

On Finite Bases for Weak Semantics: Failures versus Impossible Futures

Taolue Chen

CWI, Department of Software Engineering,
Amsterdam, The Netherlands

Joint work with **Wan Fokkink** (Free University Amsterdam) and
Rob van Glabbeek (National ICT Australia)

Introduction (I)

- Labeled transition system: a fundamental model of concurrent computation.

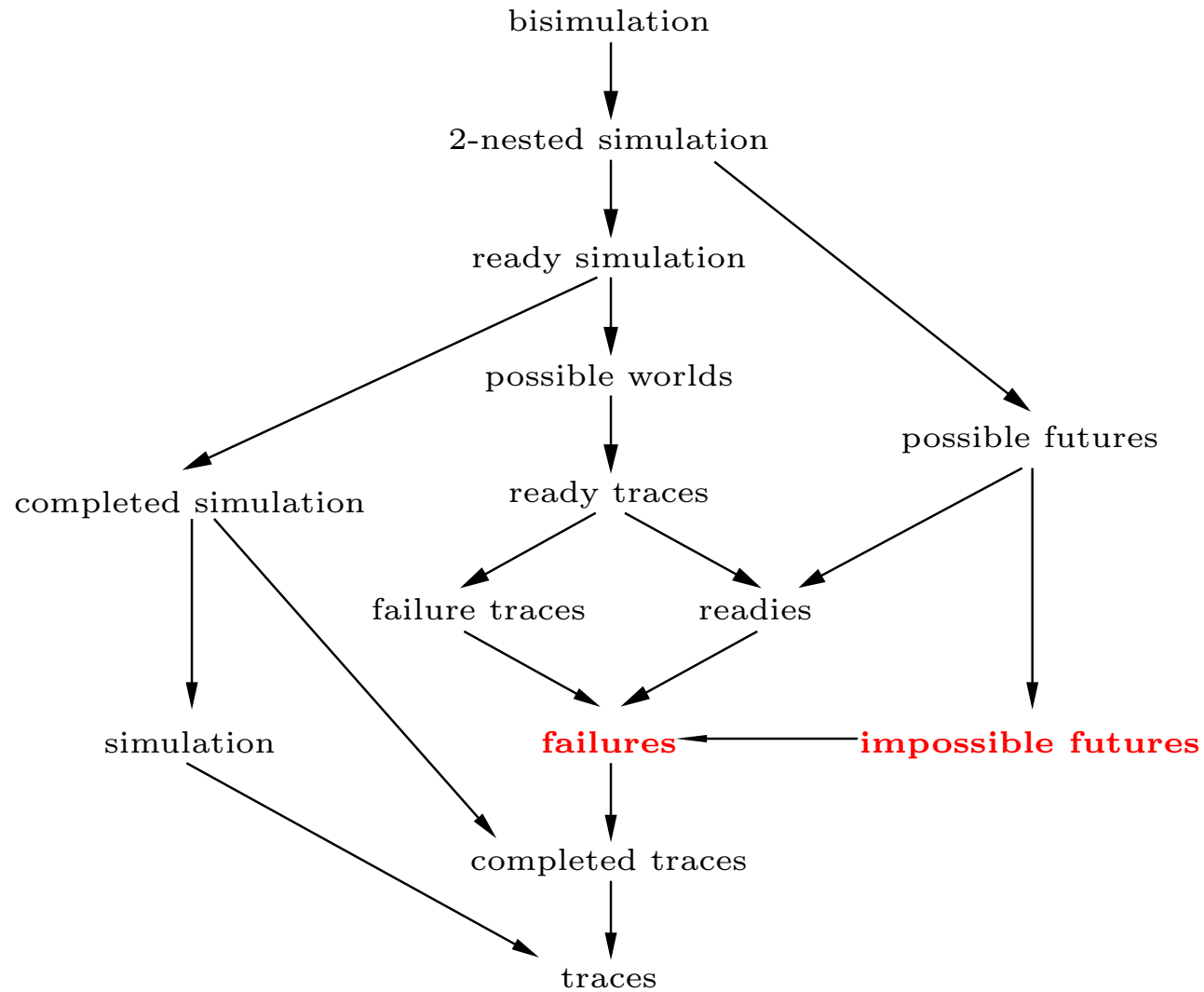
$$\mathcal{L} = (S, L, \{\xrightarrow{\ell}\}_{\ell \in L})$$

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

Introduction (II)

- **Behavioral equivalence**: identify those states of labeled transition systems that afford the same behaviors;
- No consensus on what is an appropriate notion of “behavioral equivalence” for reactive systems;
- One of the main tasks of concurrency theory is to provide a uniform classification of system (or process) behavior. This forms the study of **comparative concurrency semantics**;
- E.g. **Linear time - branching time spectrum I** of behavioral **preorders** and **equivalences** for finitely branching, sequential, **concrete** processes (van Glabbeek).

Linear Time - Branching Time Spectrum



Weak Semantics

Van Glabbeek's spectrum has two parts:

- Spectrum I deals with **concrete** processes (without silent moves τ), as showed before;
 —→ **concrete** semantics
- Spectrum II expands I with one dimension to deal with processes with **abstraction** (silent moves τ)
 —→ **weak** semantics;

Our work focuses on **weak** semantics. In particular, the **axiomatizability** of **weak failures** semantics and **weak impossible futures** semantics.

Failures and Impossible Futures

Assume a labeled transition system with the label set $A_\tau = A \cup \{\tau\}$:

- A pair $(a_1 \cdots a_k, B)$, with $k \geq 0$ and $B \subseteq A$, is a **weak failure pair** of a state s if there is a path $s \Rightarrow \xrightarrow{a_1} \Rightarrow \cdots \Rightarrow \xrightarrow{a_k} \Rightarrow s_k$ with $\mathcal{I}(s_k) \cap B = \emptyset$.
- A pair $(a_1 \cdots a_k, B)$, with $k \geq 0$ and $B \subseteq A^*$, is a **weak impossible future** of a state s if there is a path $s \Rightarrow \xrightarrow{a_1} \Rightarrow \cdots \Rightarrow \xrightarrow{a_k} \Rightarrow s_k$ with $\mathcal{T}(s_k) \cap B = \emptyset$.

Tip: \Rightarrow is the transitive closure of $\xrightarrow{\tau}$; $\mathcal{I}(s) = \{a \in A \mid t \Rightarrow \xrightarrow{a}\}$ and $\mathcal{T}(s)$ denotes the set of traces of s .

These definitions naturally induce corresponding **preorders** and **equivalences**.

Axiomatization (I)

Process Calculi:

We work in the setting of the process algebra BCCS (BCCSP extended by τ):

BCCS **nil** 0 **prefixing** αt (with $\alpha \in A_\tau$)
choice $t + u$ **variables** x

$$\frac{}{\alpha x \xrightarrow{\alpha} x} \quad \frac{x \xrightarrow{\alpha} x'}{x + y \xrightarrow{\alpha} x'} \quad \frac{y \xrightarrow{\alpha} y'}{x + y \xrightarrow{\alpha} y'}$$

Note: BCCSP = BCCS - τ

Axiomatization (II)

- **Axiomatization** (a set of (in)equations) to characterize the semantics in the spectrum. For example:

Axiomatization for **concrete bisimulation**:

$$\text{A1} \quad x + y \approx y + x$$

$$\text{A2} \quad (x + y) + z \approx x + (y + z)$$

$$\text{A3} \quad x + x \approx x$$

$$\text{A4} \quad x + \mathbf{0} \approx x$$

(In)Equational logic (rules): **reflexivity**, **(symmetry)**, **transitivity**, **substitution**, and **closure under context**.

$$\frac{t \approx u}{\sigma(t) \approx \sigma(u)}$$

$$\frac{t \approx u}{C[t] \approx C[u]}$$

Soundness and Ground-Completeness

Given a congruence \sim over BCCSP, give a sound and ground-complete axiomatization \approx for BCCSP:

$$P \sim Q \begin{array}{c} \xleftarrow{\text{sound}} \\ \xrightarrow{\text{g-comp}} \end{array} \vdash P \approx Q$$

for closed terms P, Q . (Likewise for preorders \preceq .)

For example,

$$P \Leftrightarrow Q \Leftrightarrow \text{A1} - \text{A4} \vdash P \approx Q \text{ for closed terms } P, Q$$

Note: $\sim = \preceq \cap \preceq^{-1}$;

Congruence: closed under the context of the process algebra

ω -Completeness

An axiomatization E is ω -complete if:

$$E \vdash \sigma(t) \approx \sigma(u) \text{ for all closed substitutions } \sigma \Rightarrow E \vdash t \approx u$$

Note that t and u are open terms, i.e. terms with variables.

Notable examples of ω -incomplete axiomatizations:

- $\lambda K\beta\eta$ -calculus
- equational theory of CCS: laws such as commutativity of parallelism,

$$t || (u || v) \approx (t || u) || v$$

is valid in the initial model but cannot be derived.

In universal algebra, an ω -complete axiomatization is referred to as a basis for the equational theory of the algebra it axiomatizes.

Existing Results on Ground-completeness

ground	$1 \leq A < \infty$	$ A = \infty$
bisim	+	+
2-nested sim	-	-
possible futu	-	-
ready sim	+	+
compl sim	+	+
sim	+	+
possible worl	+	+
ready tr	+	-
readies	+	+
failure tr	+	+
failures	+	+
completed tr	+	+
partial tr	+	+

van Glabbeek

Aceto, Fokkink,
van Glabbeek, Ingolfsdottir

Blom, Fokkink, Nain

Existing Results on ω -completeness

	$ A = 1$	$1 < A < \infty$	$ A = \infty$
bisim	+	+	+
2-nes sim	-	-	-
poss futu	-	-	-
ready sim	\oplus	-	+
compl sim	\oplus	-	-
sim	\oplus	-	+
poss worl	\oplus	-	+
ready tr	\oplus	-	-
readies	\oplus	-	+
failure tr	\oplus	-	+
failures	\oplus	\oplus	+
compl tr	\oplus	+	+
partial tr	\oplus	+	+

Problems

We have achieved a (relatively) comprehensive understanding on the axiomatizability of **concrete** semantics. But

What about **weak** semantics?

Some existing results:

- Milner's classical axiomatization for observational congruence;
- Van Glabbeek's ground-complete axiomatizations for weak failures, weak traces, etc;
- [Voorhoeve and Mauw, 2001]: (1) an **inequational** axiomatization of BCCS modulo **weak** impossible futures preorder; (2) ω -completeness in case of an infinite alphabet.

This talk: Answers the questions regarding **failures** and **impossible futures**. For each one, we consider two dimensions: (1) preorder vs. equivalence; (2) ground-completeness vs. ω -completeness.

Congruences

Please bear in mind: the axiomatizability only makes sense when **congruences** are considered.

Failures:

- The **weak failures preorder** \sqsubseteq_{WF} is given by: $p \sqsubseteq_{\text{WF}} q$ iff (1) the weak failure pairs of p are also weak failure pairs of q and (2) $p \xrightarrow{\tau}$ implies that $q \xrightarrow{\tau}$.
- **Weak failures equivalence** \equiv_{WF} is defined as $\sqsubseteq_{\text{WF}} \cap \sqsubseteq_{\text{WF}}^{-1}$.

Impossible Futures:

- The **weak impossible futures preorder** \sqsubseteq_{WIF} is given by: $p \sqsubseteq_{\text{WIF}} q$ iff (1) the weak impossible futures of p are also weak impossible futures of q , (2) $\mathcal{T}(p) = \mathcal{T}(q)$ and (3) $p \xrightarrow{\tau}$ implies that $q \xrightarrow{\tau}$.
- **Weak impossible futures equivalence** \equiv_{WIF} is defined as $\sqsubseteq_{\text{WIF}} \cap \sqsubseteq_{\text{WIF}}^{-1}$.

Failures

Let us first recall some result regarding **concrete** semantics.

On BCCSP processes, a ground-complete axiomatization for (concrete) failures **preorder** exists. It consists of the core axioms A1-4 together with one extra axiom:

$$\text{F} \quad a(x + y) \preceq ax + a(y + z)$$

On BCCS processes, the weak failures preorder coincides with the inverse of the **must-testing preorder** due to De Nicola and Hennessy.

$$\text{WF1} \quad ax + ay \approx a(\tau x + \tau y)$$

$$\text{WF2} \quad \tau(x + y) \preceq \tau x + y$$

$$\text{WF3} \quad x \preceq \tau x + y$$

ω -completeness?

We extend this **ground-completeness** result with two **ω -completeness** results.

(1) **Infinite** alphabet: Yes!

If $|A| = \infty$, then A1-4+WF1-3 is ω -complete for BCCS(A) modulo \sqsubseteq_{WF} .

(2) **Finite** alphabet: A bit more involved ...

To get a finite basis for the inequational theory of BCCS modulo \sqsubseteq_{WF} in case $|A| < \infty$, we need to **add** the following axiom:

$$WF_A \quad \sum_{a \in A} ax_a \preceq \sum_{a \in A} ax_a + y$$

where the x_a for $a \in A$ and y are distinct variables.

Equivalences: “Ready to Preorder” approach

For BCCSP, Aceto *et al* (see also Frutos Escrig *et al*) proposed an **algorithm** \mathcal{A}

an **inequational** axiomatization E for $\sqsubseteq \longrightarrow$

an **equational** axiomatization $\mathcal{A}(E)$ for $\sqsubseteq \cap \sqsubseteq^{-1}$.

The axiomatization $\mathcal{A}(E)$ generated by the algorithm from E contains

- the axioms A1-4 for bisimulation equivalence and the axioms $b(ax + z) + b(ax + by + z) \approx b(ax + ay + z)$ for $a, b \in A$ (RS)
- for each inequational axiom $t \preceq u$ in E :
 - $t + u \approx u$; and
 - $a(t + x) + a(u + x) \approx a(u + x)$ (for each $a \in A$, and some variable x that does not occur in $t + u$).

ω -Complete Axiomatization for Equivalences

Recently, we lifted this result to weak semantics, with some extra technical conditions, which allows us to apply the algorithm to **weak failures**.

After simplification and omission of redundant axioms, we obtain the following axiomatization(s) for **equivalences**.

$$\begin{array}{lcl} \text{WF1} & ax + ay & \approx a(\tau x + \tau y) \\ \text{WFE2} & \tau(x + y) + \tau x & \approx \tau x + y \\ \text{WFE3} & ax + \tau(ay + z) & \approx \tau(ax + ay + z) \\ \hline \text{WFE}_A & \tau(\sum_{a \in A} ax_a + y + z) & \approx \tau(\sum_{a \in A} ax_a + y + z) \\ & & + \tau(\sum_{a \in A} ax_a + z) \end{array}$$

Quick Summary

Weak failures semantics enjoys very nice axiomatizability properties:

- There **exists** a finite, ground-complete axiomatization for weak failures preorders;
- The finite, ground-complete axiomatization for weak failures preorder is **ω -complete** in case of an **infinite** alphabet;
- We can obtain an **ω -complete** axiomatization in case of finite alphabet, by adding one extra axiom;
- All of above apply to weak failures **equivalences**.

In short: everything is possible! :-)

Impossible Futures

Let's first recall some result regarding concrete semantics.

[Chen and Fokkink, LICS'08]

- We find a finite, sound, ground-complete axiomatization for BCCSP modulo (**concrete**) impossible futures preorder \preceq_{IF} .
- Unfortunately, there does **not** exist any finite, sound, ground-complete axiomatization for BCCSP modulo (**concrete**) impossible futures equivalence \simeq_{IF} .
- There does not exist any finite, sound, ω -complete axiomatization when the alphabet is **finite**.

Weak Case?

A ground-complete axiomatization from concrete case

$$\text{IF1} \quad a(x + y) \preceq ax + ay$$

$$\text{IF2} \quad a(x + y) + ax + a(y + z) \approx ax + a(y + z)$$

to weak case

$$\text{WIF1 (WF1)} \quad ax + ay \approx a(\tau x + \tau y)$$

$$\text{WIF2 (WF2)} \quad \tau(x + y) \preceq \tau x + y$$

$$\text{WIF3} \quad x \preceq \tau x \quad \{+y\}$$

BTW: this is a simplification of the axiomatization given in [VM01].

Moreover, it is ω -complete in case of an infinite alphabet.

Equivalence

Claim: There does **not** exist any finite, sound, ground-complete axiomatization for BCCS modulo (**weak**) impossible futures equivalence \equiv_{WIF} .

The cornerstone is the following infinite family of closed equations, for $m \geq 0$:

$$\tau a^{2m} \mathbf{0} + \tau(a^m \mathbf{0} + a^{2m} \mathbf{0}) \approx \tau(a^m \mathbf{0} + a^{2m} \mathbf{0})$$

It is not hard to see that they are sound modulo \equiv_{WIF} . But it can be shown that any **finite** sound axiomatization cannot drive all of them.

How to Prove?

Proof theoretic approach:

Step 1: Find **sound** (in)equations e_n ($n \geq 1$) (such that any **finite** sound axiomatization E does **not** prove all e_n).

Step 2: Give a **property** P_E of equations that:

- holds true for each instantiation of the axioms in E ;
- is preserved by the rules of (in)equational logic; and
- fails for some e_n .

\implies **Contradiction!**

Applying this technique

For $m \geq 0$:

$$\tau^{2m}\mathbf{0} + \tau(a^m\mathbf{0} + a^{2m}\mathbf{0}) \approx \tau(a^m\mathbf{0} + a^{2m}\mathbf{0})$$

Lemma: Assume that, for E an axiomatization sound for \sqsubseteq_{WIF} , closed terms p, q , closed substitution σ , action a and integer m :

1. $E \vdash p \approx q$;
2. $m > \max\{|u| \mid t \approx u \in E\}$;
3. $\mathcal{CT}(q) \subseteq \{a^m, a^{2m}\}$; and
4. there is a closed term p' such that $p \Rightarrow \xrightarrow{\tau} p'$ and $\mathcal{CT}(p') = \{a^{2m}\}$.

Then there is a closed term q' such that $q \Rightarrow \xrightarrow{\tau} q'$ and $\mathcal{CT}(q') = \{a^{2m}\}$.

Remarks

- Impossible futures semantics is the first example that affords a ground-complete axiomatization for BCCS modulo the **preorder**, while missing a ground-complete axiomatization for BCCS modulo the **equivalence**.
- “Ready to preorder” algorithm? That algorithm only applies to semantics that are **at least as coarse as ready simulation semantics**. Since impossible futures semantics is incomparable to ready simulation semantics, it falls outside the scope of the algorithm.
- Main reason: $a(bx + bx + z) \approx a(bx + bx + z) + a(bx + z)$ does **not** hold anymore.

ω -Completeness for \sqsubseteq_{WIF}

Results summary:

- Negative results on **equivalence** are inherited, since ω -completeness is stronger property.
- In case $|A| = \infty$, we prove that there exists a finite basis for the inequational theory of $\text{BCCS}(A)$ modulo \sqsubseteq_{WIF} . The proof is based on an adaptation of Groote's **inverted substitutions** technique to inequations.
- In case $|A| < \infty$, we prove that a finite basis does **not** exist. We give two different proofs of this last fact, one for the case $1 < |A| < \infty$ and one for the case $|A| = 1$.

Finite Alphabet (I)

We prove that, if $1 < |A| < \infty$, the inequational theory of $\text{BCCS}(A)$ modulo \sqsubseteq_{WIF} does **not** have a finite basis.

The cornerstone for this negative result is the following infinite family of inequations, for $m \geq 0$:

$$\tau(a^m x) + \Phi_m \preceq \Phi_m$$

with

$$\Phi_m = \tau(a^m x + x) + \sum_{b \in A} \tau(a^m x + a^m b \mathbf{0})$$

It is not hard to see that these inequations are sound modulo \sqsubseteq_{WIF} .

Finite Alphabet (II)

Also, the inequational theory of $\text{BCCS}(A)$ modulo \sqsubseteq_{WIF} does **not** have a finite basis in case of a **singleton alphabet**.

The cornerstone for the negative result for $|A| = 1$ is the following infinite family of inequations, for $m \geq 0$:

$$a^m x \not\leq a^m x + x$$

If $|A| = 1$, then these inequations are clearly sound modulo \sqsubseteq_{WIF} .

Note that given a closed substitution ρ , $\mathcal{T}(\rho(x)) \subseteq \mathcal{T}(\rho(a^m x))$.

Theorem: For $|A| < \infty$, the inequational theory of $\text{BCCS}(A)$ modulo \sqsubseteq_{WIF} does **not** have a finite basis.

Conclusion

Failures versus Impossible Futures:

- Ground-completeness for preorder: $x \preceq \tau x + y$ versus $x \preceq \tau x$;
- Ground-completeness for equivalence: Yes versus No;
- ω -completeness (infinite alphabet): $x \preceq \tau x + y$ versus $x \preceq \tau x$;
- ω -completeness (finite alphabet): Yes versus No;

Future works: (1) More axiomatizability results for weak semantics?
(2) Establish links between axiomatizabilities of concrete and weak semantics.

Thank you for your attention!