namely all quasi-primal ones) are finitely based, while in [26] he presented an example of a three-element algebra that has no finite basis. Henkin [16] showed that the algebra of naturals with addition and multiplication is finitely based, while Gurevič [14] showed that after adding exponentiation the algebra is no longer finitely based. McKenzie [20] settled Tarski's Finite Basis Problem in the negative, by showing that the general question whether a finite algebra is finitely based is undecidable.

Given a finite ground-complete axiomatization, to prove that it is a finite basis, it suffices to establish that it is ω-complete. Groote [13] proposed a general technique to prove that an axiomatization is ω-complete. He applied his technique to establish ω-completeness of several of van Glabbeek's ground-complete axiomatizations. In practice, Groote's technique only works in case of an infinite alphabet of actions. [2] On the other hand, in case of a singleton alphabet, most of the semantics in the linear time – branching time spectrum collapse to either trace or completed trace semantics, in which case the equational theory of BCCSP is known to have a finite basis. However, in case of a finite alphabet with at least two actions, for most semantics in the linear time – branching time spectrum it remained unknown whether the equational theory of BCCSP has a finite basis. In this paper, we settle all remaining open questions.

We give a summary of what was known up to now, and which open questions remained. Moller [24] proved that the sound and ground-complete axiomatization for BCCSP modulo bisimulation equivalence is ω-complete, independent of the cardinality of the alphabet A. Groote [13] presented ω-completeness proofs for completed trace equivalence (again independent of the cardinality of A), for trace equivalence (if $|A| > 1$), and for ready and failure equivalence (if $|A| = \infty$). Van Glabbeek [12, p78] 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 $|A| = \infty$. The same observation can be made regarding possible worlds semantics. Blom, Fokkink and Nain [5] 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, for any A. If $|A| = 1$, then all semantics from completed traces up to ready simulation coincide with completed trace semantics, while simulation coincides with trace semantics. 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 prove that there is a finite basis for the equational theory of BCCSP modulo failure semantics, in case $1 < |A| < \infty$. For all the other question marks in Table 9 we prove that such a finite basis does not exist. This

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

paper combines results that were presented in [6,7,9,10]. Only the negative result on failure traces, in Section 4, was not published before.

The semantics considered in this paper have a natural formulation as a *preorder* relation $\precsim$, where $p \precsim q$ if p is in some way simulated by q, or if the decorated traces of p are included in those of q. The corresponding *equivalence* relation $\simeq$ is defined as: $p \simeq q$ if and only if both $p \precsim q$ and $q \precsim p$. Recently, Aceto, Fokkink and Ingolfsdottir [2] gave an algorithm that, given a sound and ground-complete axiomatization for BCCSP modulo a preorder no finer than ready simulation, produces a sound and ground-complete axiomatization for BCCSP modulo the corresponding equivalence. Moreover, if the original axiomatization for the preorder is ω-complete, then so is the resulting axiomatization for the equivalence. So for the positive result regarding failure semantics, the stronger result is obtained by considering failure preorder. On the other hand, the negative results become more general if they are proved for the equivalence relations.

This paper is set up as follows. Section 2 presents basic definitions regarding the linear time - branching time spectrum, the process algebra BCCSP, and equational logic. Section 3 contains a positive result for failure preorder. The remainder of the paper presents negative results: Section 4 for failure trace equivalence, Section 5 for any equivalence from possible worlds up to ready pairs, Section 6 for simulation equivalence, Section 7 for completed simulation equivalence, and Section 8 for ready simulation equivalence. We conclude in Section 9 with an overview of the positive and negative results pertaining to the existence of finite bases for BCCSP modulo the equivalences in the linear time – branching time spectrum.

2 Preliminaries

2.1 The linear time – branching time spectrum

Van Glabbeek presented in [11,12] the linear time – branching time spectrum of behavioral semantics for finitely branching, concrete processes. In this section we define the preorder and equivalence relations in this spectrum (except for 2-nested simulation and possible futures, which will not play a role in our paper).

A *labeled transition system* consists of a set of states S, with typical element s, and a transition relation $\rightarrow \subseteq S \times L \times S$, where L is a set of labels ranged over by a. We write $s \xrightarrow{a} s'$ if the triple (s, a, s') is an element of $\rightarrow$. The set $\mathcal{I}(s)$ consists of those labels a for which there exists s' such that $s \xrightarrow{a} s'$.

Let $a_1 \cdots a_k$ be a sequence of labels; we write $s \xrightarrow{a_1 \cdots a_k} s'$ if there are states $s_0, \ldots, s_k$ such that $s = s_0 \xrightarrow{a_1} \cdots \xrightarrow{a_k} s_k = s'$.

First we define six semantics based on decorated versions of execution traces.

Definition 1 (Decorated Traces) *Assume a labeled transition system.*

- *A sequence* $a_1 \cdots a_k$, *with* $k \geq 0$, *is a* trace *of a state* s *if there is a state* s' *such that* $s \xrightarrow{a_1 \cdots a_k} s'$. *It is a* completed trace *of* s *if moreover* $\mathcal{I}(s') = \emptyset$.
- *A pair* $(a_1 \cdots a_k, B)$, *with* $k \geq 0$ *and* $B \subseteq A$, *is a* ready pair *of a state* s_0 *if there is a sequence of transitions* $s_0 \xrightarrow{a_1} \cdots \xrightarrow{a_k} s_k$ *with* $\mathcal{I}(s_k) = B$. *It is a* failure pair *of* s_0 *if there is such a sequence with* $\mathcal{I}(s_k) \cap B = \emptyset$.
- *A sequence* $B_0 a_1 B_1 \ldots a_k B_k$, *with* $k \geq 0$ *and* $B_0, \ldots, B_k \subseteq A$, *is a* ready trace *of a state* s_0 *if there is a sequence of transitions* $s_0 \xrightarrow{a_1} \cdots \xrightarrow{a_k} s_k$ *with* $\mathcal{I}(s_i) = B_i$ *for* $i = 0, \ldots, k$. *It is a* failure trace *of* s_0 *if there is such a sequence with* $\mathcal{I}(s_i) \cap B_i = \emptyset$ *for* $i = 0, \ldots, k$.

We write $s \precsim_{\Box} s'$ *with* $\Box \in \{\mathrm{T}, \mathrm{CT}, \mathrm{R}, \mathrm{F}, \mathrm{RT}, \mathrm{FT}\}$ *if the traces, completed traces, ready pairs, failure pairs, ready traces, or failure traces, respectively, of* s *are included in those of* s'. *We write* $s \simeq_{\Box} s'$ *if both* $s \precsim_{\Box} s'$ *and* $s' \precsim_{\Box} s$.

Next we define five semantics based on simulation.

Definition 2 (Simulations) *Assume a labeled transition system.*

- *A binary relation* $\mathcal{R}$ *on states is a* simulation *if* $s_0 \mathrel{\mathcal{R}} s_1$ *and* $s_0 \xrightarrow{a} s_0'$ *imply* $s_1 \xrightarrow{a} s_1'$ *for some state* s_1' *with* $s_0' \mathrel{\mathcal{R}} s_1'$.
- *A simulation* $\mathcal{R}$ *is a* completed simulation *if* $s_0 \mathrel{\mathcal{R}} s_1$ *and* $\mathcal{I}(s_0) = \emptyset$ *imply* $\mathcal{I}(s_1) = \emptyset$.
- *A simulation* $\mathcal{R}$ *is a* ready simulation *if* $s_0 \mathrel{\mathcal{R}} s_1$ *and* $a \notin \mathcal{I}(s_0)$ *imply* $a \notin \mathcal{I}(s_1)$.
- *The set* D *of* deterministic *states is the largest set such that for each* $s \in D$ *and* $a \in \mathcal{I}(s)$ *there is exactly one state* s' *such that* $s \xrightarrow{a} s'$, *and always* $s' \in D$. *A state* s_0 *is a* possible world *of a state* s_1 *if* s_0 *is deterministic and* $s_0 \mathrel{\mathcal{R}} s_1$ *for some ready simulation* $\mathcal{R}$.
- *A* bisimulation *is a symmetric simulation.*

We write $s \precsim_{\Box} s'$ *with* $\Box \in \{\mathrm{S}, \mathrm{CS}, \mathrm{RS}\}$ *if there exists a simulation, completed simulation, or ready simulation* $\mathcal{R}$, *respectively, with* $s \mathrel{\mathcal{R}} s'$, *and we write* $s \precsim_{PW} s'$ *if the possible worlds of* s *are included in those of* s'. *We write* $s \simeq_{\Box} s'$ *if both* $s \precsim_{\Box} s'$ *and* $s' \precsim_{\Box} s$.

BCCSP is a basic process algebra for expressing finite process behavior. Its signature consists of the constant $\mathbf{0}$, the binary operator $\_ + \_$, and unary prefix operators $a\_$, where a ranges over a nonempty set A of actions, called the *alphabet*, with typical elements a, b, c. Intuitively, closed BCCSP terms, denoted by p, q, r, represent finite process behaviors, where $\mathbf{0}$ does not exhibit any behavior, $p + q$ offers a choice between the behaviors of p and q, and ap executes action a to transform into p. This intuition is captured by the transition rules below, in which a ranges over A. They give rise to A-labeled transitions between BCCSP terms.

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

We also assume a countably infinite set V of variables; x, y, z denote elements of V, and X, Y, Z denote finite subsets of V. Open BCCSP terms, which may contain variables from V, are denoted by t, u, v, w. A term t is called a *prefix* if $t = at'$ for some $a \in A$ and for some term t'.

The preorders $\precsim$ in the linear time – branching time spectrum are all *precongruences* with respect to BCCSP, meaning that $p_1 \precsim q_1$ and $p_2 \precsim q_2$ imply $p_1 + p_2 \precsim q_1 + q_2$ and $ap_1 \precsim aq_1$ for $a \in A$. Likewise, the equivalences in the spectrum are all *congruences* with respect to BCCSP.

A (closed) substitution, denoted by ρ, σ, τ, maps variables in V to (closed) BCCSP terms. For open BCCSP terms t and u, and a preorder $\precsim$ (or equivalence $\simeq$) on closed BCCSP terms, 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.

It is technically convenient to extend the operational semantics to open BCCSP terms. We do not include additional rules for variables, which effectively means that they do not exhibit any behavior. The *depth* of a BCCSP term t, denoted by $depth(t)$, is the length of the longest trace that t can exhibit, i.e.,

$$depth(t) = \max\{k \mid \exists a_1 \cdots a_k, t'.t \xrightarrow{a_1 \cdots a_k} t'\} \ .$$

Let $k \geq 0$. If $t \xrightarrow{a_1 \cdots a_k} t'$ for some sequence of actions $a_1 \cdots a_k$, and t' has the variable x as a summand, then we say that *x occurs in t at depth k*. The set of variables with an occurrence in t at depth k will be denoted by $var_k(t)$; the set of *all* variables with an occurrence in t will be denoted by $var(t)$. Similarly, if $t \xrightarrow{a_1 \cdots a_k} t'$ for some sequence of actions $a_1 \cdots a_k$, and the action a is an element of $\mathcal{I}(t')$, then we say that *a occurs in t at depth k*. The set of actions with an occurrence in t at depth k will be denoted by $act_k(t)$.

We provide some basic facts.

Lemma 3 *(1) If $t \precsim_{\mathrm{T}} u$, then $depth(t) \leq depth(u)$.*

(2) If $t \precsim_{\mathrm{T}} u$, then $act_k(t) \subseteq act_k(u)$ for all $k \geq 0$. Moreover, if $t \precsim_F u$, then also $act_0(u) \subseteq act_0(t)$, so $\mathcal{I}(t) = \mathcal{I}(u)$.

(3) Suppose $|A| > 1$. If $t \precsim_{\mathrm{T}} u$, then, for all variables x, $t \xrightarrow{a_1 \cdots a_k} x + t'$ for some term t' implies $u \xrightarrow{a_1 \cdots a_k} x + u'$ for some term u'. Hence $var_k(t) \subseteq var_k(u)$ for all $k \geq 0$.

Proof:

(1) If $depth(t) = k$, then there exists a sequence of actions $a_1 \cdots a_k$ and a term t' such that $t \xrightarrow{a_1 \cdots a_k} t'$. Let ρ be the closed substitution defined by $\rho(x) = \mathbf{0}$ for all $x \in V$. Then $a_1 \cdots a_k$ is a trace of $\rho(t)$ and hence, since $t \precsim_{\mathrm{T}} u$, of $\rho(u)$. From the definition of ρ it is then clear that there exists a term u' such that $u \xrightarrow{a_1 \cdots a_k} u'$. It follows that $depth(t) = k \leq depth(u)$.

(2) First suppose $t \precsim_{\mathrm{T}} u$ and let $a \in act_k(t)$ for some $k \geq 0$. Then there exists a sequence of actions $a_1 \cdots a_k$ and a term t' such that $t \xrightarrow{a_1 \cdots a_k} t'$ and $a \in \mathcal{I}(t')$. Now, let ρ be the closed substitution defined by $\rho(x) = \mathbf{0}$ for all $x \in V$. Then $a_1 \cdots a_k a$ is a trace of $\rho(t)$ and hence, since $t \precsim_{\mathrm{T}} u$, of $\rho(u)$. From the definition of ρ it is then clear that there exists a term u' such that $u \xrightarrow{a_1 \cdots a_k} u'$ with $a \in \mathcal{I}(u')$, so $a \in act_k(u)$.

Next, suppose $t \precsim_{\mathrm{F}} u$ and let ρ be the closed substitution defined by $\rho(x) = \mathbf{0}$ for all $x \in V$. Then $(\lambda, A \setminus \mathcal{I}(t))$ (with λ denoting the empty sequence) is a failure pair of $\rho(t)$, and hence of $\rho(u)$, so $\mathcal{I}(u) \cap (A \setminus \mathcal{I}(t)) = \emptyset$; it follows that $act_0(u) \subseteq act_0(t)$. Since $t \precsim_{\mathrm{F}} u$ implies $t \precsim_{\mathrm{T}} u$, and hence $act_0(t) \subseteq act_0(u)$, it immediately follows that $\mathcal{I}(t) = act_0(t) = act_0(u) = \mathcal{I}(u)$.

(3) Let x be a variable and suppose $t \xrightarrow{a_1 \cdots a_k} x + t'$ for some term t'. Let $m \geq depth(u)$, let a and b be two distinct elements of A, and let ρ be the closed substitution defined by $\rho(x) = a^m b\mathbf{0}$ and $\rho(y) = \mathbf{0}$ for any variable $y \neq x$. Then $\rho(t) \xrightarrow{a_1 \cdots a_{k+m} b} \mathbf{0}$ (with $a_{k+1} \cdots a_{k+m} = a^m$). Since $\rho(t) \precsim_{\mathrm{T}} \rho(u)$, $a_1 \cdots a_{k+m} b$ is also a trace of $\rho(u)$. Since $m \geq depth(u)$, clearly $u \xrightarrow{a_1 \cdots a_i} z + u'$ for some $i < m$, where $\rho(z) \xrightarrow{a_{i+1} \cdots a_{k+m} b} p$. By the definition of ρ, $z = x$ and $i = k$, so $u \xrightarrow{a_1 \cdots a_k} x + u'$ for some term u'. Clearly it follows that $x \in var_k(t)$ implies $x \in var_k(u)$ for all variables x, so $var_k(t) \subseteq var_k(u)$. $\Box$

Note that Lemma 3(3) fails in case $|A| = 1$, for if $A = \{a\}$, then $x \precsim_{\mathrm{T}} ax$. In the remainder of this paper we will assume that $|A| > 1$.

An *equational axiomatization* is a collection of equations $t \approx u$, and an *inequational axiomatization* is a collection of inequations $t \preccurlyeq u$. The (in)equations in an axiomatization E are referred to as *axioms*. If E is an equational axiomatization, we write $E \vdash t \approx u$ if the equation $t \approx u$ is derivable from the axioms in E using the rules of equational logic (reflexivity, symmetry, transitivity, substitution, and closure under BCCSP contexts):

$$\frac{}{t \approx t} \quad \frac{t \approx u}{u \approx t} \quad \frac{t \approx u \quad u \approx v}{t \approx v} \quad \frac{t \approx u}{\rho(t) \approx \rho(u)} \quad \frac{t \approx u}{at \approx au} \quad \frac{t_1 \approx u_1 \quad t_2 \approx u_2}{t_1 + t_2 \approx u_1 + u_2}$$

For the derivation of an inequation $t \preccurlyeq u$ from an inequational axiomatization E of inequations, denoted by $E \vdash t \preccurlyeq u$, the second rule, for symmetry, is omitted.

It is well-known that whenever there exists a derivation of the equation $t \approx u$ from an equational axiomatization E, then there exists a derivation in which

- every application of the symmetry rule has an axiom as its premise; and
- every application of the substitution rule has either an axiom or the conclusion of an application of the symmetry rule as its premise.

This fact can be used to simplify proofs by induction on equational derivations. Let E' be the collection of equations that consists of all substitution instances of the axioms in E and their symmetric variants, i.e.,

$$E' = \{\rho(t) \approx \rho(u) \mid (t \approx u) \in E \text{ or } (u \approx t) \in E,\ \rho \text{ a substitution}\}\ .$$

By a *normalized derivation* of an equation $t \approx u$ from E we shall henceforth mean a derivation of the equation $t \approx u$ from E' by means of the rules of equational logic but not using the symmetry and substitution rules. Now if $E \vdash t \approx u$, then there exists a normalized derivation of $t \approx u$ from E.

An axiomatization E is *sound* modulo $\precsim$ (or $\simeq$) if for any open BCCSP 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 BCCSP terms p and q; it is *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* BCCSP terms p and q. Finally, E is *ω-complete* if for any open BCCSP terms t and 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 $E \vdash t \approx u$). A preorder $\precsim$ or an equivalence $\simeq$ is said to be *finitely based* if there exists a finite axiomatization E that is sound and complete modulo $\precsim$ or $\simeq$.

The core axioms A1-4 [23] for BCCSP below are ω-complete, and sound and ground-complete modulo bisimulation equivalence. Since every equivalence in the linear time – branching time spectrum (see Figure 1) includes bisimulation equivalence, it follows that the axioms A1-4 are sound modulo every equivalence in the spectrum. Furthermore, each of the axioms A1-4 induces two inequations, obtained by replacing $\approx$ by $\preccurlyeq$ or $\succcurlyeq$, that are both sound modulo every preorder in the linear time – branching time spectrum.

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

We write $t = u$ if terms t and u are equal modulo associativity, commutativity and idempotence of $+$, and modulo absorption of $\mathbf{0}$ summands. For every preorder $\precsim$ and equivalence $\simeq$ in the linear time – branching time spectrum, soundness of the axioms A1-4 ensures that whenever we write $t = u$, then also $t \precsim u$ and $t \simeq u$. Furthermore, we will (tacitly) assume that the axioms A1-4 above are included in every axiomatization E considered below, so that from $t = u$ we may always conclude $t \preccurlyeq u$ and $t \approx u$.

Let $\{t_1, \ldots, t_n\}$ be a finite set of terms; we use summation $\sum\{t_1, \ldots, t_n\}$ to denote $t_1 + \cdots + t_n$, adopting the convention that the summation of the empty set denotes $\mathbf{0}$. Furthermore, we write $a^n t$ to denote the term obtained from t by prefixing it n times with a, i.e., $a^0 t = t$ and $a^{n+1} t = a(a^n t)$. When writing terms, we adopt as binding convention that $\_ + \_$ and summation bind weaker than $a\_$. With abuse of notation, we often let a finite set X denote the term $\sum_{x \in X} x$.

Note that, with the above notational conventions, for every term t there always exist a finite family of actions $\{a_i \mid i \in I\}$, a finite family of terms $\{t_i \mid i \in I\}$, and a finite set of variables $X \subseteq V$ such that

$$t = \sum_{i \in I} a_i t_i + X \quad .$$

A term t is called a *summand* of u (notation: $t \sqsubseteq u$) if it is a variable or a prefix and $u = u + t$.

2.3 Two proof techniques

We give a short introduction to two proof techniques that will be exploited in the remainder of this paper. The first technique is especially designed for BCCSP, while the second technique is more generally applicative.

Cover equations. This technique, which was introduced in [9], aims to obtain an explicit description of the equational theory of BCCSP modulo some equivalence.

The central idea is that if an equation $t \approx u$ is sound for BCCSP modulo some equivalence in the linear time – branching time spectrum, then $u + t \approx t$ and $t + u \approx u$ are sound as well; and from the last two equations one can derive $t \approx u$. Therefore, to extend an axiomatization consisting of A1-4 to a complete axiomatization of some equivalence in the linear time – branching time spectrum, it suffices to add sound equations of the form $x + u \approx u$ and $at + u \approx u$; such equations are called *cover equations*.

In order to further limit the form of the cover equations that need to be considered, one usually tries to establish the following properties for the equivalence $\simeq$ at hand:

(1) If $at + u + bv \simeq u + bv$ with $a \neq b$, then $at + u \simeq u$.
(2) If $t \simeq u$, then t and u contain the same variables, at the same depths.
(3) If $t + x \simeq u + x$, and x is not a summand of $t + u$,[3] then $t \simeq u$.

If the properties above hold, then it suffices to only consider cover equations of the form $at + au_1 + \cdots + au_n \approx au_1 + \cdots + au_n$.

By Lemma 3(3), the second property holds for all equivalences finer than or as fine as trace equivalence, in case $|A| > 1$. The first and third properties have to be proved for each equivalence separately. Proving the first property is generally easy, but proving the third property can be a challenge.

When the cover equations have been classified, one can proceed in two ways. Either one can determine a finite basis among the cover equations, or one can determine an infinite family of cover equations that obstructs a finite basis. We will follow the latter approach in Section 5, considering only equations of depth at most one, for congruences that are finer than or as fine as ready equivalence and coarser than or as coarse as possible worlds equivalence. Moreover, the cover equations technique turned out to be helpful in finding the infinite families of equations that obstruct a finite basis in Sections 4, 6, 7 and 8.

Proof-theoretic technique. To prove that no finite basis exists for an equivalence $\simeq$ it suffices to provide an infinite family of equations $t_n \approx u_n$ ($n = 1, 2, 3, \ldots$) that are all sound modulo $\simeq$, and to associate with every finite set of sound equations E a property P_E that holds for all equations derivable from E, but does not hold for at least one of the equations $t_n \approx u_n$.

[3] To see that this side condition is needed, note that, in general, $x + x \simeq \mathbf{0} + x$ but $x \not\simeq \mathbf{0}$.

It then follows that for every finite set of sound equations E there exists a sound equation $t_n \approx u_n$ that is not derivable from E. It follows that every finite set of sound equations is necessarily incomplete, and hence $\simeq$ is not finitely based.

We shall apply this proof-theoretic technique in Section 4 and in Sections 6–8, and in each case we proceed in three steps:

(1) We provide an infinite family of sound equations $t_n \approx u_n$ $(n = 1, 2, 3, \dots)$ and a suitable family of properties P_n $(n = 1, 2, 3, \dots)$ such that the property P_n fails for all the equations $t_i \approx u_i$ with $i \geq n$.
(2) We establish that the property P_n holds for every substitution instance of any sound equation $t \approx u$ with $depth(t), depth(u) \leq n$.
(3) We prove that P_n holds for every equation derivable from a collection E of sound equations $t \approx u$ with $depth(t), depth(u) \leq n$; the latter proof is by induction on normalized derivations, using (2) for the base case.

3 Failures

In this section we consider the failures preorder $\precsim_{\mathrm{F}}$. Van Glabbeek [12] presented a sound and ground-complete axiomatization of the failures preorder consisting of the axioms A1-4, the axiom

$$\mathrm{F1} \quad a(x+y) \preccurlyeq ax + a(y+z)$$

and the axiom $ax \preccurlyeq ax + az$. Note that the latter axiom is actually superfluous, since it can be obtained from F1 by substituting $\mathbf{0}$ for y and applying A3.

Below, we provide a basis for the equational theory of BCCSP modulo $\precsim_{\mathrm{F}}$. We shall prove that A1-4+F1 is a basis if $|A| = \infty$ (see Corollary 9). To get a basis for the case that $1 < |A| < \infty$, it will be necessary to add the following axiom:

$$\mathrm{F2}_A \quad \textstyle\sum_{a \in A} ax_a \preccurlyeq \sum_{a \in A} ax_a + y \ ,$$

where $\{x_a \mid a \in A\}$ is a family of distinct variables and $y \notin \{x_a \mid a \in A\}$. To see that $\mathrm{F2}_A$ is sound modulo $\precsim_{\mathrm{F}}$, let ρ be an arbitrary closed substitution and consider a failure pair $(a_1 \cdots a_k, B)$ of $\rho(\sum_{a \in A} ax_a)$. If $k > 0$, then clearly $(a_2 \cdots a_k, B)$ is a failure pair of $\rho(x_{a_1})$, so $(a_1 \cdots a_k, B)$ is a failure pair of $\rho(\sum_{a \in A} ax_a + y)$. On the other hand, if $k = 0$, then note that $\mathcal{I}(\rho(\sum_{a \in A} ax_a)) = A$, so $B = \emptyset$, and hence $(a_1 \cdots a_k, B)$ is a failure pair of $\rho(\sum_{a \in A} ax_a + y)$. To see that $\mathrm{F2}_{A'}$ is not sound modulo $\precsim_{\mathrm{F}}$ if A' is a proper subset of A, let ρ be the closed substitution such that $\rho(y) = b\mathbf{0}$ for some $b \notin A'$; then $\mathcal{I}(\rho(\sum_{a \in A'} ax_a)) = A' \neq A' \cup \{b\} = \mathcal{I}(\rho(\sum_{a \in A'} ax_a + y))$. Since

A1-4+F1 are sound modulo $\precsim_{\mathrm{F}}$ independent of the alphabet, it also follows that F2$_A$ cannot be derived from A1-4+F1.

Axiom F2$_A$ expresses that additional variable summands may be added to a term t whenever $\mathcal{I}(t) = A$. The following lemma confirms that the proviso $\mathcal{I}(t) = A$ is necessary.

Lemma 4 *If $t \precsim_F u$, then $var_0(t) \subseteq var_0(u)$, and if moreover $\mathcal{I}(t) \neq A$, then $var_0(t) = var_0(u)$.*

Proof: Suppose $t \precsim_{\mathrm{F}} u$.

That $var_0(t) \subseteq var_0(u)$ follows immediately from Lemma 3(3).

To prove that $\mathcal{I}(t) \neq A$ implies $var_0(t) = var_0(u)$, suppose, towards a contradiction, that $a \notin \mathcal{I}(t)$ for some $a \in A$ and that $x \in var_0(u) \setminus var_0(t)$ for some $x \in V$. Define a closed substitution ρ by $\rho(x) = a\mathbf{0}$ and $\rho(y) = \mathbf{0}$ for $y \neq x$. Since $a \notin \mathcal{I}(t)$ and $x \notin var_0(t)$, $(\lambda, \{a\})$ (with λ the empty trace) is a failure pair of $\rho(t)$. Since $x \in var_0(u)$, $(\lambda, \{a\})$ is not a failure pair of $\rho(u+Y)$. This contradicts the assumption that $t \precsim_{\mathrm{F}} u$. We conclude that $\mathcal{I}(t) \neq A$ implies $var_0(t) = var_0(u)$. $\square$

According to Lemma 4, all the variable summands of t are also summands of u. Moreover, if u has a variable summand x that t does not have, then $\mathcal{I}(t) = A$, so we can derive $t \preccurlyeq t + x$ with an application of F2$_A$. We proceed to establish, for all $a \in A$, a relation between a prefix summand at' of t and the sum of all similar prefix summands au' of u. To conveniently express this relation, we first introduce some further notation.

Let t be a term, and let $A' \subseteq A$; we define the *restriction* $t{\restriction_{A'}}$ of t to A' by

$$t{\restriction_{A'}} = \sum\{at' \mid a \in A' \;\&\; at' \sqsubseteq t\} \ .$$

Recall that $t \precsim_{\mathrm{F}} u$ if, for all closed substitutions ρ, the failure pairs of $\rho(t)$ are included in $\rho(u)$. The preorder $\precsim_{\mathrm{F}}$ fails to have certain structural properties with respect to the operations of BCCSP; in particular, we cannot in general conclude from $at \precsim_{\mathrm{F}} au$ that $t \precsim_{\mathrm{F}} u$. It will therefore be technically convenient to also have notation for a preorder that is slightly coarser than $\precsim_{\mathrm{F}}$. We define the *length* of a failure pair $(a_1 \cdots a_k, B)$ as the length of the sequence $a_1 \cdots a_k$, and we write $t \precsim_{\mathrm{F}}^1 u$ if, for all closed substitutions ρ, the failure pairs of length ≥ 1 of $\rho(t)$ are included in those of $\rho(u)$. We leave it to the reader to verify that $t \precsim_{\mathrm{F}} u$ if and only if $t \precsim_{\mathrm{F}}^1 u$ and $\mathcal{I}(u) \subseteq \mathcal{I}(t)$, and that $at \precsim_{\mathrm{F}}^1 au$ implies $t \precsim_{\mathrm{F}}^1 u$.

Lemma 5 *If $t \precsim_F^1 u$, then, for every summand at' of t, $at' \precsim_F u{\restriction_{\{a\}}}$.*

Proof: Suppose $t \precsim_{\mathrm{F}}^1 u$. Let at' be a summand of t and let ρ be a closed substitution.

We first prove that the failure pairs of length ≥ 1 of $\rho(at')$ are included in those of $\rho(u\lceil_{\{a\}})$, and then we will conclude that also the failure pairs of length 0 of $\rho(at')$ are included in those of $\rho(u\lceil_{\{a\}})$.

Consider a failure pair $(a_1 \cdots a_k, B)$ of $\rho(at')$ with $k \geq 1$. Then $(a_1 \cdots a_k, B)$ is a failure pair of $\rho(t)$. By our assumption that $t \precsim_{\mathrm{F}}^{1} u$, it follows that $(a_1 \cdots a_k, B)$ is a failure pair of $\rho(u)$. From this we cannot directly conclude that u has a summand au' such that $(a_1 \cdots a_k, B)$ is a failure pair of $\rho(au')$, as u may have a variable summand x such that $(a_1 \cdots a_k, B)$ is a failure pair of $\rho(x)$. To ascertain that u nevertheless also has the desired summand au', we define a modification ρ' of ρ such that for all $\ell < k$ and for all terms v, $\rho(v)$ and $\rho'(v)$ have the same failure pairs $(b_1 \cdots b_\ell, B)$, while $(a_1 \cdots a_k, B)$ is not a failure pair of $\rho'(x)$ for all $x \in V$.

We obtain $\rho'(x)$ from $\rho(x)$ by replacing subterms ap at depth $k-1$ by $\mathbf{0}$ if $a \notin B$ and by $a a\mathbf{0}$ if $a \in B$. That is,

$$\rho'(x) = \mathit{chop}_{k-1}(\rho(x))$$

with chop_m for all $m \geq 0$ inductively defined by

$$\begin{aligned}
\mathit{chop}_m(\mathbf{0}) &= \mathbf{0}\\
\mathit{chop}_m(p+q) &= \mathit{chop}_m(p) + \mathit{chop}_m(q)\\
\mathit{chop}_0(ap) &= \begin{cases} \mathbf{0} & \text{if } a \notin B\\ a a\mathbf{0} & \text{if } a \in B \end{cases}\\
\mathit{chop}_{m+1}(ap) &= a\,\mathit{chop}_m(p)
\end{aligned}$$

We first prove two properties concerning the failure pairs of $\mathit{chop}_m(p)$, for $m \geq 0$ and closed terms p.

(I) For all $\ell \leq m$, the closed terms p and $\mathit{chop}_m(p)$ have the same failure pairs $(b_1 \cdots b_\ell, B)$.

We apply induction on m.

Base case: Since the summands of $\mathit{chop}_0(p)$ are $a a\mathbf{0}$ for all $a \in \mathcal{I}(p) \cap B$, $\mathcal{I}(p) \cap B = \emptyset$ if and only if $\mathcal{I}(\mathit{chop}_0(p)) \cap B = \emptyset$.

Inductive case: Let $\ell \leq m+1$; we distinguish cases according to whether $\ell = 0$ or $\ell > 0$. If $\ell = 0$, then, since $\mathcal{I}(p) = \mathcal{I}(\mathit{chop}_{m+1}(p))$, it follows that $\mathcal{I}(p) \cap B = \emptyset$ if and only if $\mathcal{I}(\mathit{chop}_{m+1}(p)) \cap B = \emptyset$, so $(b_1 \cdots b_\ell, B)$ is a failure pair of p if and only if it is a failure pair of $\mathit{chop}_{m+1}(p)$. If $\ell > 0$, then, since $p \xrightarrow{b_1} p'$ if and only if $\mathit{chop}_{m+1}(p) \xrightarrow{b_1} \mathit{chop}_m(p')$ and, by the induction hypothesis, p' and $\mathit{chop}_m(p')$ have the same failure pairs

$(b_2 \cdots b_\ell, B)$, $(b_1 \cdots b_\ell, B)$ is a failure pair of p if and only if it is a failure pair of $chop_{m+1}(p)$.

(II) $chop_m(p)$ does not have any failure pair $(b_1 \cdots b_{m+1}, B)$.

We apply induction on m.

Base case: Since the summands of $chop_0(p)$ are $aa\mathbf{0}$ with $a \in \mathcal{I}(p) \cap B$, $chop_0(p)$ does not have a failure pair (b_1, B).

Inductive case: By induction, for closed terms q, $chop_m(q)$ does not have failure pairs $(b_2 \cdots b_{m+2}, B)$. Since the transitions of $chop_{m+1}(p)$ are $chop_{m+1}(p) \xrightarrow{b_1} chop_m(p')$ for $p \xrightarrow{b_1} p'$, it follows that $chop_{m+1}(p)$ does not have failure pairs $(b_1 \cdots b_{m+2}, B)$.

We proceed to prove that ρ' has the desired properties mentioned above.

(A) For all $\ell < k$ and for all terms v, $\rho(v)$ and $\rho'(v)$ have the same failure pairs $(b_1 \cdots b_\ell, B)$,

We apply induction on ℓ.

Base case: From the definition of $chop_{k-1}$ it follows that $\mathcal{I}(\rho'(x)) \cap B = \mathcal{I}(\rho(x)) \cap B$ for all $x \in V$. Hence, $\mathcal{I}(\rho(v)) \cap B = \emptyset$ if and only if $\mathcal{I}(\rho'(v)) \cap B = \emptyset$.

Inductive case: Let $\ell + 1 < k$. We prove for each summand of v that applying ρ or ρ' gives rise to the same failure pairs $(b_1 \cdots b_{\ell+1}, B)$. By property (I), $\rho(x)$ and $\rho'(x) = chop_{k-1}(\rho(x))$ have the same failure pairs $(b_1 \cdots b_{\ell+1}, B)$. Furthermore, by induction, for each summand $b_1 v'$ of v, $\rho(v')$ and $\rho'(v')$ have the same failure pairs $(b_2 \cdots b_{\ell+1}, B)$; so $\rho(b_1 v')$ and $\rho'(b_1 v')$ have the same failure pairs $(b_1 \cdots b_{\ell+1}, B)$.

(B) $(a_1 \cdots a_k, B)$ is not a failure pair of $\rho'(x)$ for all $x \in V$.

This is immediate from property (II).

Now, since $(a_1 \cdots a_k, B)$ is a failure pair of $\rho(at')$, $(a_2 \cdots a_k, B)$ is a failure pair of $\rho(t')$, and hence, by property (A), of $\rho'(t')$. It follows that $(a_1 \cdots a_k, B)$ is a failure pair of $\rho'(t)$, and hence, by our assumption that $t \precsim^1_{\mathrm{F}} u$, of $\rho'(u)$. Since, according to property (B), u does not have a variable summand x such that $(a_1 \cdots a_k, B)$ is a failure pair of $\rho'(x)$, and since $a_1 = a$, u must have a summand au' such that $(a_1 \cdots a_k, B)$ is a failure pair of $\rho'(au')$ of u. Then, again by property (A), $(a_1 \cdots a_k, B)$ is a failure pair of $\rho(au')$ and hence of $\rho(u{\restriction}_{\{a\}})$.

We have now established that the failure pairs of length ≥ 1 of $\rho(at')$ are included in those of $\rho(u{\restriction}_{\{a\}})$. In particular, since $\rho(at')$ has the failure pair $(a, \emptyset)$, so does $\rho(u{\restriction}_{\{a\}})$, and hence $\mathcal{I}(\rho(at')) = \{a\} = \mathcal{I}(\rho(u{\restriction}_{\{a\}}))$. As an immediate consequence we get that also the failure pairs of length 0 of $\rho(at')$ are included in those of $\rho(u{\restriction}_{\{a\}})$.

We conclude that $at' \precsim_{\mathrm{F}} u\lceil_{\{a\}}$. $\square$

We now proceed to establish that if the inequation $at' \preccurlyeq \sum_{j\in J} au_j$ is sound modulo the failures preorder, then it can be derived from A1-4+F1+F2$_A$. For the case that $\mathcal{I}(t) \neq A$, we need the following lemma.

Lemma 6 *If $at \precsim_F \sum_{j\in J} au_j$ and $\mathcal{I}(t) \neq A$, then there exists $j \in J$ such that $\mathcal{I}(u_j) \subseteq \mathcal{I}(t)$ and $var_0(u_j) \subseteq var_0(t)$.*

Proof: Suppose $at \precsim_{\mathrm{F}} \sum_{j\in J} u_j$ and $\mathcal{I}(t) \neq A$. Let $b \in A \setminus \mathcal{I}(t)$ and define the closed substitution ρ by $\rho(x) = \mathbf{0}$ if $x \in var_0(t)$ and $\rho(x) = b\mathbf{0}$ if $x \notin var_0(t)$. Then $(a, A \setminus \mathcal{I}(t))$ is a failure pair of $\rho(at)$, so there exists $j \in J$ such that $(a, A \setminus \mathcal{I}(t))$ is a failure pair of au_j. From $(A \setminus \mathcal{I}(t)) \cap \mathcal{I}(\rho(u_j)) = \emptyset$ it follows that $\mathcal{I}(u_j) \subseteq \mathcal{I}(t)$ and $var_0(u_j) \subseteq var_0(t)$. $\square$

The following lemma constitutes the crucial step in our completeness proof.

Lemma 7 *If $at \precsim_F \sum_{j\in J} au_j$, then A1-4+F1+F2$_A$ $\vdash at \preccurlyeq \sum_{j\in J} au_j$.*

Proof: We apply induction on the depth of t.

Note that from $at \precsim_{\mathrm{F}} \sum_{j\in J} au_j$ it follows that $t \precsim^1_{\mathrm{F}} \sum_{j\in J} u_j$. Let $t\lceil_{\mathcal{I}(t)} = \sum_{i\in I} b_i t_i$. Then, for all $i \in I$, by Lemma 5 $b_i t_i \precsim_{\mathrm{F}} \sum_{j\in J} u_j\lceil_{\{b_i\}}$, and hence by the induction hypothesis A1-4+F1+F2$_A$ $\vdash b_i t_i \preccurlyeq \sum_{j\in J} u_j\lceil_{\{b_i\}}$. It follows that

$$\text{A1-4+F1+F2}_A \vdash t\lceil_{\mathcal{I}(t)} = \sum_{i\in I} b_i t_i \preccurlyeq \sum_{i\in I}\sum_{j\in J} u_j\lceil_{\{b_i\}} = \sum_{j\in J} u_j\lceil_{\mathcal{I}(t)} \ . \qquad (1)$$

We distinguish two cases.

Case 1: $\mathcal{I}(t) \neq A$.

According to Lemma 6 that there exists $j_0 \in J$ such that $\mathcal{I}(u_{j_0}) \subseteq \mathcal{I}(t)$ and $var_0(u_{j_0}) \subseteq var_0(t)$, and hence

$$u_{j_0}\lceil_{\mathcal{I}(t)} + var_0(t) = u_{j_0} + var_0(t) \ . \qquad (2)$$

We get the following derivation:

$$\begin{aligned} at &= a(t\restriction_{\mathcal{I}(t)} + var_0(t)) \\ &\preccurlyeq a(\sum_{j\in J} u_j\restriction_{\mathcal{I}(t)} + var_0(t)) && \text{(by (1))} \\ &= a(u_{j_0} + \sum_{j\in J} u_j\restriction_{\mathcal{I}(t)} + var_0(t)) && \text{(by (2))} \\ &\preccurlyeq au_{j_0} + a(\sum_{j\in J} u_j + var_0(t)) && \text{(by F1)} \\ &= au_{j_0} + a\sum_{j\in J} u_j && \text{(by Lemma 3(3))} \\ &\preccurlyeq au_{j_0} + \sum_{j\in J} au_j && \text{(by F1)} \\ &= \sum_{j\in J} au_j \ . \end{aligned}$$

Case 2: $\mathcal{I}(t) = A$.

If $\mathcal{I}(t) = A$, then, since $var_0(t) \subseteq \bigcup_{j\in J} var_0(u_j)$ by Lemma 3(3), with an application of F2$_A$

$$t = t\restriction_{\mathcal{I}(t)} + var_0(t) \preccurlyeq t\restriction_{\mathcal{I}(t)} + \bigcup_{j\in J} var_0(u_j) \ . \tag{3}$$

We now get the following derivation:

$$\begin{aligned} at &= a(t\restriction_{\mathcal{I}(t)} + var_0(t)) \\ &\preccurlyeq a(t\restriction_{\mathcal{I}(t)} + \bigcup_{j\in J} var_0(u_j)) && \text{(by (3))} \\ &\preccurlyeq a(\sum_{j\in J} u_j\restriction_{\mathcal{I}(t)} + \bigcup_{j\in J} var_0(u_j)) && \text{(by (1))} \\ &= a\sum_{j\in J} u_j && \text{(since } \mathcal{I}(t) = A\text{)} \\ &\preccurlyeq \sum_{j\in J} au_j && \text{(by F1)} \end{aligned}$$

Concluding, we have proved that A1-4+F1+F2$_A \vdash at \preccurlyeq \sum_{j\in J} au_j$. □

We are now in a position to establish that A1-4+F1+F2$_A$ constitutes a complete axiomatization of the failures preorder.

Theorem 8 *If $0 < |A| < \infty$, then A1-4+F1+F2$_A$ is a complete axiomatization of BCCSP modulo failures preorder, i.e., for all terms t and u, if $t \precsim_F u$, then A1-4+F1+F2$_A \vdash t \preccurlyeq u$.*

Proof: Suppose $t \precsim_{\mathrm{F}} u$, and suppose $t = \sum_{i\in I} a_i t_i + var_0(t)$. Then, for all $i \in I$, by Lemma 5 $a_i t_i \precsim_{\mathrm{F}} u\restriction_{\{a_i\}}$, so by Lemma 7, A1-4+F1+F2$_A \vdash a_i t_i \preccurlyeq u\restriction_{\{a_i\}}$.

Clearly, since $\mathcal{I}(t) = \mathcal{I}(u)$ by Lemma 3(2), it follows that

$$\text{A1-4+F1+F2}_A \vdash t{\restriction_{\mathcal{I}(t)}} \preccurlyeq u{\restriction_{\mathcal{I}(u)}} \enspace .$$

There are now two cases:

CASE 1: $\mathcal{I}(t) \neq A$.

Then $var_0(t) = var_0(u)$ by Lemma 4, so clearly

$$\text{A1-4+F1+F2}_A \vdash t = t{\restriction_{\mathcal{I}(t)}} + var_0(t) \preccurlyeq u{\restriction_{\mathcal{I}(u)}} + var_0(u) = u \enspace .$$

CASE 2: $\mathcal{I}(t) = A$.

Then $var_0(t) \subseteq var_0(u)$ by Lemma 4, so $t = t{\restriction_{\mathcal{I}(t)}} + var_0(t) \preccurlyeq t{\restriction_{\mathcal{I}(t)}} + var_0(u)$ by F2_A, and hence

$$\text{A1-4+F1+F2}_A \vdash t = t{\restriction_{\mathcal{I}(t)}} + var_0(t) \preccurlyeq u{\restriction_{\mathcal{I}(u)}} + var_0(u) = u \enspace .$$

The proof is now complete. □

Groote [13] proved that in case $|A| = \infty$, BCCSP modulo failures *equivalence* has a finite basis. Here we can obtain the same result for failure *preorder*, by copying the proofs of Lemma 7 and Theorem 8, but omitting in both proofs "CASE 2", which is only relevant for finite alphabets.

Corollary 9 *If $|A| = \infty$, then A1-4+F1 is a complete axiomatization of BCCSP modulo failures preorder.*

4 Failure Traces

In this section we consider failure trace equivalence $\simeq_{\rm FT}$. Blom, Fokkink and Nain [5] gave a finite axiomatization that is sound and ground-complete for BCCSP modulo $\simeq_{\rm FT}$. It consists of axioms A1-4 together with

$$\begin{array}{ll} \text{FT} & ax + ay \approx ax + ay + a(x+y) \\ \text{RS} & a(bx + by + z) \approx a(bx + by + z) + a(bx + z) \enspace , \end{array}$$

where a, b range over A. Groote [13] applied his technique of inverted substitutions to prove that this axiomatization is ω-complete in case A is infinite.

In this section we consider the case $1 < |A| < \infty$. We prove that then there does not exist a finite sound and ground-complete axiomatization for BCCSP modulo $\simeq_{\rm FT}$ that is ω-complete as well, and therefore failure trace equivalence is not finitely based over BCCSP. The corner stone for this negative result is the following infinite family of equations e_n ($n \geq 1$):

$$a^{n+1}x + a(a^n x + x) + a \sum_{b \in A \setminus \{a\}} a^n(b\mathbf{0} + x)$$
$$\approx a(a^n x + x) + a \sum_{b \in A \setminus \{a\}} a^n(b\mathbf{0} + x) \ .$$

These equations are sound modulo $\simeq_{\mathrm{FT}}$. The idea is that, given a closed substitution ρ, either $\mathcal{I}(\rho(x)) \subseteq \{a\}$, in which case the failure traces of $\rho(a^{n+1}x)$ are included in those of $\rho(a(a^n x+x))$. Or $c \in \mathcal{I}(\rho(x))$ for some $c \neq a$, in which case the failure traces of $\rho(a^{n+1}x)$ are included in those of $\rho(a\sum_{b \in A \setminus \{a\}} a^n(b\mathbf{0}+x))$.

We shall use the proof-theoretic technique to show that $\simeq_{\mathrm{FT}}$ is not finitely based. The intuition behind our proof is that if the axioms in E have depth at most n, then the summand $a^{n+1}x$ at the left-hand side of e_n cannot be eliminated by means of a derivation from E. There is, however, one complication: the summand $a^{n+1}x$ may be "glued together" with other summands. For example, using the axioms FT and RS we can derive for $n \geq 1$:

$$a^{n+1}x + a \sum_{b \in A \setminus \{a\}} a^n(b\mathbf{0} + x) \approx a(a^n x + \sum_{b \in A \setminus \{a\}} a^n(b\mathbf{0} + x)) \ .$$

The right-hand side of the equation above does not have a summand $a^{n+1}x$, so the property of having a summand $a^{n+1}x$ is not preserved. Note that the right-hand side still does have a summand of the form av such that $a^n x \precsim_{\mathrm{FT}} v$ (take $v = (a^n x + \sum_{b \in A \setminus \{a\}} a^n(b\mathbf{0} + x))$). We shall be able to show that if the equation $t \approx u$ is derivable from a collection of sound equations of terms with a depth $\leq n$, then it satisfies the following property P_n^{FT}:

> If $t, u \precsim_{\mathrm{FT}} a(a^n x + x) + a\sum_{b \in A \setminus \{a\}} a^n(b\mathbf{0} + x)$, then t has a summand at' such that $a^n x \precsim_{\mathrm{FT}} t'$, then u has a summand au' such that $a^n x \precsim_{\mathrm{FT}} u'$.

In Lemma 10 we shall first establish that a substitution instance of a sound equation of terms with a depth $\leq n$ satisfies P_n^{FT}. Then, in Proposition 11, we prove that P_n^{FT} is preserved in derivations from a collection of sound equations of depth $\leq n$. Finally, we shall conclude that the family of equations e_n ($n \geq 1$) obstructs a finite basis, because the left-hand side has the summand $a^{n+1}x$, while the right-hand side does *not* have a summand au' with $a^{n+1}x \precsim_{\mathrm{FT}} au'$.

Lemma 10 *Suppose that $t \simeq_{\mathrm{FT}} u$, let $n \geq 1$ be a natural number greater than or equal to the depth of t and u, and suppose*

$$\sigma(t), \sigma(u) \precsim_{\mathrm{FT}} a(a^n x + x) + a \sum_{b \in A \setminus \{a\}} a^n(b\mathbf{0} + x) \ . \qquad (4)$$

Then $\sigma(t)$ has a summand av such that $a^n x \precsim_{\mathrm{FT}} v$ if and only if $\sigma(u)$ has a summand aw such that $a^n x \precsim_{\mathrm{FT}} w$.

Proof: Clearly, by symmetry, it suffices to only consider the implication from left to right. So suppose that $\sigma(t)$ has a summand av such that $a^n x \precsim_{\mathrm{FT}} v$; then there are two cases:

CASE 1: t has a variable summand z and $\sigma(z)$ has av as a summand.

Since $t \simeq_{\mathrm{FT}} u$, by Lemma 3(3), u also has z as summand. Therefore, since $\sigma(z)$ has av as a summand, so does $\sigma(u)$.

CASE 2: t has a summand at' such that $a^n x \precsim_{\mathrm{FT}} \sigma(t')$.

First, we establish that

$$\sigma(t') \xrightarrow{a^n} x \text{ and } var_m(\sigma(t')) = \emptyset \text{ for all } 0 \leq m < n. \tag{5}$$

From the assumption (4) we conclude using Lemmas 3(2,3) that $\mathcal{I}(\sigma(t)) = \{a\}$, $var_0(\sigma(t')), var_n(\sigma(t')) \subseteq \{x\}$ and $var_m(\sigma(t')) = \emptyset$ for all $0 < m < n$. It follows that $a\sigma(t') \precsim_{\mathrm{FT}} \sigma(t)$, and hence

$$a\sigma(t') \precsim_{\mathrm{FT}} a(a^n x + x) + a \sum_{b \in A \setminus \{a\}} a^n(b\mathbf{0} + x) \ . \tag{6}$$

Now, let ρ_1 be a closed substitution with $\rho_1(x) = \mathbf{0}$. Since $a^n\mathbf{0} \precsim_{\mathrm{FT}} \rho_1(\sigma(t'))$, we have $\rho_1(\sigma(t')) \xrightarrow{a^n} \mathbf{0}$. Since $var_n(\sigma(t')) \subseteq \{x\}$, it follows that either $\sigma(t') \xrightarrow{a^n} x$ or $\sigma(t') \xrightarrow{a^n} \mathbf{0}$.

Note that, to establish (5), it remains to prove $\sigma(t') \stackrel{a^n}{\nrightarrow} \mathbf{0}$ and $x \notin var_0(\sigma(t'))$. For this we consider $\sigma(t')$ under another closed substitution ρ_2 that satisfies $\rho_2(x) = c\mathbf{0}$ with c an action distinct from a. Then, according to (6), $a\rho_2(\sigma(t')) \precsim_{\mathrm{FT}} a(a^n c\mathbf{0} + c\mathbf{0}) + a\sum_{b \in A \setminus \{a\}} a^n(b\mathbf{0} + c\mathbf{0})$, and since the closed term at the right-hand side does not exhibit the failure trace

$$\underbrace{\emptyset\, a \cdots \emptyset\, a}_{n+1 \text{ times}} A \ ,$$

we have $\rho_2(\sigma(t')) \stackrel{a^n}{\nrightarrow} \mathbf{0}$, so $\sigma(t') \stackrel{a^n}{\nrightarrow} \mathbf{0}$. Furthermore, since $a^n x \precsim_{\mathrm{FT}} \sigma(t')$, we have $a^n c\mathbf{0} \precsim_{\mathrm{FT}} \rho_2(\sigma(t'))$. So $c \notin \mathcal{I}(\rho_2(\sigma(t')))$, and hence $x \notin var_0(\sigma(t'))$. This completes the proof of (5).

We proceed to prove that u has a summand au' such that

$$\sigma(u') \xrightarrow{a^n} x \text{ and } var_0(\sigma(u')) = \emptyset \ . \tag{7}$$

From (5) and the assumption that $depth(\sigma(t)) \leq n$ it follows that there exist $\ell < n$, a variable y and a term t'' such that $t' \xrightarrow{a^\ell} y + t''$ and $\sigma(y) \xrightarrow{a^{n-\ell}} x$.

Define Z as the set of variables z such that $\sigma(z)$ has x as a summand, i.e.,

$$Z = \{z \in V \mid x \in var_0(\sigma(z))\} \ .$$

Since y has an occurrence in t' at depth $\ell < n$, it follows from (5) that $x \notin var_0(\sigma(y))$, so $y \notin Z$. Therefore, we can define a closed substitution ρ_3 by

$$\rho_3(z) = \begin{cases} a^{n+1}\mathbf{0} & \text{if } z = y \\ c\mathbf{0} & \text{if } z \in Z \\ \mathbf{0} & \text{otherwise.} \end{cases}$$

where c is again an action distinct from a.

Since $t \xrightarrow{a} t' \xrightarrow{a^\ell} y + t''$, $\rho_3(y) \xrightarrow{a^{n+1}} \mathbf{0}$, $c \notin \mathcal{I}(t')$, and $x \notin var_0(\sigma(t'))$ implies $var_0(t') \cap Z = \emptyset$, $\rho_3(t)$ admits the failure trace

$$\emptyset\, a\, \{c\}\, \underbrace{a\, \emptyset \cdots a\, \emptyset}_{\ell+n \text{ times}}\, a\, \{a\} \enspace ,$$

which by the assumption $t \simeq_{\rm FT} u$ is then also a failure trace of $\rho_3(u)$. Since $depth(u') < n$, and in view of the definition of ρ_3, this clearly means that u has a summand au' such that $c \notin \mathcal{I}(\rho_3(u'))$ and $u' \xrightarrow{a^\ell} y + u''$ for some term u''. Since $\sigma(y) \xrightarrow{a^{n-\ell}} x$, it follows that $\sigma(u') \xrightarrow{a^n} x$. Moreover, from $c \notin \mathcal{I}(\rho_3(u'))$ it follows that $var_0(u') \cap Z = \emptyset$, and hence $x \notin var_0(\sigma(u'))$. So we have now established (7).

From the assumption (4) we conclude, by Lemmas 3(2,3), that $act_m(\sigma(u')) \subseteq \{a\}$ for all $0 \leq m < n$ and that $var_m(\sigma(u')) = \emptyset$ for all $0 < m < n$, and (7) adds that $\sigma(u') \xrightarrow{a^n} x$, and $var_0(\sigma(u')) = \emptyset$. These facts together easily imply $a^n x \precsim_{\rm FT} \sigma(u')$. $\Box$

We shall now prove that the property $P_n^{\rm FT}$ holds for every equation derivable from a collection of equations between terms of depth less than or equal to n. By the preceding lemma, it suffices to prove that the transitivity and congruence rules preserve $P_n^{\rm FT}$.

Proposition 11 *Let E be a finite axiomatization over BCCSP that is sound modulo $\simeq_{\rm FT}$, let $n \geq 1$ be a natural number greater than or equal to the depth of any term in E, and suppose $E \vdash t \approx u$ and*

$$t, u \precsim_{\rm FT} a(a^n x + x) + a \sum_{b \in A \setminus \{a\}} a^n(b\mathbf{0} + x) \enspace .$$

Then t has a summand at' such that $a^n x \precsim_{\rm FT} t'$ if and only if u has a summand au' such that $a^n x \precsim_{\rm FT} u'$.

Proof: We prove the proposition by induction on the depth of a normalized derivation of the equation $t \approx u$ from E.

To establish the base case, note that if the derivation of $t \approx u$ consists of an application of the reflexivity rule, then the proposition is immediate, and if there exist terms v and w and a substitution σ such that $\sigma(v) = t$ and $\sigma(w) = u$ and $(v \approx w) \in E$ or $(w \approx v) \in E$, then $v \simeq_{\mathrm{FT}} w$ by the soundness of E, so the proposition follows by Lemma 10.

For the inductive step we distinguish cases according to the last rule applied.

Case 1: the last rule applied is the transitivity rule.

Then there exist a term v and normalized derivations of $t \approx v$ and $v \approx u$. By the soundness of E, $v \simeq_{\mathrm{FT}} u \precsim_{\mathrm{FT}} a(a^n x + x) + a\sum_{b \in A\setminus\{a\}} a^n(b\mathbf{0} + x)$. Hence, by the induction hypothesis, v has a summand av' such that $a^n x \precsim_{\mathrm{FT}} v'$, and therefore, again by induction, u has a summand au' such that $a^n x \precsim_{\mathrm{FT}} u'$.

Case 2: the last rule applied is the congruence rule for a.

Then $t = at'$ and $u = au'$ for some terms t' and u', and there exists a normal derivation of $t' \approx u'$. Since t consists of a single summand at', $a^n x \precsim_{\mathrm{FT}} t'$. So by the soundness of E, $a^n x \precsim_{\mathrm{FT}} u'$.

Case 3: the last rule applied is the congruence rule for $+$.

Then $t = t_1 + t_2$ and $u = u_1 + u_2$ for some terms t_1, t_2, u_1 and u_2, and there exist normal derivations of $t_1 \approx u_1$ and $t_2 \approx u_2$. Since t has a summand at' with $a^n x \precsim_{\mathrm{FT}} t'$, so does either t_1 or t_2. Assume, without loss of generality, that t_1 has a summand at' such that $a^n x \precsim_{\mathrm{FT}} t'$. Since $\mathcal{I}(u) = \{a\}$, clearly $u_1 \precsim_{\mathrm{FT}} u \precsim_{\mathrm{FT}} a(a^n x + x) + a\sum_{b \in A\setminus\{a\}} a^n(b\mathbf{0} + x)$. So by the induction hypothesis u_1, and hence u, has a summand au' with $a^n x \precsim_{\mathrm{FT}} u'$. □

Now we are in a position to prove the main theorem of this section.

Theorem 12 *Let $1 < |A| < \infty$. Then the equational theory of BCCSP modulo $\simeq_{\mathrm{FT}}$ is not finitely based.*

Proof: Let E be a finite axiomatization over BCCSP that is sound modulo $\simeq_{\mathrm{FT}}$. Let $n \geq 1$ be greater than or equal to the depth of any term in E.

Note that $a(a^n x + x) + a\sum_{b \in A\setminus\{a\}} a^n(b\mathbf{0} + x)$ does not contain a summand au' such that $a^n x \precsim_{\mathrm{FT}} u'$. So according to Proposition 11, the equation

$$a^{n+1}x + a(a^n x + x) + a \sum_{b \in A\setminus\{a\}} a^n(b\mathbf{0} + x) \approx a(a^n x + x) + a \sum_{b \in A\setminus\{a\}} a^n(b\mathbf{0} + x) \ ,$$

which is sound modulo $\simeq_{\mathrm{FT}}$, cannot be derived from E. It follows that every finite collection of equations that are sound modulo $\simeq_{\rm FT}$ is necessarily incomplete, and hence the equational theory of BCCSP modulo $\simeq_{\rm FT}$ is not finitely based. □

5 From Ready Pairs to Possible Worlds

In this section we consider all congruences $\simeq$ that finer than or as fine as ready equivalence and coarser than or coarse as possible worlds equivalence (i.e., $\simeq_{\rm PW} \subseteq \simeq \subseteq \simeq_{\rm R}$). We prove that if $1 < |A| < \infty$, then no finite sound and ground-complete axiomatization for BCCSP modulo $\simeq$ is ω-complete.

In [11,12], van Glabbeek gave a finite axiomatization that is sound and ground-complete for BCCSP modulo $\simeq_{\rm R}$. It consists of axioms A1-4 together with

$$\text{R} \quad a(bx + z_1) + a(by + z_2) \approx a(bx + by + z_1) + a(by + z_2)$$

where a, b range over A. In case A is infinite, Groote [13] proved with his technique of inverted substitutions that this axiomatization is ω-complete. So in that case, ready equivalence is finitely based over BCCSP.

Note that $\simeq_{\rm PW} \subseteq \simeq_{\rm RT} \subseteq \simeq_{\rm R}$. Blom, Fokkink and Nain [5] proved that if $|A| = \infty$, then no finite axiomatization is sound and ground-complete for BCCSP modulo $\simeq_{\rm RT}$. They also proved that if $|A| < \infty$, then a finite sound and ground-complete axiomatization for BCCSP modulo $\simeq_{\rm RT}$ is obtained by extending axioms A1-4 with

$$\text{RT} \quad a(\textstyle\sum_{i=1}^{|A|}(b_i x_i + b_i y_i) + z) \approx a(\sum_{i=1}^{|A|} b_i x_i + z) + a(\sum_{i=1}^{|A|} b_i y_i + z)$$

where $a, b_1, \ldots, b_{|A|}$ range over A.

In [11,12], van Glabbeek gave a finite axiomatization that is sound and ground-complete for BCCSP modulo $\simeq_{\rm PW}$. It consists of axioms A1-4 together with

$$\text{PW} \quad a(bx + by + z) \approx a(bx + z) + a(by + z)$$

where a, b range over A. If A is infinite, then Groote's technique of inverted substitutions can be applied in a straightforward fashion to prove that this axiomatization is ω-complete. So in that case, possible worlds equivalence is finitely based over BCCSP.

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

$$a(x_1 + \cdots + x_n) + \sum_{i=1}^{n} a(x_1 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_n)$$

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

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

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 ρ with $\rho(x_i) = x_i + x_n$ 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 then moved to a more complicated family of equations (see Definition 19), 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 $\simeq_{\mathrm{PW}}$, such a cancellation is not possible for the new family of equations (see Lemma 21). We prove that they do obstruct a finite ω-complete axiomatization (see Theorem 24).

5.1 Cover equations

We introduce a class of *cover equations* (cf. Section 2.3), and show that they are sound modulo $\simeq_{\mathrm{PW}}$. We prove that each equation that involves terms of depth ≤ 1 and that is sound modulo $\simeq_{\mathrm{R}}$ 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 Proposition 18).

Definition 13 *A term $\sum_{i\in I} aY_i$ is a* cover *of a term aX if:*

(1) $\forall Z \subseteq X$ with $|Z| \leq |A| - 1$, $\exists i{\in}I$ $(Z \subseteq Y_i \subseteq X)$; 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: $\sum_{i=1}^{n} a(x_1 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_n) \trianglerighteq a(x_1 + \cdots + x_n)$ for $n > |A|$. Hence the equations that were given at the start of this section are cover equations.

If $|X| \leq |A| - 1$, then by Definition 13(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 19).

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

Lemma 14 *If* $\sum_{i\in I} aY_i \trianglerighteq aX$, *then* $aX + \sum_{i\in I} aY_i \simeq_{\mathrm{PW}} \sum_{i\in I} aY_i$.

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

Case 1: $|\mathcal{I}(\rho(X))| \leq |A| - 1$.

By Definition 13(1), $Z \subseteq Y_{i_0} \subseteq X$ for some $i_0 \in I$. Then clearly p is a possible world of $\rho(Y_{i_0})$. Thus ap is a possible world of $\rho(\sum_{i\in I} aY_i)$.

Case 2: $|\mathcal{I}(\rho(X))| = |A|$.

By Definition 13(2), $Z \subseteq Y_{i_0}$ for some $i_0 \in I$. Then $\mathcal{I}(\rho(Z)) \subseteq \mathcal{I}(\rho(Y_{i_0}))$, and hence, since $\mathcal{I}(\rho(Z)) = A$, it follows that $\mathcal{I}(\rho(Y_{i_0})) = \mathcal{I}(\rho(Z))$. From $Z \subseteq Y_{i_0}$ and $\mathcal{I}(\rho(Y_{i_0})) = \mathcal{I}(\rho(Z))$ we conclude that every possible world of Z is a possible word of Y_{i_0}. Since p is a possible world of $\rho(Z)$, it follows that p is a possible world of $\rho(Y_{i_0})$. Thus ap is a possible world of $\rho(\sum_{i\in I} aY_i)$. $\square$

We proceed to prove that each sound equation $t \approx u$ modulo $\simeq_{\mathrm{R}}$ 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 Proposition 18). First we present some notations.

Definition 15 $C^k = \{aX + \sum_{i\in I} aY_i \approx \sum_{i\in I} aY_i \mid \sum_{i\in I} aY_i \trianglerighteq aX \wedge |I| \leq k\}$ *for* $k \geq 0$.

Definition 16 R_1 *denotes the set of equations* $t \approx u$ *with depth*$(t) =$ *depth*$(u) \leq 1$ *that are sound modulo* $\simeq_{\mathrm{R}}$.

Let $S(t)$ denote the number of distinct summands (modulo A1-4) unequal to $\mathbf{0}$ *of term t. For $k \geq 0$,*

$$R_1^k = \{t \approx u \in R_1 \mid S(t) \leq k \wedge S(u) \leq k\}.$$

In the remainder of this section we assume that $A = \{a_1, \ldots, a_{|A|}\}$.

We present part of the proof of Proposition 18 as a separate lemma, as this lemma will be reused in the proof of Lemma 22.

Lemma 17 *If $t \approx u \in R_1$, then t and u contain exactly the same summands aX with $|X| \leq |A| - 1$.*

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

By symmetry, each summand aX with $|X| \leq |A| - 1$ of u is also a summand of t. $\square$

Proposition 18 $C^k \vdash R_1^k$ *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.

CASE 1: $Z = \{z_1, \ldots, z_k\} \subseteq X$ with $k \leq |A| - 1$.

We define $\rho(z_i) = a_i\mathbf{0}$ for $i = 1, \ldots, k$, $\rho(x) = \mathbf{0}$ for $x \in X \setminus Z$, and $\rho(y) = a_{|A|}\mathbf{0}$ for $y \notin X$. The ready pair $(a, \{a_1, \ldots, a_k\})$ of $\rho(aX)$ must also be a ready pair of $\rho(u)$. Since $depth(u) \leq 1$, this implies that there is a summand aY of u with $Z \subseteq Y \subseteq X$.

CASE 2: $Z = \{z_1, \ldots, z_{|A|}\} \subseteq X$.

We define $\rho(z_i) = a_i\mathbf{0}$ for $i = 1, \ldots, |A|$ and $\rho(y) = \mathbf{0}$ for $y \notin Z$. The ready pair (a, A) of $\rho(aX)$ must also be a ready pair of $\rho(u)$. Since $depth(u) \leq 1$, this implies that there is a summand aY of u with $Z \subseteq Y$.

Concluding, in view of Definition 13, $u = u_1 + u_2$ with $u_1 \trianglerighteq aX$. Since $S(u_1) \leq S(u) \leq k$, we have $aX + u_1 \approx u_1 \in C^k$. So $C^k \vdash aX + u \approx u$.

By Lemmas 3(3) and 17, each summand $x \in V$ and aX with $|X| \leq |A| - 1$ 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 $C^k \vdash t \approx t + u \approx u$. $\square$

We now turn our attention to a special kind of cover equation $a_1X_n + \Theta_n \approx \Theta_n$ for $n \geq |A|$, where Θ_n contains $n+1$ summands (see Definition 19 and Lemma 20). If a term u is obtained by eliminating one or more summands from Θ_n, then $a_1X_n + u \not\approx_{\mathrm{R}} u$ (see Lemma 21); moreover, if a summand of a term u is not a summand of $a_1X_n + \Theta_n$, then $\Theta_n \not\approx_{\mathrm{R}} u$ (see Lemma 22). These two facts together imply that $a_1X_n + \Theta_n \approx \Theta_n$ cannot be derived from C^n (see Proposition 23). Propositions 18 and 23 form the corner stones of the proof of Theorem 24, which contains the main result of this section.

Definition 19 *Let $n \geq |A|$. Let $x_1, \ldots, x_n, \hat{x}_{|A|}, \ldots, \hat{x}_n$ be distinct variables. Let $X_{|A|-1}$ and X_n denote $\{x_1, \ldots, x_{|A|-1}\}$ and $\{x_1, \ldots, x_n\}$, respectively. We define that Θ_n denotes the term*

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

Lemma 20 *$\Theta_n \trianglerighteq a_1X_n$ for $n \geq |A|$.*

Proof: Let $Z \subseteq X_n$ with $|Z| \leq |A| - 1$. We need to find a summand a_1Y of Θ_n with $Z \subseteq Y \subseteq X_n$. We distinguish two cases. On the one hand, if $Z \subseteq X_{|A|-1}$, then $Z \subseteq X_{|A|-1} \subseteq X_n$. On the other hand, if $Z \not\subseteq X_{|A|-1}$, then $Z \subseteq X_n \setminus \{x_i\} \subseteq X_n$ for some $1 \leq i \leq |A| - 1$.

Let $Z \subseteq X_n$ with $|Z| = |A|$. We need to find a summand a_1Y of Θ_n with $Z \subseteq Y$. Again there are two cases. On the one hand, if $X_{|A|-1} \subset Z$, then $Z \subseteq X_{|A|-1} \cup \{x_i, \hat{x}_i\}$ for some $|A| \leq i \leq n$. On the other hand, if $X_{|A|-1} \not\subset Z$, then then $Z \subseteq X_n \setminus \{x_i\}$ for some $1 \leq i \leq |A| - 1$. □

Lemma 21 *Let $n \geq |A|$. If the summands of u are a proper subset of the summands of Θ_n, then $a_1X_n + u \not\approx_{\mathrm{R}} u$.*

Proof: Suppose that all summands of u are summands of Θ_n, but that some summand a_1Y of Θ_n is not a summand of u. We consider the three possible forms of Y, and for each case give a closed substitution ρ such that some ready pair of $\rho(a_1X_n)$ is not a ready pair of $\rho(u)$.

CASE 1: $Y = X_{|A|-1}$.

We define $\rho(x_i) = a_i\mathbf{0}$ for $i = 1, \ldots, |A| - 1$, $\rho(x_i) = \mathbf{0}$ for $i = |A|, \ldots, n$, and $\rho(y) = a_{|A|}\mathbf{0}$ for $y \notin X_n$. Then the ready pair $(a_1, \{a_1, \ldots, a_{|A|-1}\})$ of $\rho(a_1X_n)$ is not a ready pair of $\rho(u)$.

CASE 2: $Y = X_n \setminus \{x_{i_0}\}$ for some $1 \leq i_0 \leq |A| - 1$.

We define $\rho(x_i) = a_i\mathbf{0}$ for $i = 1, \ldots, i_0-1, i_0+1, \ldots, |A|$, $\rho(x_i) = \mathbf{0}$ for $i = i_0$ and $i = |A|+1, \ldots, n$, and $\rho(y) = a_{i_0}\mathbf{0}$ for $y \notin X_n$. Then the ready pair $(a_1, \{a_1, \ldots, a_{i_0-1}, a_{i_0+1}, \ldots, a_{|A|}\})$ of $\rho(a_1X_n)$ is not a ready pair of $\rho(u)$.

CASE 3: $Y = X_{|A|-1} \cup \{x_{i_0}, \hat{x}_{i_0}\}$ for some $|A| \leq i_0 \leq n$.

We define $\rho(x_i) = a_i\mathbf{0}$ for $i = 1, \ldots, |A|-1$, $\rho(x_{i_0}) = a_{|A|}\mathbf{0}$, and $\rho(y) = \mathbf{0}$ for $y \notin X_{|A|-1} \cup \{x_{i_0}\}$. Then the ready pair $(a_1, \{a_1, \ldots, a_{|A|}\})$ of $\rho(a_1X_n)$ is not a ready pair of $\rho(u)$. $\square$

Lemma 22 *Let $n \geq |A|$. If $\Theta_n \simeq_{\mathrm{R}} u$, then each summand of u is a summand of $a_1X_n + \Theta_n$.*

Proof: Let $\Theta_n \simeq_{\mathrm{R}} u$. By Lemma 3(1), $\mathit{depth}(u) = 1$. By Lemma 3(3), u does not have summands $x \in V$, so clearly each summand of u is of the form a_1Y. If $|Y| \leq |A|-1$, then by Lemma 17, a_1Y is a summand of Θ_n. Let $|Y| \geq |A|$; we prove that a_1Y is a summand of $a_1X_n + \Theta_n$.

By Lemma 3(3), $Y \subseteq X_n \cup \{\hat{x}_i \mid i{=}|A|, \ldots, n\}$. We distinguish two cases.

CASE 1: $\hat{x}_i \in Y$ for some $|A| \leq i \leq n$.

Suppose, towards a contradiction, that there is a $y \in Y \setminus (X_{|A|-1} \cup \{x_i, \hat{x}_i\})$. We define $\rho(y) = a_1\mathbf{0}$, $\rho(\hat{x}_i) = a_2\mathbf{0}$, and $\rho(z) = \mathbf{0}$ for $z \notin \{y, \hat{x}_i\}$. The ready pair $(a_1, \{a_1, a_2\})$ of $\rho(a_1Y)$ is not a ready pair of $\rho(\Theta_n)$, contradicting $\Theta_n \simeq_{\mathrm{R}} u$.

Suppose, towards a contradiction, that there is an $x \in (X_{|A|-1} \cup \{x_i, \hat{x}_i\}) \setminus Y$. Note that $\hat{x}_i \in Y$ implies $x \neq \hat{x}_i$. We define $\rho(x) = a_1\mathbf{0}$, $\rho(\hat{x}_i) = a_2\mathbf{0}$, and $\rho(z) = \mathbf{0}$ for $z \notin \{x, \hat{x}_i\}$. The ready pair $(a_1, \{a_2\})$ of $\rho(a_1Y)$ is not a ready pair of $\rho(\Theta_n)$, contradicting $\Theta_n \simeq_{\mathrm{R}} u$.

Hence, $Y = X_{|A|-1} \cup \{x_i, \hat{x}_i\}$.

CASE 2: $Y \subseteq X_n$.

Since $|Y| \geq |A|$, there is a $Z = \{z_1, \ldots, z_{|A|-1}\} \subseteq Y$ with $Z \not\subseteq X_{|A|-1}$. We define $\rho(z_i) = a_i\mathbf{0}$ for $i = 1, \ldots, |A|-1$, $\rho(y) = \mathbf{0}$ for $y \in Y \setminus Z$, and $\rho(z) = a_{|A|}\mathbf{0}$ for $z \notin Y$. The ready pair $(a_1, \{a_1, \ldots, a_{|A|-1}\})$ of $\rho(a_1Y)$ must be a ready pair of $\rho(\Theta_n)$, which implies that there is a summand a_1Y' of Θ_n with $Z \subseteq Y' \subseteq Y$. Since $Z \not\subseteq X_{|A|-1}$ and $Y \subseteq X_n$, it follows that $Y' = X_n \setminus \{x_{i_0}\}$ for some $1 \leq i_0 \leq |A|-1$. Hence, either $Y = X_n$ or $Y = X_n \setminus \{x_{i_0}\}$.

Concluding, each summand of u is a summand of $a_1X_n + \Theta_n$. $\square$

The following example shows that Lemma 22 would fail if $|A| = 1$.

Example: Let $|A| = 1$ and $n = 1$. Note that $\Theta_1 = a_1\mathbf{0} + a_1(x_1 + \hat{x}_1)$ and $a_1X_1 = a_1x_1$. Since $|A| = 1$, $a_1\mathbf{0} + a_1(x_1 + \hat{x}_1) \simeq_{\rm R} a_1\hat{x}_1 + a_1\mathbf{0} + a_1(x_1 + \hat{x}_1)$. However, $a_1\hat{x}_1$ is not a summand of $a_1x_1 + a_1\mathbf{0} + a_1(x_1 + \hat{x}_1)$.

Proposition 23 *$C^n \nvdash a_1X_n + \Theta_n \approx \Theta_n$ for $n \geq |A|$.*

Proof: Suppose, towards a contradiction, that there is a derivation of $a_1X_n + \Theta_n \approx \Theta_n$ using only equations in C^n: $a_1X_n + \Theta_n = u_0 \approx u_1 \approx \cdots \approx u_j = \Theta_n$ for some $j \geq 1$. By Lemma 3(1), $u_1, \ldots, u_j$ have depth 1. Since $u_0 = a_1X_n + \Theta_n$, $u_j = \Theta_n$, 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 $\Theta_n \simeq_{\rm R} u_i$, Lemma 22 implies that all summands of u_i are summands of Θ_n. Since $a_1X_n + u_i \simeq_{\rm R} u_i$, Lemma 21 implies that $u_i = \Theta_n$. Hence, $a_1X_n + \Theta_n \approx \Theta_n$ can be derived using a single application of an equation $a_1Y + v \approx v \in C^n$. Then $\sigma(Y) = X_n$ and $\sigma(v) + w = \Theta_n$ for some substitution σ and term w. Since $a_1X_n + \sigma(v) \simeq_{\rm R} \sigma(v)$ and $\sigma(v) + w = \Theta_n$, Lemma 21 implies that $\sigma(v) = \Theta_n$. 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 $S(\sigma(v)) = S(\Theta_n) = n + 1$. Concluding, $C^n \nvdash a_1X_n + \Theta_n \approx \Theta_n$. □

Theorem 24 *Let $1 < |A| < \infty$. Let $\simeq$ be a congruence that is included in ready equivalence and includes possible worlds equivalence. Then the equational theory of BCCSP modulo $\simeq$ is not finitely based.*

Proof: Let E be a finite axiomatization that is sound and ground-complete for BCCSP modulo a congruence $\simeq$ that is included in ready equivalence and includes possible worlds equivalence. Suppose, towards a contradiction, that E is ω-complete. By Lemmas 20 and 14, $a_1X_n + \Theta_n \approx \Theta_n$ for $n \geq |A|$ is sound modulo $\simeq_{\rm PW}$, so also modulo $\simeq$. Then these equations can be derived from E. Let E_1 denote the equations in E of depth ≤ 1. By Lemma 3(1), $E_1 \vdash a_1X_n + \Theta_n \approx \Theta_n$ for $n \geq |A|$.

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 $\simeq$, so also modulo $\simeq_{\rm R}$, it follows that $E_1 \subseteq R_1^n$. By Proposition 18, $C^n \vdash E_1$. This implies that $C^n \vdash a_1X_n + \Theta_n \approx \Theta_n$, which contradicts Proposition 23.

Concluding, E is not ω-complete. □

6 Simulation

In this section we consider simulation equivalence $\simeq_{\rm S}$. In [11,12], van Glabbeek gave a finite axiomatization that is sound and ground-complete for BCCSP modulo $\simeq_{\mathrm{S}}$. It consists of axioms A1-4 together with

$$\mathrm{S} \quad a(x+y) \approx a(x+y) + ax \ ,$$

where a ranges over A. In case A is infinite, Groote's technique of inverted substitutions from [13] can be applied in a straightforward fashion to prove that van Glabbeek's axiomatization is ω-complete; see [6].

An infinite supply of actions is crucial in this particular application of the inverted substitutions technique, for we shall prove below that the equational theory of BCCSP modulo $\simeq_{\mathrm{S}}$ does not have a finite basis if $1 < |A| < \infty$. The corner stone for this negative result is the following infinite family of equations:

$$a(x+\Psi_n) + \sum_{\theta \in A^n} a(x+\Psi_n^\theta) + a\Phi_n \approx \sum_{\theta \in A^n} a(x+\Psi_n^\theta) + a\Phi_n \qquad (n \geq 0) \ .$$

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:

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

$$\Psi_n^\theta = \textstyle\sum_{b_1 \cdots b_n \in A^n \setminus \{\theta\}} b_1 \cdots b_n \mathbf{0} \qquad \text{for } \theta \in A^n \ .$$

For any closed term p with $\mathit{depth}(p) \leq n$, clearly $p \precsim_{\mathrm{S}} \Phi_n$. So in particular, $\Psi_n \precsim_{\mathrm{S}} \Phi_n$.

It is not hard to see that the equations above are sound modulo $\simeq_{\mathrm{S}}$. The idea is that, given a closed substitution ρ, either $\mathit{depth}(\rho(x)) < n$, in which case $a(\rho(x)+\Psi_n)$ is simulated by $a\Phi_n$. Or some $b_1 \cdots b_n \in A^n$ is a trace of $\rho(x)$, in which case $a(\rho(x)+\Psi_n)$ is simulated by $a(\rho(x)+\Psi_n^{b_1 \cdots b_n})$.

We shall prove below that $\simeq_{\mathrm{S}}$ is not finitely based, using the proof-theoretic technique, by showing that whenever an equation $t \approx u$ is derivable from a set of sound axioms of depth $\leq n$, then it satisfies the following property P_n^{S}:

> if $t, u \precsim_{\mathrm{S}} \sum_{\theta \in A^n} a(x+\Psi_n^\theta) + a\Phi_n$, then t has a summand similar to $a(x+\Psi_n)$ if and only if u has a summand similar to $a(x+\Psi_n)$.

We shall first establish in Lemma 26 that an equation satisfies P_n^{S} if it is a substitution instance of a sound equation of terms with a depth $\leq n$. Then, in

Proposition 27, we prove, using Lemma 26, that P_n^{S} holds for every equation derivable from a collection of sound equations E, provided that the depth of the terms in E does not exceed n. From the proposition we can directly infer that the infinite family of equations above obstructs a finite basis, because the left-hand side contains a summand similar to $a(x + \Psi_n)$, while the right-hand side does not.

The following lemma constitutes an important step in the proof that P_n^{S} is preserved by substitution instances of sound equations of terms with a depth $\leq n$.

Lemma 25 *If* $a(x + \Psi_n) \precsim_S at \precsim_S \sum_{\theta\in A^n} a(x + \Psi_n^\theta) + a\Phi_n$*, then* $at \simeq_S a(x + \Psi_n)$.

Proof: Since $x + \Psi_n \precsim_{\mathrm{S}} t$, by Lemma 3(3), x is a summand of t. Clearly, there exists a term t' that does not have x as a summand such that $t = x + t'$ (modulo A3). Since $a(x + t') \precsim_{\mathrm{S}} \sum_{\theta\in A^n} a(x + \Psi_n^\theta) + a\Phi_n$, by Lemma 3(3), t' is a closed term.

We prove that $t' \precsim_{\mathrm{S}} \Psi_n$. Consider a closed substitution ρ with $\rho(x) = a^{n+1}\mathbf{0}$. Since $a(\rho(x) + t') \precsim_{\mathrm{S}} \sum_{\theta\in A^n} a(\rho(x) + \Psi_n^\theta) + a\Phi_n$ and clearly $\rho(x) + t' \not\precsim_{\mathrm{S}} \Phi_n$, it follows that $\rho(x) + t' \precsim_{\mathrm{S}} \rho(x) + \Psi_n^\theta$ for some $\theta \in A^n$. Hence $t' \precsim_{\mathrm{S}} a^{n+1}\mathbf{0} + \Psi_n^\theta$. Since $at \precsim_{\mathrm{S}} \sum_{\theta\in A^n} a(x + \Psi_n^\theta) + a\Phi_n$, by Lemma 3(1), $\mathit{depth}(t') \leq \mathit{depth}(t) \leq n$. So $t' \precsim_{\mathrm{S}} a^n\mathbf{0} + \Psi_n^\theta \precsim_{\mathrm{S}} \Psi_n$.

Then $at = a(x + t') \precsim_{\mathrm{S}} a(x + \Psi_n)$, and, by assumption, $a(x + \Psi_n) \precsim_{\mathrm{S}} at$, so $at \simeq_{\mathrm{S}} a(x + \Psi_n)$. $\square$

We shall now establish that substitution instances of sound equations of depth $\leq n$ satisfy P_n^{S}.

Lemma 26 *Suppose* $t \simeq_S u$*, let* $n > 1$ *be a natural number greater than or equal to the depth of* t *and* u*, and suppose* $\sigma(t), \sigma(u) \precsim_S \sum_{\theta\in A^n} a(x+\Psi_n^\theta)+a\Phi_n$*. Then* $\sigma(t)$ *has a summand similar to* $a(x + \Psi_n)$ *if and only if* $\sigma(u)$ *has a summand similar to* $a(x + \Psi_n)$*.*

Proof: Clearly, by symmetry, it suffices to only consider the implication from left to right. So suppose that $\sigma(t)$ has a summand similar to $a(x + \Psi_n)$; then there are two cases:

Case 1: t has a variable summand z and $\sigma(z)$ has a summand similar to $a(x + \Psi_n)$.

Since $t \simeq_{\mathrm{S}} u$, by Lemma 3(3), u also has z as summand. Since $\sigma(z)$ has a summand similar to $a(x + \Psi_n)$, the same holds for $\sigma(u)$.

Case 2: t has a summand at' and $\sigma(at') \simeq_{\mathrm{S}} a(x + \Psi_n)$.

Note that from $\sigma(t') \simeq_S x + \Psi_n$ it follows by Lemma 3(3) that x is a summand of $\sigma(t')$, and this means that t' has a variable summand y with x a summand of $\sigma(y)$.

The following claim constitutes a crucial step in the remainder of the proof for this case.

Claim The term u has a summand au' such that, for every $m \geq 0$ and for every variable z, if $t' \xrightarrow{a_1 \cdots a_m} z + v$ for some term v, then $u' \xrightarrow{a_1 \cdots a_m} z + w$ for some term w.

Proof of Claim: We consider the terms t and u under a special closed substitution ρ, that we now proceed to define. Let a and b be distinct actions, and let $\ulcorner . \urcorner : V \to \mathbb{Z}_{>0}$ be an injection (which exists since V is countable); then ρ is defined by

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

From the assumption that $t \simeq_S u$, it follows that $\rho(t) \simeq_S \rho(u)$.

Since $\rho(t) \xrightarrow{a} \rho(t')$, there exists a closed term p such that $\rho(u) \xrightarrow{a} p$ and $\rho(t') \precsim_S p$.

To establish that u has a summand au' such that $\rho(t') \precsim_S \rho(u')$, we argue that u cannot have a variable summand z such that $\rho(z) \xrightarrow{a} p$. Recall that t' has a variable summand y; since $\rho(y) = a^{\ulcorner y \urcorner \cdot n} b\mathbf{0}$ and $\rho(t') \precsim_S p$, it follows that b has an occurrence at depth $\ulcorner y \urcorner \cdot n$ in p. Now assume towards a contradiction that z is a variable summand of u such that $\rho(z) \xrightarrow{a} p$. Then $p = a^{\ulcorner z \urcorner \cdot n - 1} b\mathbf{0}$, which, since clearly $\ulcorner y \urcorner \cdot n \neq \ulcorner z \urcorner \cdot n - 1$, contradicts that b occurs in p at depth $\ulcorner y \urcorner \cdot n$ in p. So u has a summand au' such that $\rho(t') \precsim_S \rho(u')$.

Now suppose that $t' \xrightarrow{a_1 \cdots a_m} z + v$ for some term v. Then, since $\rho(t') \precsim_S \rho(u')$, there exists a closed term q such that $\rho(u') \xrightarrow{a_1 \cdots a_m} q$ and $\rho(z+v) \precsim_S q$.

We shall now first prove that there exists u'' such that $u' \xrightarrow{a_1 \cdots a_m} u''$ and $\rho(u'') = q$. Assume towards a contradiction that there is no such u''. Then clearly there exist $\ell < m$, a variable z', and a term u''' such that $u' \xrightarrow{a_1 \cdots a_\ell} z' + u'''$ and $\rho(z') \xrightarrow{a_{\ell+1} \cdots a_m} q$. Since $\rho(z') = a^{\ulcorner z' \urcorner \cdot n} b\mathbf{0}$, it follows that $q = a^{\ulcorner z' \urcorner \cdot n - (m-\ell)} b\mathbf{0}$, and hence the single occurrence of b in p is at depth $\ulcorner z' \urcorner \cdot n - (m - \ell)$. Since $0 < m - \ell < n$, it follows that b does not occur at depth $\ulcorner z \urcorner \cdot n$ in q; this contradicts $\rho(z + v) \precsim_S q$.

So there exists u'' such that $u \xrightarrow{a_1 \cdots a_m} u''$ and $\rho(u'') = q$. Since $\rho(z+v) \precsim_S q = \rho(u'')$ and $\rho(z) = a^{\ulcorner z \urcorner \cdot n} b\mathbf{0}$, $\rho(u'') \xrightarrow{a^{\ulcorner z \urcorner \cdot n}} b\mathbf{0}$. Hence, since $\mathit{depth}(u'') < n$ and $\ulcorner z \urcorner > 0$, there exists a variable z', a term w, and $\ell < n$ such that $u'' \xrightarrow{a^\ell} z' + w$ and $\rho(z') \xrightarrow{a^{\ulcorner z \urcorner \cdot n - \ell}} b\mathbf{0}$. From the definition of ρ it is clear that $\ulcorner z \urcorner \cdot n - \ell = \ulcorner z' \urcorner \cdot n$. Since $\ell \leq \mathit{depth}(u'') < n$, it follows that $\ell = 0$, so $\ulcorner z' \urcorner = \ulcorner z \urcorner$, and hence, since $\ulcorner . \urcorner$ is an injection, $z' = z$. We have established that $u'' = z + w$, and thereby the proof of the claim is complete.

Now consider any $a_1 \cdots a_n \in A^n$. Since $\Psi_n \precsim_S \sigma(t')$ and $\mathit{depth}(t') < n$, there exist $0 \leq m < n$, a variable z and a term v such that $t' \xrightarrow{a_1 \cdots a_m} z + v$ and $a_{m+1} \cdots a_n$ a trace of $\sigma(z)$. By our claim above, $u' \xrightarrow{a_1 \cdots a_m} z + w$ for some term w. Since $a_{m+1} \cdots a_n$ is a trace of $\sigma(z)$, it follows that $a_1 \cdots a_n$ is a trace of $\sigma(u')$. This holds for all $a_1 \cdots a_n \in A^n$, so $\Psi_n \precsim_{\rm S} \sigma(u')$.

Furthermore, recall that y is a summand of t', and that x is a summand of $\sigma(y)$. Since $t' \xrightarrow{\lambda} t'$ (with λ the empty sequence of actions), by our claim it follows that $u' \xrightarrow{\lambda} u + w$ for some term w. So y is a summand of u', and hence x is a summand of $\sigma(u')$.

We conclude that $x + \Psi_n \precsim_{\rm S} \sigma(u')$, and hence $a(x + \Psi_n) \precsim_{\rm S} a\sigma(u')$. From the assumption of the lemma that $\sigma(u) \precsim_{\rm S} \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$ it follows that $a\sigma(u') \precsim_{\rm S} \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$. So, by Lemma 25, $a\sigma(u') \simeq_{\rm S} a(x + \Psi_n)$. □

We shall now prove that $P_n^{\rm S}$ holds for every equation derivable from a collection of equations between terms of depth less than or equal to n. By the preceding lemma, it only remains to prove that the transitivity and congruence rules preserve $P_n^{\rm S}$.

Proposition 27 *Let E be a finite axiomatization over BCCSP that is sound modulo $\simeq_S$, let n be a natural number greater than the depth of any term in E, and suppose $E \vdash t \approx u$ and $t, u \precsim_S \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$. Then t has a summand similar to $a(x + \Psi_n)$ if and only if u has a summand similar to $a(x + \Psi_n)$.*

Proof: We prove the proposition by induction on the depth of a normalized derivation of the equation $t \approx u$ from E.

To establish the base case, note that if the derivation of $t \approx u$ consists of an application of the reflexivity rule, then the proposition is immediate, and if there exist terms v and w and a substitution σ such that $\sigma(v) = t$, $\sigma(w) = u$, and $(v \approx w) \in E$ or $(w \approx v) \in E$, then $v \simeq_{\rm S} w$ by the soundness of E, so the proposition follows from Lemma 26.

For the inductive step we distinguish cases according to the last rule applied.

CASE 1: the last rule applied is the transitivity rule.

Then there exist a term v and normalized derivations of $t \approx v$ and $v \approx u$. By the soundness of E, $v \simeq_{\rm S} u \precsim_{\rm S} \sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$. So, by the induction hypothesis, v has a summand similar to $a(x + \Psi_n)$, and hence, again by the induction hypothesis, u has a summand similar to $a(x + \Psi_n)$.

CASE 2: the last rule applied is the congruence rule for a.

Then $t = at'$ and $u = au'$ for some terms t' and u', and there exists a normal derivation of $t' \approx u'$. Since t consists of a single summand, $at' \simeq_S a(x+\Psi_n)$. So, by the soundness of E, $u = au' \simeq_S a(x+\Psi_n)$.

CASE 3: the last rule applied is the congruence rule for $+$.

Then $t = t_1 + t_2$ and $u = u_1 + u_2$ for some terms t_1, t_2, u_1 and u_2, and there exist normal derivations of $t_1 \approx u_1$ and $t_2 \approx u_2$. Since t has a summand similar to $a(x+\Psi_n)$, so does either t_1 or t_2. Assume, without loss of generality, that t_1 has a summand completed similar to $a(x+\Psi_n)$. Then clearly $\mathcal{I}(t_1) = \mathcal{I}(u_1) = \{a\}$, so $t_1, u_1 \precsim_S t, u \precsim_S \sum_{\theta \in A^n} a(x+\Psi_n^\theta) + a\Phi_n$. By the induction hypothesis, it follows that u_1, and hence u, has a summand similar to $a(x+\Psi_n)$. □

Now we are in a position to prove the main theorem of this section.

Theorem 28 *Let $1 < |A| < \infty$. Then the equational theory of BCCSP modulo $\simeq_S$ is not finitely based.*

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

Note that $\sum_{\theta \in A^n} a(x+\Psi_n^\theta) + a\Phi_n$ does not contain a summand similar to $a(x+\Psi_n)$. So according to Proposition 27, 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 $\simeq_S$, cannot be derived from E. It follows that every finite collection of equations that are sound modulo $\simeq_S$ is necessarily incomplete, and hence the equational theory of BCCSP modulo $\simeq_S$ is not finitely based. □

7 Completed Simulation

In this section we consider completed simulation equivalence $\simeq_{CS}$. In [11,12], van Glabbeek gave a finite axiomatization that is sound and ground-complete for BCCSP modulo $\simeq_{CS}$. It consists of axioms A1-4 together with

$$\text{CS} \quad a(bx+y+z) \approx a(bx+y+z) + a(bx+z)$$

where a, b range over A. We prove that the equational theory of BCCSP modulo $\simeq_{CS}$ does not have a finite basis if $|A| > 1$. (Note that our proof in this section also works in case $|A| = \infty$, whereas all the other proofs of negative results assume $|A| < \infty$). The corner stone for this negative result is the following infinite family of equations:

$$a^n x + a^n\mathbf{0} + a^n(x+y) \approx a^n\mathbf{0} + a^n(x+y) \qquad (n \geq 1) \ .$$

It is not hard to see that these equations are sound modulo $\simeq_{\mathrm{CS}}$. The idea is that, given a closed substitution ρ, either $\rho(x)$ cannot perform any action, in which case $\rho(a^n x)$ is completed simulated by $a^n\mathbf{0}$, or x can perform some action, in which case $\rho(a^n x)$ is completed simulated by $\rho(a^n(x+y))$.

We shall prove that there cannot be a finite sound axiomatization E for BCCSP modulo $\simeq_{\mathrm{CS}}$ from which the equations above can all be derived. We apply the proof-theoretic technique, showing that if the axioms in E have depth smaller than n and the equation $t \approx u$ is derivable from E, then it satisfies the following property P_n^{CS}:

> if $t, u \precsim_{\mathrm{CS}} a^n\mathbf{0} + a^n(x+y)$, then t has a summand completed similar to $a^n x$ if and only if u has a summand completed similar to $a^n x$.

The crucial step is to prove that P_n^{CS} holds for all substitution instances of sound equations of depth $\leq n$ (see Lemma 29). The proof that the transitivity and congruence rules preserve P_n^{CS}, in Proposition 31, will then be analogous to our proof in the previous section that they preserve P_n^{S}. We infer that the infinite family of equations above obstructs a finite basis, by noting that the left-hand sides of the equations have a summand $a^n x$, while the right-hand sides do not.

The following lemma constitutes an crucial step in the proof that substitution instance of sound equations of depth $\leq n$ satisfy P_n^{CS}.

Lemma 29 *If $at \precsim_{\mathrm{CS}} a^n\mathbf{0}+a^n(x+y)$ and $at \xrightarrow{a^n} t'$ with $t' = x$, then $at = a^n x$.*

Proof: We first prove by induction on n that if $at \precsim_{\mathrm{CS}} a^n\mathbf{0} + a^n(x+y)$, then $at = a^n\mathbf{0}$ or $at = a^n x$ or $at = a^n y$ or $at = a^n(x+y)$.

Suppose $n = 1$. Then $\mathcal{I}(t) = \emptyset$ by Lemma 3(2) and $var_0(t) \subseteq \{x, y\}$ by Lemma 3(3), so $t = \mathbf{0}$ or $t = x$ or $t = y$ or $t = x + y$.

Suppose $n > 1$. Then by Lemma 3(2) $\mathcal{I}(t) = \{a\}$ and by Lemma 3(3) $var_0(t) = \emptyset$, so $t = \sum_{i\in I} at_i$ with $I \neq \emptyset$. Clearly, $at_i \precsim_{\mathrm{CS}} a^{n-1}\mathbf{0} + a^{n-1}(x+y)$, so by the induction hypothesis $at_i = a^{n-1}\mathbf{0}$ or $at_i = a^{n-1}x$ or $at_i = a^{n-1}y$ or $at_i = a^{n-1}(x+y)$, for all $i \in I$.

It remains to establish that $at_i = at_j$ for all $i, j \in I$. Suppose, towards a contradiction, that $at_i \neq at_j$ for some $i, j \in I$. Then clearly there exist t_i' and t_j' such that $at_i \xrightarrow{a^{n-1}} t_i'$, $at_j \xrightarrow{a^{n-1}} t_j'$ and $t_i' \neq t_j'$. Modulo symmetry we can distinguish six cases, and in each of them it suffices to provide a closed substitution ρ such that $\rho(at) \not\precsim_{\mathrm{CS}} \rho(a^n\mathbf{0} + a^n(x+y))$.

CASES 1,2,3: $t'_i = \mathbf{0}$ and $t'_j = x$ or $t'_j = y$ or $t'_j = x + y$.

Define ρ such that $\rho(x) \not\simeq_{\mathrm{CS}} \mathbf{0}$ and $\rho(y) \not\simeq_{\mathrm{CS}} \mathbf{0}$. Then $\rho(t) \not\precsim_{\mathrm{CS}} a^{n-1}\mathbf{0}$ (because $\rho(t) \xrightarrow{a^{n-1}} \rho(t'_j) \not\simeq_{\mathrm{CS}} \mathbf{0}$), and $\rho(t) \not\precsim_{\mathrm{CS}} a^{n-1}\rho(x+y)$ (because $\rho(t) \xrightarrow{a^{n-1}} \rho(t_i) \simeq_{\mathrm{CS}} \mathbf{0}$ whereas $\rho(x+y) \not\simeq_{\mathrm{CS}} \mathbf{0}$). So $\rho(at) \not\precsim_{\mathrm{CS}} \rho(a^n\mathbf{0} + a^n(x+y))$.

CASES 4,5: $t'_i = x$ and $t'_j = y$ or $t'_j = x + y$.

Define ρ such that $\rho(x) = \mathbf{0}$ and $\rho(y) \not\simeq_{\mathrm{CS}} \mathbf{0}$. Then $\rho(t) \not\precsim_{\mathrm{CS}} a^{n-1}\mathbf{0}$ (because $\rho(t) \xrightarrow{a^{n-1}} \rho(t'_j) \not\simeq_{\mathrm{CS}} \mathbf{0}$) and $\rho(t) \not\precsim_{\mathrm{CS}} a^{n-1}\rho(x+y)$ (because $\rho(t) \xrightarrow{a^{n-1}} \rho(t'_i) \simeq_{\mathrm{CS}} \mathbf{0}$ and $\rho(x+y) \not\simeq_{\mathrm{CS}} \mathbf{0}$). So $\rho(at) \not\precsim_{\mathrm{CS}} \rho(a^n\mathbf{0} + a^n(x+y))$.

CASE 6: $t'_i = y$ and $t'_j = x + y$.

Define ρ such that $\rho(x) \not\simeq_{\mathrm{CS}} \mathbf{0}$ and $\rho(y) = \mathbf{0}$. Then $\rho(t) \not\precsim_{\mathrm{CS}} a^{n-1}\mathbf{0}$ (because $\rho(t) \xrightarrow{a^{n-1}} \rho(t'_j) \not\simeq_{\mathrm{CS}} \mathbf{0}$) and $\rho(t) \not\precsim_{\mathrm{CS}} a^{n-1}\rho(x+y)$ (because $\rho(t) \xrightarrow{a^{n-1}} \rho(t'_i) \simeq_{\mathrm{CS}} \mathbf{0}$ and $\rho(x+y) \not\simeq_{\mathrm{CS}} \mathbf{0}$). So $\rho(at) \not\precsim_{\mathrm{CS}} \rho(a^n\mathbf{0} + a^n(x+y))$.

We have established that $at_i = at_j$ for all $i, j \in I$, so we may conclude that if $at \precsim_{\mathrm{CS}} a^n\mathbf{0} + a^n(x+y)$, then $at = a^n\mathbf{0}$ or $at = a^n x$ or $at = a^n y$ or $at = a^n(x+y)$. If, moreover, $at \xrightarrow{a^n} t'$ with $t' = x$, then it is easy to define closed substitutions showing that $at \neq a^n\mathbf{0}$, $at \neq a^n y$ and $at \neq a^n(x+y)$, so the proof of the lemma is complete. □

In the following lemma we establish that substitution instances of sound equations of depth $< n$ satisfy P_n^{CS}.

Lemma 30 *Suppose $t \simeq_{\mathrm{CS}} u$, let $n \geq 1$ be a natural number greater than the depth of t and u, and suppose $\sigma(t), \sigma(u) \precsim_{\mathrm{CS}} a^n\mathbf{0} + a^n(x+y)$. Then $\sigma(t)$ has a summand $a^n x$ if and only if $\sigma(u)$ has a summand $a^n x$.*

Proof: Clearly, by symmetry, it suffices to establish the direction from left to right. So suppose $\sigma(t)$ has a summand $a^n x$; then there are two cases:

CASE 1: t has a variable summand z and $\sigma(z)$ has a summand $a^n x$.

Then, since $t \simeq_{\mathrm{CS}} u$, by Lemma 3(3) u also has z as a summand, so clearly $\sigma(u)$ also has a summand $a^n x$.

CASE 2: t has a summand at' and $\sigma(at') = a^n x$.

Then, since $depth(at') < n$, from $\sigma(at') = a^n x$ it follows that there exist a variable z and a term t'' such that $at' \xrightarrow{a^m} z + t''$ and $\sigma(z) = a^{n-m}x$ for some $1 \leq m < n$. Since $t \simeq_{\mathrm{CS}} u$, by Lemma 3(3), u has a summand au' such that $au' \xrightarrow{a^m} z + u''$ for some term u'', and consequently $a\sigma(u') \xrightarrow{a^n} u'''$ with $u''' = x$. Since also $a\sigma(u') \precsim_{\mathrm{CS}} \sigma(u) \precsim_{\mathrm{CS}} a^n\mathbf{0} + a^n(x+y)$, it follows by Lemma 29 that $a\sigma(u') = a^n x$. So $\sigma(u)$ has a summand $a^n x$. $\Box$

We shall now prove that if an equation derivable from a collection of equations of depth $< n$, then it satisfies P_n^{CS}.

Proposition 31 *Let E be a finite axiomatization over BCCSP that is sound modulo $\simeq_{\mathrm{CS}}$, let n be a natural number greater than the depth of any term in E, and suppose $E \vdash t \approx u$ and $t, u \precsim_{\mathrm{CS}} a^n\mathbf{0} + a^n(x+y)$. Then t has a summand completed similar to $a^n x$ if and only if u has a summand completed similar to $a^n x$.*

Proof: A straightforward adaptation of the proof of Proposition 27, using Lemma 30 instead of Lemma 26, replacing $\simeq_{\mathrm{S}}$ by $\simeq_{\mathrm{CS}}$, $\precsim_{\mathrm{S}}$ by $\precsim_{\mathrm{CS}}$, "similar" by "completed similar" and $\sum_{\theta \in A^n} a(x + \Psi_n^\theta) + a\Phi_n$ by $a^n\mathbf{0} + a^n(x+y)$. $\Box$

Now we are in a position to prove the main theorem of this section.

Theorem 32 *Let $|A| > 1$. Then the equational theory of BCCSP modulo $\simeq_{\mathrm{CS}}$ is not finitely based.*

Proof: Let E be any finite axiomatization over BCCSP that is sound modulo $\simeq_{\mathrm{CS}}$ and let $n \geq 1$ greater than the depth of any term in E. Since $a^n\mathbf{0}+a^n(x+y)$ does not have a summand completed similar to $a^n x$, by Proposition 31 the equation

$$a^n x + a^n\mathbf{0} + a^n(x+y) \approx a^n\mathbf{0} + a^n(x+y) \ ,$$

which is sound modulo $\simeq_{\mathrm{CS}}$, cannot be derived from E. It follows that every finite collection of equations that are sound modulo $\simeq_{\mathrm{CS}}$ is necessarily incomplete, and hence the equational theory of BCCSP modulo $\simeq_{\mathrm{CS}}$ is not finitely based. $\Box$

8 Ready Simulation

In this section we consider ready simulation equivalence $\simeq_{\mathrm{RS}}$. Blom, Fokkink and Nain [5] gave a finite axiomatization that is sound and ground-complete for BCCSP modulo $\simeq_{\mathrm{RS}}$. It consists of axioms A1-4 together with the axiom RS presented at the start of Section 4.

Note that the equations in the infinite family presented in the previous section to show that $\simeq_{\mathrm{CS}}$ is not finitely based if $|A| > 1$, are not sound modulo $\simeq_{\mathrm{RS}}$.

To see this, let a and b be distinct actions, and let ρ be a closed substitution such that $\rho(x) = a\mathbf{0}$ and $\rho(y) = b\mathbf{0}$. Then $\rho(a^n x)$ is not ready simulated by $\rho(a^n\mathbf{0})$ because $\mathcal{I}(\rho(x)) = \{a\} \neq \emptyset = \mathcal{I}(\mathbf{0})$, and $\rho(a^n x)$ is not ready simulated by $\rho(a^n(x + y)$, because $\mathcal{I}(\rho(x)) = \{a\} \neq \{a, b\} = \rho(x + y)$.

To obtain a negative result for $\simeq_{\mathrm{RS}}$, we proceed to consider below the following adaptation of the infinite family of equations of the previous section:

$$a^n x + a^n\mathbf{0} + \sum_{b\in A} a^n(x + b\mathbf{0}) \approx a^n\mathbf{0} + \sum_{b\in A} a^n(x + b\mathbf{0}) \qquad (n \geq 1) \ .$$

These equations are sound modulo $\simeq_{\mathrm{RS}}$. The idea is that, given a closed substitution ρ, either $\rho(x)$ cannot perform any action, in which case $\rho(a^n x)$ is ready simulated by $\rho(a^n\mathbf{0})$, or $\rho(x)$ can perform some action b, in which case $\rho(a^n x)$ is ready simulated by $\rho(a^n(x + b\mathbf{0}))$. Note, however, that the summations in the above equations only abbreviate BCCSP terms if $|A| < \infty$. So we assume $1 < |A| < \infty$ in the remainder of this section.

The condition $|A| < \infty$ is, in fact, necessary for the negative result that we are about to prove, for if $A = \infty$, then Groote's technique of inverted substitutions from [13] can be applied in a straightforward fashion to prove that the axiomatization of Blom, Fokkink and Nain [5] is ω-complete; see [7].

The proof that there cannot be a finite sound axiomatization E for BCCSP modulo $\simeq_{\mathrm{RS}}$ from which the equations above can all be derived, is again with an application of the proof-theoretic technique. Let P_n^{RS} be the property

> if $t, u \precsim_{\mathrm{RS}} a^n\mathbf{0} + \sum_{b\in A} a^n(x + b\mathbf{0})$, then t has a summand ready similar to $a^n x$ if and only if u has a summand ready similar to $a^n x$.

Note that this is essentially the same property as P_n^{CS} of the previous section. Also the proof that P_n^{RS} is satisfied by every equation $t \approx u$ derivable from a collection of sound equations of depth $< n$ is analogous to the proof in the previous section. We only need to reconsider Lemma 29 in the light of the new family of equations.

Lemma 33 *If* $at \precsim_{\mathrm{RS}} a^n\mathbf{0} + \sum_{b\in A} a^n(x + b\mathbf{0})$ *and* $at \xrightarrow{a^n} t'$ *with* $t' = x$*, then* $at = a^n x$*.*

Proof: We first prove by induction on n that if $at \precsim_{\mathrm{CS}} a^n\mathbf{0} + \sum_{b\in A} a^n(x + b\mathbf{0})$, then $at = a^n\mathbf{0}$ or $at = a^n x$ or $at = a^n(x + b\mathbf{0})$ for some $b \in A$.

Suppose $n = 1$. Note that $var_0(t) \subseteq \{x\}$ by Lemma 3(3). Next, we establish that $\mathcal{I}(t) \subseteq \{b\}$ for some $b \in A$. To this end, let ρ be a closed substitution such that $\rho(x) = \mathbf{0}$. Then $\mathcal{I}(\rho(t)) = \mathcal{I}(\rho(\mathbf{0})) = \emptyset$ or $\mathcal{I}(\rho(t)) = \mathcal{I}(\rho(x + b\mathbf{0})) = \{b\}$ for some $b \in A$, and hence $\mathcal{I} \subseteq \{b\}$ for some $b \in A$. Now it has been shown that $t = \mathbf{0}$ or $t = x$ or $t = b\mathbf{0}$ or $t = x + b\mathbf{0}$. To exclude the case that $t = b\mathbf{0}$, suppose that $\mathcal{I}(t) = \{b\}$, and consider a substitution ρ such that $\rho(x) = c\mathbf{0}$ for some $c \neq b$. Since $\mathcal{I}(\rho(t)) \neq \mathcal{I}(\rho(\mathbf{0}))$ and $\mathcal{I}(\rho(t)) \neq \mathcal{I}(\rho(x + b'\mathbf{0}))$ for $b' \neq b$, it follows that $\mathcal{I}(\rho(t)) = \mathcal{I}(\rho(x + b\mathbf{0})) = \{b, c\}$. So $x \in \mathit{var}_0(t)$, and hence $t = x + b\mathbf{0}$.

Suppose $n > 1$. Then $\mathcal{I}(t) = \{a\}$ by Lemma 3(2) and $\mathit{var}_0(t) = \emptyset$ by Lemma 3(3), so $t = \sum_{i \in I} at_i$ with $I \neq \emptyset$. Clearly, $at_i \precsim_{\mathrm{RS}} a^{n-1}\mathbf{0} + \sum_{b \in A} a^{n-1}(x + b\mathbf{0})$, so by the induction hypothesis, for all $i \in I$, $at_i = a^{n-1}\mathbf{0}$ or $at_i = a^{n-1}x$ or $at_i = a^{n-1}(x + b_i\mathbf{0})$ for some $b_i \in A$.

It remains to establish that $at_i = at_j$ for all $i, j \in I$. Suppose, towards a contradiction, that $at_i \neq at_j$ for some $i, j \in I$. Then clearly there exist t_i' and t_j' such that $at_i \xrightarrow{a^{n-1}} t_i'$, $at_j \xrightarrow{a^{n-1}} t_j'$ and $t_i' \neq t_j'$. Modulo symmetry we can distinguish four cases, and in each of them it suffices to provide a closed substitution ρ such that $\rho(at) \not\precsim_{\mathrm{RS}} \rho(a^n\mathbf{0} + \sum_{b \in A} a^n(x + b\mathbf{0}))$.

Cases 1,2: $t_i' = \mathbf{0}$ and $t_j' = x$ or $t_j' = x + b_j\mathbf{0}$.

Define ρ such that $\rho(x) \not\simeq_{\mathrm{RS}} \mathbf{0}$. Then $\rho(t) \not\precsim_{\mathrm{RS}} a^{n-1}\mathbf{0}$ (because $\rho(t) \xrightarrow{a^{n-1}} \rho(t_j') \not\simeq_{\mathrm{RS}} \mathbf{0}$) and $\rho(t) \not\precsim_{\mathrm{RS}} a^{n-1}\rho(x + b_j\mathbf{0})$ (because $\rho(t) \xrightarrow{a^{n-1}} \rho(t_i') \simeq_{\mathrm{RS}} \mathbf{0}$).

Case 3: $t_i' = x$ and $t_j' = x + b_j\mathbf{0}$.

Define ρ such that $\rho(x) = \mathbf{0}$. Then $\rho(t) \not\precsim_{\mathrm{RS}} a^{n-1}\mathbf{0}$ (because $\rho(t) \xrightarrow{a^{n-1}} \rho(t_j') \not\simeq_{\mathrm{RS}} \mathbf{0}$) and $\rho(t) \not\precsim_{\mathrm{RS}} a^{n-1}\rho(x + b_j\mathbf{0})$ (because $\rho(t) \xrightarrow{a^{n-1}} \rho(t_i') = \mathbf{0}$).

Case 4: $t_i' = x + b_i\mathbf{0}$ and $t_j' = x + b_j\mathbf{0}$ for some $b_i, b_j \in A$ with $b_i \neq b_j$.

Define ρ such that $\rho(x) = \mathbf{0}$. Then $\rho(t) \not\precsim_{\mathrm{RS}} a^{n-1}\mathbf{0}$ (because $\rho(t) \xrightarrow{a^{n-1}} \rho(t_i') \not\simeq_{\mathrm{RS}} \mathbf{0}$) and $\rho(t) \not\precsim_{\mathrm{RS}} a^{n-1}\rho(x + b\mathbf{0})$ for all $b \in A$ (because $b \neq b_k$ for $k = i$ or $k = j$, so that $\rho(t) \xrightarrow{a^{n-1}} \rho(t_k') \simeq_{\mathrm{RS}} b_k\mathbf{0}$ and $\rho(x + b\mathbf{0}) \not\simeq_{\mathrm{RS}} b_k\mathbf{0}$).

We have established that $at_i = at_j$ for all $i, j \in I$, so we may conclude that if $at \precsim_{\mathrm{RS}} a^n\mathbf{0} + \sum_{b \in A} a^n(x + b\mathbf{0})$, then $at = a^n\mathbf{0}$ or $at = a^n x$ or $at = a^n(x + b\mathbf{0})$ for some $b \in A$. If, moreover, $at \xrightarrow{a^n} t'$ with $t' = x$, then it is easy to define closed substitutions showing that $at \neq a^n\mathbf{0}$ and $at \neq a^n(x + b\mathbf{0})$, so the proof of the lemma is complete. □

The following lemma corresponds to Lemma 30 of the previous section.

Lemma 34 *Suppose $t \simeq_{\mathrm{RS}} u$, let $n \geq 1$ be a natural number greater than the depth of t and u, and suppose $\sigma(t), \sigma(u) \precsim_{\mathrm{RS}} a^n\mathbf{0} + \sum_{b \in A} a^n(x + b)$. Then $\sigma(t)$ has a summand $a^n x$ if and only if $\sigma(u)$ has a summand $a^n x$.*

Proof: A straightforward adaptation of the proof of Lemma 30, using Lemma 33 instead of Lemma 29, replacing $\simeq_{\mathrm{CS}}$ by $\simeq_{\mathrm{RS}}$, $\precsim_{\mathrm{CS}}$ by $\precsim_{\mathrm{RS}}$, and $a^n\mathbf{0} + a^n(x + y)$

by $a^n\mathbf{0} + \sum_{b\in A} a^n(x + b\mathbf{0})$ $\square$

The following proposition corresponds to Proposition 31 from the previous section.

Proposition 35 *Let E be a finite axiomatization over BCCSP that is sound modulo $\simeq_{\mathrm{RS}}$, let n be a natural number greater than the depth of any term in E, and suppose $E \vdash t \approx u$ and $t, u \precsim_{\mathrm{RS}} a^n\mathbf{0} + \sum_{b\in A} a^n(x + b\mathbf{0})$. Then t has a summand ready similar to $a^n x$ if and only if u has a summand ready similar to $a^n x$.*

Proof: A straightforward adaptation of the proof of Proposition 27, using Lemma 34 instead of Lemma 26, replacing $\simeq_{\mathrm{S}}$ by $\simeq_{\mathrm{RS}}$, $\precsim_{\mathrm{S}}$ by $\precsim_{\mathrm{RS}}$, "similar" by "ready similar" and $\sum_{\theta\in A^n} a(x + \Psi_n^\theta) + a\Phi_n$ by $a^n\mathbf{0} + \sum_{b\in A} a^n(x + b\mathbf{0})$. $\square$

Now we are in a position to prove the main theorem of this section.

Theorem 36 *Let $1 < |A| < \infty$. Then the equational theory of BCCSP modulo $\simeq_{\mathrm{RS}}$ is not finitely based.*

Proof: Let E be a finite axiomatization over BCCSP that is sound modulo $\simeq_{\mathrm{RS}}$. Let n be greater than the depth of any term in E.

Note that $a^n\mathbf{0} + \sum_{b\in A} a^n(x + b\mathbf{0})$ does not contain a summand ready similar to $a^n x$. So according to Proposition 35, the equation

$$a^n x + a^n\mathbf{0} + \sum_{b\in A} a^n(x + b\mathbf{0}) \approx a^n\mathbf{0} + \sum_{b\in A} a^n(x + b\mathbf{0}) \ ,$$

which is sound modulo $\simeq_{\mathrm{RS}}$, cannot be derived from E. It follows that every finite collection of equations that are sound modulo $\simeq_{\mathrm{RS}}$ is necessarily incomplete, and hence the equational theory of BCCSP modulo $\simeq_{\mathrm{RS}}$ is not finitely based. $\square$

9 Conclusions

For every equivalence in van Glabbeek's linear time – branching time spectrum it has now been determined whether it is finitely based or not. Table 9 presents an overview, with a $+$ indicating that a finite basis exists and a $-$ indicating that a finite basis does not exist. We distinguish three categories, according to the cardinality of the alphabet A: singleton, finite with at least two actions, and infinite.

	$\|A\| = 1$	$1 < \|A\| < \infty$	$\|A\| = \infty$
bisimulation	+	+	+
2-nested simulation	−	−	−
possible futures	−	−	−
ready simulation	+	−	+
completed simulation	+	−	−
simulation	+	−	+
possible worlds	+	−	+
ready traces	+	−	−
failure traces	+	−	+
readies	+	−	+
failures	+	+	+
completed traces	+	+	+
traces	+	+	+

Table 1
The existence of finite bases for BCCSP in the linear time – branching time spectrum

Acknowledgements

We are most grateful to Luca Aceto and Anna Ingolfsdottir for stimulating discussions, and to the anonymous referees for suggesting many improvements.

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, and A. Ingolfsdottir. Ready to preorder: Get your BCCSP axiomatization for free! In *Proceedings 2nd Conference on Algebra and Coalgebra in Computer Science (CALCO'07)*, to appear.

[3] 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.

[4] 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 4052, pp. 492–503. Springer, 2006.

[5] 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.

[6] T. Chen and W. Fokkink. On finite alphabets and infinite bases III: Simulation. In *Proceedings 17th Conference on Concurrency Theory (CONCUR'06)*, Bonn, LNCS 4137, pp. 421-434. Springer, 2006.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] R. van Glabbeek. The linear time – branching time spectrum (Extended Abstract). In *Proceedings 1st Conference on Concurrency Theory (CONCUR'90)*, Amsterdam, LNCS 458, pp. 278-297. Springer, 1990.

[12] 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.

[13] 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.

[14] R. Gurevič. Equational theory of positive natural numbers with exponentiation is not finitely axiomatizable. *Annals of Pure and Applied Logic*, 49:1–30, 1990.

[15] J. Heering. Partial evaluation and ω-completeness of algebraic specifications. *Theoretical Computer Science*, 43:149–167, 1986.

[16] L. Henkin. The logic of equality. *American Mathematical Monthly*, 84(8):597–612, 1977.

[17] H. Lin. PAM: A process algebra manipulator. *Formal Methods in System Design*, 7(3):243–259, 1995.

[18] 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.

[19] R. Lyndon. Identities in two-valued calculi. *Transactions of the American Mathematical Society*, 71:457–465, 1951.

[20] R. McKenzie. Tarski's finite basis problem is undecidable. *Journal of Algebra and Computation*, 6(1):49–104, 1996.

[21] R. McKenzie, G. McNulty, and W. Taylor. *Algebras, Varieties, Lattices.* Wadsworth & Brooks/Cole, 1987.

[22] R. Milner. *A Calculus of Communicating Systems.* LNCS 92. Springer, 1980.

[23] R. Milner. *Communication and Concurrency.* Prentice Hall, 1989.

[24] F. Moller. *Axioms for Concurrency.* PhD thesis, University of Edinburgh, 1989.

[25] F. Moller. The Nonexistence of Finite Axiomatisations for CCS Congruences. In *Proceedings 5th Annual IEEE Symposium on Logic in Computer Science (LICS'90)*, Philadelphia, pp. 142-153. IEEE Computer Society, 1990.

[26] 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.

[27] 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.

[28] G.D. Plotkin. The λ-calculus is ω-incomplete. *Journal of Symbolic Logic*, 39(2):313–317, 1974.