A Meta-Theorem of Unaximatizability

Luca Aceto\textsuperscript{1}, Wan Fokkink\textsuperscript{2}, Anna Ingólfsdóttir\textsuperscript{1}, Mohammad Mousavi\textsuperscript{3}

\textsuperscript{1}Reykjavík University, Reykjavík, Iceland
\textsuperscript{2}VU Amsterdam, Amsterdam, The Netherlands
\textsuperscript{3}TU/Eindhoven, Eindhoven, The Netherlands

Prose November 22, 2007, TU/Eindhoven
Negative results are the only possible self-contained theoretical results in Computer Science.

-- Christos Papadimitriou
General Idea

- Reduce your difficult problem to other difficult, yet solved, problems and use their solutions.

- A very common practice, among others, in complexity theory.

- E.g., to prove undecidability: show that your problem is (at least) as difficult as halting problem in Turing machines.
Outline

1 Preliminaries

2 Outline of the Method

3 Some Applications

4 A Negative Result About a Negative Meta-Theorem

5 Conclusions
A Cute Subset of CCS

Syntax

\[ P ::= 0 \mid a.P \mid P + P \mid P \parallel P \]

Semantics

\[
\begin{align*}
    a.x & \rightarrow x \\
    x_0 & \xrightarrow{a} y_0 \\
    x_0 + x_1 & \xrightarrow{a} y_0 \\
    x_1 & \xrightarrow{a} y_1 \\
    x_0 || x_1 & \xrightarrow{a} y_0 || x_1 \\
    x_0 & \xrightarrow{a} x_0 || y_1
\end{align*}
\]
Notational Conventions

1. Binding power: $a \_ > \_ + \_ > \_ \| \_ \$, i.e., $a.0 + a.0 \| a.0$ is $((a.0) + (a.0)) \| (a.0)$;

2. Omit the trailing 0: write $a.a + a$ for $(a.a.0) + (a.0)$

Sum Notation

Write $\sum_{i \in \{0, \ldots, n\}} P_i$ for $P_0 + \ldots + P_n$. ($\sum_{i \in \emptyset} = 0$)

The scope of $\sum$ goes as far as possible.
Bisimulation and Bisimilarity

Bisimulation relation \( R \):
\[
p R q \Rightarrow \\
\forall p' p \xrightarrow{a} p' \Rightarrow \exists q' q \xrightarrow{a} q' \land p' R q'
\]
and vice versa...

- \( p \leftrightarrow q \) when there exists a bisim. rel. \( R \) s.t. \( p R q \);
- \( s \leftrightarrow t \) when for all closing subst. \( \sigma \), \( \sigma(s) \leftrightarrow \sigma(t) \).
Derivation Logic

Assume a set $E$ of axioms of the form $t = t'$:

\[
\begin{align*}
\text{(refl)} & \quad \frac{}{E \vdash t = t} \\
\text{(trans)} & \quad \frac{E \vdash t_0 = t_1 \quad E \vdash t_1 = t_2}{E \vdash t_0 = t_2} \\
\text{(cong)} & \quad \frac{E \vdash t_0 = t'_0 \quad \ldots \quad E \vdash t_n = t'_n}{E \vdash f(t_0, \ldots, t_n) = f(t'_0, \ldots, t'_n)} \\
\text{(E)} & \quad \frac{t = t' \in E}{E \vdash \sigma(t) = \sigma(t')} 
\end{align*}
\]

Symmetry is intentionally left out.
Soundness and (ω-)Completeness

$E$ is

1. **sound** when $E \vdash p = q \Rightarrow p \leftrightarrow q$;
   (calculation is **correct**)

2. **ground-complete** when $p \leftrightarrow q \Rightarrow E \vdash p = q$;
   (calculation is **sufficient**; forget about models)

3. **ω-complete** when if for all $\sigma$, $E \vdash \sigma(s) = \sigma(t) \Rightarrow E \vdash s = t$.
   (calculations is sufficient even for the most general results; the relevant notion in universal algebra)

In this talk:
Axiomatization = Sound and (ground- and ω-)complete axiom system.
All our impossibility (meta-)results easily generalize to sound and ground-complete axioms systems.
### Axioms Systems

#### Soundness and (ω-)Completeness

**E is**

1. **sound** when $E \vdash p = q \Rightarrow p \leftrightarrow q$;
   (calculation is correct)

2. **ground-complete** when $p \leftrightarrow q \Rightarrow E \vdash p = q$;
   (calculation is sufficient; forget about models)

3. **ω-complete** when if for all $\sigma$, $E \vdash \sigma(s) = \sigma(t) \Rightarrow E \vdash s = t$.
   (calculations is sufficient even for the most general results; the relevant notion in universal algebra)

In this talk:
Axiomatization = Sound and (ground- and ω-)complete axiom system.
All our impossibility (meta-)results easily generalize to sound and ground-complete axiom systems.
### CCS without Parallel

<table>
<thead>
<tr>
<th></th>
<th>Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0</td>
<td>( x + y = y + x )</td>
</tr>
<tr>
<td>A1</td>
<td>( (x + y) + z = x + (y + z) )</td>
</tr>
<tr>
<td>A2</td>
<td>( x + x = x )</td>
</tr>
<tr>
<td>A3</td>
<td>( 0 + x = x )</td>
</tr>
</tbody>
</table>

### Parallel?

\[ a \parallel a \leftrightarrow a.a \]
### CCS without Parallel

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A0</td>
<td>( x + y = y + x )</td>
<td>A1</td>
</tr>
<tr>
<td>A2</td>
<td>( x + x = x )</td>
<td>A3</td>
</tr>
</tbody>
</table>

### Parallel?

\[ a \parallel a \leftrightarrow \text{true} \]
Faron Moller [ICALP’90 and Ph.D. Thesis]: CCS modulo bisimilarity does not afford a finite axiomatization.

Moller’s Proof (Put Informally)

Assume that there is a sound and complete equational theory $E$ for CCS, then

- For sufficiently large $m$, one cannot prove

\[ E \vdash \sum_{1 \leq i \leq m} a.a^{\leq i} \parallel a = a.(\sum_{1 \leq i \leq m} a.a^{\leq i}) + \sum_{1 \leq i \leq m} a.(a^{\leq i} \parallel a) \]

where $a^{\leq i} = a + \ldots + a^i$, $a^0 = 0$ and $a^i = a.a^{i-1}$
Unaxiomatizability

CCS with Parallel

Faron Moller [ICALP’90 and Ph.D. Thesis]: CCS modulo bisimilarity does not afford a finite axiomatization.

Moller’s Proof (Put Informally)

Assume that there is a sound and complete equational theory $E$ for CCS, then

- For sufficiently large $m$, one cannot prove

$$E \vdash \sum_{1 \leq i \leq m} a.a^{\leq i} \parallel a = a.(\sum_{1 \leq i \leq m} a.a^{\leq i}) + \sum_{1 \leq i \leq m} a.(a^{\leq i} \parallel a)$$

where $a^{\leq i} = a + \ldots + a^i$, $a^0 = 0$ and $a^i = a.a^{i-1}$
Unaxiomatizability

Moller’s Proof Sketch

Defnition 4.1. A term t ∈ T(Σ) is a Σ-axiom if it cannot be expressed as p ∨ q for any two Σ-formulas p ∈ Σ and q ∈ Σ.

A useful and somewhat revealing result about these axiom and inequality schemes is given by the following proposition, which provides a structural definition of a Σ-instance.

Theorem 4.1. If t is a Σ-axiom and if p ∨ q is a Σ-formula, then for all Σ-formulas t, t ∈ Σ implies p ∨ q.

Proof. Let t ∈ Σ be a Σ-axiom. Then, for any two Σ-formulas p ∈ Σ and q ∈ Σ, t ∨ p ∨ q ∈ Σ.

4. Technical Lemmata

In this section, we show that the technical lemmata which we need for our result can be proven by a simple proof. We begin by proving a series of lemmata which will be used in the proof of the main theorem.

Lemma 4.1. Let p, q ∈ P be two Σ-formulas. Then, for all Σ-formulas t, t ∈ Σ implies p ∨ q.

Proof. Let t ∈ Σ be a Σ-formula. Then, for any two Σ-formulas p ∈ Σ and q ∈ Σ, t ∨ p ∨ q ∈ Σ.

5. Main Result

In this section, we prove the main result of this paper. We begin by proving a series of lemmata which will be used in the proof of the main theorem.

Lemma 5.1. Let p, q ∈ P be two Σ-formulas. Then, for all Σ-formulas t, t ∈ Σ implies p ∨ q.

Proof. Let t ∈ Σ be a Σ-formula. Then, for any two Σ-formulas p ∈ Σ and q ∈ Σ, t ∨ p ∨ q ∈ Σ.

6. Conclusion

In this section, we summarize the results of this paper and discuss their implications.

Conclusion 6.1. We have shown that the main result of this paper can be proven by a simple proof. We believe that this result has important implications for the study of unaxiomatizable theories.

Acknowledgments

This work was supported by the Natural Sciences and Engineering Research Council of Canada.
Beyond CCS and Bisimilarity

Most other unaxiomatizability proofs are as difficult and tedious.

Goal

1. Take the calculus of your choice $\Sigma_e$;
2. Take the behavioral pre-order of your choice $\preceq_e$;
3. Give a well-behaved reduction from $T(\Sigma_e)$ to CCS terms (or any other unaxiomatizable calculus).
4. AFIM meta-theorem guarantees unaxiomatizability!
\[ \tilde{\cdot} : \mathcal{T}(\Sigma_e) \rightarrow \mathcal{T}(\Sigma_o) \] is a reduction from \( \Sigma_e \) to \( \Sigma_o \), when \( \forall t,u \in \mathcal{T}(\Sigma_e) \),

1. \( t \sim_e u \Rightarrow \hat{t} \sim_o \hat{u} \) and
2. \( E \vdash t = u \Rightarrow \hat{E} \vdash \hat{t} = \hat{u}. \)

\[ \hat{E} \doteq \{ \hat{t} = \hat{u} | t = u \in E \} . \]
\( \hat{\sim} : \mathcal{I}(\Sigma_e) \rightarrow \mathcal{I}(\Sigma_o) \) is structural, when \( \hat{\sigma}(t) \equiv \hat{\sigma}(\hat{t}) \), where \( \hat{\sigma} \equiv \{ x \mapsto \sigma(x) \} \).

**Lemma.** For a structural mapping \( \hat{\sim} \), \( E \vdash t = u \Rightarrow \hat{E} \vdash \hat{t} = \hat{u} \).
Given an axioms system $E$ on $\mathcal{I}(\Sigma_o)$, a reduction $\hat{\sim}$ is $E$-reflecting, when for each $t = u \in E$, there exists a sound equation $t' = u'$ on $\mathcal{I}(\Sigma_e)$ w.r.t. $\sim_e$ such that $\hat{t'} \equiv t$ and $\hat{u'} \equiv u$. 
**Theorem.** If there is
- a sound (possibly infinite) set of axioms $E$ w.r.t. $\sim_o$ not provable from any finite sound axiom system on $\mathcal{T}(\Sigma_o)$ such that
- there exists an $E$-reflecting structural reduction from $\Sigma_e$ to $\Sigma_o$
then $\mathcal{T}(\Sigma_e)/\sim_e$ affords no finite axiomatization.
Basic Theory (Recap)

Syntax

\[ P ::= 0 \mid a.P \mid P + P \mid P \parallel P \]

Moller’s Equations

One cannot prove the following set of sound axioms w.r.t. CCS/ \(\leftrightarrow\):

\[ \mathcal{M} = \{ \sum_{1 \leq i \leq m} a.a^{\leq i} \parallel a = a.(\sum_{1 \leq i \leq m} a.a^{\leq i}) + \sum_{1 \leq i \leq m} a.(a^{\leq i} \parallel a) \mid m \in \mathbb{N} \} \]
Syntax ($\Sigma_e$)

\[
P ::= 0 \mid \alpha.P \mid \epsilon(1).P \mid P + P \mid P || P
\]

where $\alpha$ is an action taken from a set $A \cup \overline{A} \cup \{\tau\}$. 

$TACS^{UT}$ and Faster-Than Pre-Order
**Semantics**

\[(tn)\]
\[
0 \xrightarrow{\epsilon(1)} 0
\]

\[(dd0)\]
\[
\epsilon(1).x \xrightarrow{\epsilon(1)} x
\]

\[(dd1)\]
\[
x \xrightarrow{\alpha} y
\]

\[(c0)\]
\[
x_0 \xrightarrow{\chi} y
\]

\[(tc)\]
\[
x_0 \xrightarrow{\epsilon(1)} y_0 \quad x_1 \xrightarrow{\epsilon(1)} y_1
\]

\[(p0)\]
\[
x_0 \xrightarrow{\chi} y_0
\]

\[(p2)\]
\[
x_0 \xrightarrow{\mu} y_0 \quad x_1 \xrightarrow{\mu} y_1
\]

\[(tp)\]
\[
x_0 \xrightarrow{\epsilon(1)} y_0 \quad x_1 \xrightarrow{\epsilon(1)} y_1
\]

\[
\chi \in A \cup \overline{A} \cup \{\tau, \epsilon(1)\}, \quad \alpha \in A \cup \overline{A} \cup \{\tau\}, \quad \mu \in A \cup \overline{A}
\]
The faster-than pre-order is the largest relation $\sqsupseteq$ satisfying $\forall p, q \; p \sqsupseteq q$ whenever:

1. $\forall p' \; p \xrightarrow{a} p' \Rightarrow \exists q' \; q \xrightarrow{a} q' \land p' \sqsupseteq q'$,
2. $\forall q' \; q \xrightarrow{a} q' \Rightarrow \exists p' \; p \xrightarrow{a} p' \land p' \sqsupseteq q'$ and
3. $\forall p' \; p \xrightarrow{(1)} p' \Rightarrow \mathcal{U}(p) \subseteq \mathcal{U}(q) \land \exists q' \; q \xrightarrow{(1)} q' \land p' \sqsupseteq q'$.

where $\mathcal{U}(p)$ is the set of all possible first actions of $p$. 

**Meta-Theorem**
Reduction from $TACS^U T$ to CCS

\[
\begin{align*}
\hat{0} &= 0 & \hat{x} &= x \\
\hat{a}.t &= a\hat{t} & \hat{\alpha}.t &= 0 \text{ for } \alpha \neq a \\
\hat{\epsilon(1)}.t &= \hat{t} & \hat{t} + \hat{u} &= \hat{t} + \hat{u} & \hat{t} || \hat{u} &= \hat{t} || \hat{u}
\end{align*}
\]
Meta-Theorem: Applied to $TACS^{UT}$

1. $t \sqsupset u \Rightarrow \hat{t} \leftrightarrow \hat{u}$,
2. $\hat{\_}$ is structural,
3. all Moller’s axioms in $M$ are sound w.r.t. $\sqsupset$ and remain intact under $\hat{\_}$,

thus $TACS^{UT}/\equiv$ affords no finite axiomatization.
Other Examples

1. Discrete-Timed CCS modulo Timed Bisimulation
2. $TACS^{LT}$ modulo MT-preorder
3. TACS modulo Urgent Bisimulation
4. IMC modulo Markovian Bisimulation
**CCS\(_\Omega\): Syntax**

\[ P ::= 0 \mid \Omega \mid a.P \mid P + P \mid P \parallel P \]

**CCS\(_\Omega\): Semantics**

Transition semantics: just like CCS (thus, no transition for \(\Omega\)).

\[
\begin{array}{cccc}
0 & a.p & 0 + q & p \parallel q \\
\end{array}
\]

N.B. for each CCS process \(p\), \(p \downarrow\).
Free Lunch?

Prebisimilarity

The relation $\sqsubseteq_{pre}$ is the largest relation satisfying $p \sqsubseteq_{pre} q$ when

1. $\forall p', p \xrightarrow{a} p'$ then $\exists q' q \xrightarrow{a} q'$ and $p' \sqsubseteq_{pre} q'$;
2. $p \downarrow$, then
   1. $q \downarrow$ and
   2. $\forall q', q \xrightarrow{a} q'$, $\exists p' p \xrightarrow{a} p'$ and $p' \sqsubseteq_{pre} q'$.

N.B. $\forall p \Omega \sqsubseteq_{pre} p$. 
Suppose \( \hat{\sim} \) is a reduction from \( CCS_\Omega \) to CCS;

\[
\forall p \Omega \sim_{pre} p, \text{ hence, } \hat{\Omega} \leftrightarrow \hat{p};
\]

thus, \( \hat{\sim} \) is a constant function modulo \( \leftrightarrow \);

For \( m \neq n \) it does not hold that

\[
\sum_{1 \leq i \leq m} a.a^{\leq i} \parallel a \leftrightarrow \sum_{1 \leq i \leq n} a.a^{\leq i} \parallel a;
\]

Hence, \( \hat{\sim} \) cannot be \( M \)-reflecting.
Conclusions

Done

1. A reduction method for proving unaxiomatizability
2. with general algebraic conditions;
3. applied to many examples from the literature (leading to novel results);
4. investigated the limitations of the method.

To be Done

1. Finding concrete sufficient criteria by committing concrete models,
2. SOS meta-theory is a promising candidate: e.g., the link with conservative and orthogonal extensions;
3. removing the limitation by taking partial reductions.