A Meta-Theorem of Unaximatizability

Luca Aceto[1], Wan Fokkink[2],
Anna Ingólfsdóttir[1], Mohammad Mousavi[3]

[1]Reykjavík University, Reykjavík, Iceland

[2]VU Amsterdam, Amsterdam, The Netherlands

[3]TU/Eindhoven, Eindhoven, The Netherlands

Prose November 22, 2007, TU/Eindhoven

Motto

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

A Cute Subset of CCS

Syntax

$$P \quad ::= \quad 0 \mid a.P \mid P + P \mid P \mid\mid P$$

Semantics

$$\frac{}{a.x \xrightarrow{a} x} \qquad \frac{x_0 \xrightarrow{a} y_0}{x_0 + x_1 \xrightarrow{a} y_0} \qquad \frac{x_1 \xrightarrow{a} y_1}{x_0 + x_1 \xrightarrow{a} y_1}$$

$$\frac{x_0 \xrightarrow{a} y_0}{x_0 \mid\mid x_1 \xrightarrow{a} y_0 \mid\mid x_1} \qquad \frac{x_1 \xrightarrow{a} y_1}{x_0 \mid\mid x_1 \xrightarrow{a} x_0 \mid\mid y_1}$$

CCS

Notational Conventions

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

$p \; R \; q \quad \Rightarrow$

$$\forall_{p'} p \xrightarrow{a} p' \Rightarrow \exists_{q'} q \xrightarrow{a} q' \wedge p' \; R \; q'$$

and vice versa...

- $p \underline{\leftrightarrow} q$ when there exists a bisim. rel. R s.t. $p \; R \; q$;
- $s \underline{\leftrightarrow} t$ when for all closing subst. σ, $\sigma(s) \; \underline{\leftrightarrow} \; \sigma(t)$.

Derivation Logic

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

$$(\textbf{refl})\frac{}{E \vdash t = t} \quad (\textbf{trans})\frac{E \vdash t_0 = t_1 \quad E \vdash t_1 = t_2}{E \vdash t_0 = t_2}$$

$$(\textbf{cong})\frac{E \vdash t_0 = t_0' \quad \ldots \quad E \vdash t_n = t_n'}{E \vdash f(t_0, \ldots, t_n) = f(t_0', \ldots, t_n')} \quad (\textbf{E})\frac{t = t' \in E}{E \vdash \sigma(t) = \sigma(t')}$$

Symmetry is intentionally left out.

Soundness and (ω-)Completeness

E is

1. sound when $E \vdash p = q \Rightarrow p \underline{\leftrightarrow} q$;
   (calculation is correct)
2. ground-complete when $p \underline{\leftrightarrow} q \Rightarrow E \vdash p = q$;
   (calculation is sufficient; forget about models)
3. ω-complete when if for all σ, $E \vdash \sigma(s) = \sigma(t) \Rightarrow E \vdash s = t$.
   (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 $E \vdash p = q \Rightarrow p \,\underline{\leftrightarrow}\, q$;
   (calculation is correct)
2. ground-complete when $p \,\underline{\leftrightarrow}\, q \Rightarrow E \vdash p = q$;
   (calculation is sufficient; forget about models)
3. ω-complete when if for all σ, $E \vdash \sigma(s) = \sigma(t) \Rightarrow E \vdash s = t$.
   (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.

CCS without Parallel

$$
\begin{array}{lrcllrcl}
\text{A0} & x+y & = & y+x & \text{A1} & (x+y)+z & = & x+(y+z) \\
\text{A2} & x+x & = & x & \text{A3} & 0+x & = & x
\end{array}
$$

Parallel?

$$a \parallel a \underline{\leftrightarrow} a.a$$

CCS

CCS without Parallel

$$
\begin{array}{llcl}
\mathrm{A0} & x + y & = & y + x \\
\mathrm{A2} & x + x & = & x
\end{array}
\qquad
\begin{array}{llcl}
\mathrm{A1} & (x + y) + z & = & x + (y + z) \\
\mathrm{A3} & 0 + x & = & x
\end{array}
$$

Parallel?

$$a \mid\mid a \underline{\leftrightarrow} a.a$$

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

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

where $a^{\leq i} = a + \ldots + a^i$, $a^0 = 0$ and 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

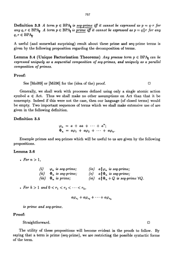
- For sufficiently large m, one cannot prove

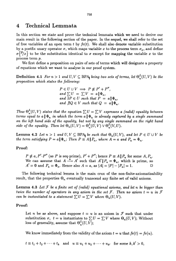
$$E \vdash \sum_{1 \leq i \leq m} a.a^{\leq i} \parallel a \quad = \quad a.(\sum_{1 \leq i \leq m} a.a^{\leq i}) + \sum_{1 \leq i \leq m} a.(a^{\leq i} \parallel a)$$

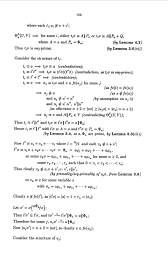
where $a^{\leq i} = a + \ldots + a^{i}$, $a^{0} = 0$ and and $a^{i} = a.a^{i-1}$

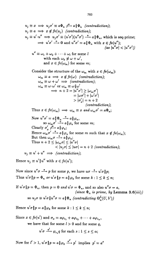
Unaxiomatizability

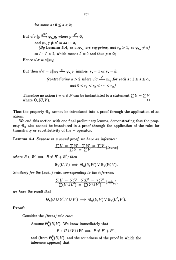
Moller's Proof Sketch

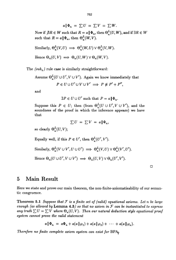












Unaxiomatizability

Beyond CCS and Bisimilarity

Most other unaxiomatizability proofs are as difficult and tedious.

Goal

1. Take the calculus of your choice Σ_e;
2. Take the behavioral pre-order of your choice $\lesssim_e$;
3. Give a well-behaved reduction from $\mathcal{T}(\Sigma_e)$ to *CCS* terms (or any other unaxiomatizable calculus).
4. AFIM meta-theorem guarantees unaxiomatizability!

Reduction

$\widehat{\_} : \mathcal{T}(\Sigma_e) \to \mathcal{T}(\Sigma_o)$ is a reduction from Σ_e to Σ_o, when $\forall_{t,u \in \mathcal{T}(\Sigma_e)}$,

1. $t \sim_e u \Rightarrow \widehat{t} \sim_o \widehat{u}$ and
2. $E \vdash t = u \Rightarrow \widehat{E} \vdash \widehat{t} = \widehat{u}$.

$$\widehat{E} \doteq \{\widehat{t} = \widehat{u} \mid t = u \in E\}.$$

Structural Mapping

$\widehat{\_} : \mathcal{T}(\Sigma_e) \rightarrow \mathcal{T}(\Sigma_o)$ is structural, when $\widehat{\sigma(t)} \equiv \widehat{\sigma}(\widehat{t})$,
where $\widehat{\sigma} \doteq \{x \mapsto \widehat{\sigma(x)}\}$.

Lemma. For a structural mapping $\widehat{\_}$, $E \vdash t = u \Rightarrow \widehat{E} \vdash \widehat{t} = \widehat{u}$.

E-reflecting

Given an axioms system E on $\mathcal{T}(\Sigma_o)$, a reduction $\widehat{\_}$ is E-reflecting, when for each $t = u \in E$, there exists a sound equation $t' = u'$ on $\mathcal{T}(\Sigma_e)$ w.r.t. $\sim_e$ such that $\widehat{t'} \equiv t$ and $\widehat{u'} \equiv u$.

Main Theorem

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 Σ_e to Σ_o

then $\mathcal{T}(\Sigma_e)/\sim_e$ affords no finite axiomatization.

Basic Theory (Recap)

Syntax

$$P \quad ::= \quad 0 \mid a.P \mid P + P \mid P \parallel P$$

Moller's Equations

One cannot prove the following set of sound axioms w.r.t. CCS/ $\underline{\leftrightarrow}$:

$$\mathcal{M} = \{\textstyle\sum_{1 \leq i \leq m} a.a^{\leq i} \parallel a \quad = \quad a.(\sum_{1 \leq i \leq m} a.a^{\leq i}) + \sum_{1 \leq i \leq m} a.(a^{\leq i} \parallel a) \mid m \in N\}$$

Syntax (Σ_e)

$$P \quad ::= \quad 0 \mid \underline{\alpha}.P \mid \underline{\epsilon(1)}.P \mid P + P \mid P \parallel P$$

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

Semantics

$$(\mathbf{tn})\ \frac{}{0 \stackrel{\epsilon(1)}{\longrightarrow} 0} \qquad (\mathbf{a})\ \frac{}{\underline{\alpha}.x \stackrel{\alpha}{\longrightarrow} x}$$

$$(\mathbf{dd0})\ \frac{}{\underline{\epsilon(1)}.x \stackrel{\epsilon(1)}{\longrightarrow} x} \qquad (\mathbf{dd1})\ \frac{x \stackrel{\alpha}{\longrightarrow} y}{\underline{\epsilon(1)}.x \stackrel{\alpha}{\longrightarrow} y}$$

$$(\mathbf{c0})\ \frac{x_0 \stackrel{\chi}{\longrightarrow} y}{x_0 + x_1 \stackrel{\chi}{\longrightarrow} y} \qquad (\mathbf{tc})\ \frac{x_0 \stackrel{\epsilon(1)}{\longrightarrow} y_0 \quad x_1 \stackrel{\epsilon(1)}{\longrightarrow} y_1}{x_0 + x_1 \stackrel{\epsilon(1)}{\longrightarrow} y_0 + y_1}$$

$$(\mathbf{p0})\ \frac{x_0 \stackrel{\chi}{\longrightarrow} y_0}{x_0 \mid\mid x_1 \stackrel{\chi}{\longrightarrow} y_0 \mid\mid x_1} \quad (\mathbf{p2})\ \frac{x_0 \stackrel{\mu}{\longrightarrow} y_0 \quad x_1 \stackrel{\overline{\mu}}{\longrightarrow} y_1}{x_0 \mid\mid x_1 \stackrel{\tau}{\longrightarrow} y_0 \mid\mid y_1} \quad (\mathbf{tp})\ \frac{x_0 \stackrel{\epsilon(1)}{\longrightarrow} y_0 \quad x_1 \stackrel{\epsilon(1)}{\longrightarrow} y_1}{x_0 \mid\mid x_{\underline{1}} \stackrel{\epsilon(1)}{\longrightarrow} y_0 \mid\mid y_1}$$

$$\chi \in A \cup \overline{A} \cup \{\tau, \epsilon(1)\},\ \alpha \in A \cup \overline{A} \cup \{\tau\}, \mu \in A \cup \overline{A}$$

Faster-Than

The faster-than pre-order is the largest relation $\sqsupseteq$ satisfying $\forall_{p,q}\ p \sqsupseteq q$ whenever:

1. $\forall_{p'}\ p \xrightarrow{a} p' \Rightarrow \exists_{q'} q \xrightarrow{a} q' \wedge p' \sqsupseteq q'$,
2. $\forall_{q'}\ q \xrightarrow{a} q' \Rightarrow \exists_{p'} p \xrightarrow{a} p' \wedge p' \sqsupseteq q'$ and
3. $\forall_{p'}\ p \xrightarrow{\epsilon(1)} p' \Rightarrow \mathcal{U}(p) \subseteq \mathcal{U}(q) \wedge \exists_{q'} q \xrightarrow{\epsilon(1)} q' \wedge p' \sqsupseteq q'$.

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

Reduction from $TACS^{UT}$ to CCS

$$\widehat{0} = 0 \qquad \widehat{x} = x$$

$$\widehat{\underline{a}.t} = a.\widehat{t} \qquad \widehat{\underline{\alpha}.t} = 0 \text{ for } \alpha \neq a$$

$$\widehat{\underline{\epsilon(1)}.t} = \widehat{t} \qquad \widehat{t + u} = \widehat{t} + \widehat{u} \qquad \widehat{t \,||\, u} = \widehat{t} \,||\, \widehat{u}$$

Meta-Theorem: Applied to $TACS^{UT}$

1. $t \sqsupseteq u \Rightarrow \widehat{t} \underline{\leftrightarrow} \widehat{u}$,
2. $\widehat{\_}$ is structural,
3. all Moller's axioms in $\mathcal{M}$ are sound w.r.t. $\sqsupseteq$ and remain intact under $\widehat{\_}$,

thus $TACS^{UT}/\sqsupseteq$ 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

Free Lunch?

CCS_Ω: Syntax

$$P ::= 0 \mid \Omega \mid a.P \mid P + P \mid P \,||\, P$$

CCS_Ω: Semantics

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

$$\frac{}{0 \downarrow} \qquad \frac{}{a.p \downarrow} \qquad \frac{p \downarrow \quad q \downarrow}{p + q \downarrow} \qquad \frac{p \downarrow \quad q \downarrow}{p \,||\, q \downarrow}$$

N.B. for each CCS process p, $p \downarrow$.

Free Lunch?

Prebisimilarity

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

1. $\forall_{p'}, p \xrightarrow{a} p'$ then $\exists_{q'}\ q \xrightarrow{a} q'$ and $p' \precsim_{pre} q'$;
2. $p \downarrow$, then
   1. $q \downarrow$ and
   2. $\forall_{q'}, q \xrightarrow{a} q', \exists_{p'}\ p \xrightarrow{a} p'$ and $p' \precsim_{pre} q'$.

N.B. $\forall_p\ \Omega \precsim_{pre} p$.

Free Lunch?

No Free Lunch (at least with Moller)

- Suppose $\widehat{-}$ is a reduction from CCS_Ω to CCS;
- $\forall_p\ \Omega \mathrel{\underset{\sim}{\sqsubset}}_{pre} p$, hence, $\widehat{\Omega} \mathrel{\underline{\leftrightarrow}} \widehat{p}$;
- thus, $\widehat{-}$ is a constant function modulo $\underline{\leftrightarrow}$;
- For $m \neq n$ it does not hold that $\sum_{1 \leq i \leq m} a.a^{\leq i} \parallel a \mathrel{\underline{\leftrightarrow}} \sum_{1 \leq i \leq n} a.a^{\leq i} \parallel a$;
- Hence, $\widehat{-}$ cannot be $\mathcal{M}$-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.