Modular Semantics for Open Transition Rules with Negative Premises

Martin Churchill, Peter D. Mosses, Mohammad Reza Mousavi
Swansea University Halmstad University

Queen Mary University of London
June 2013

Structural Operational Semantics and Negative Premises

- Structural Operational Semantics specifies a transition (evaluation) relation ($\xrightarrow{l}$) via *inductive rules*.
- Sometimes, authors of process algebras like to use negative premises. E.g.:

$$\frac{x \xrightarrow{l} x'}{x; y \xrightarrow{l} x'; y} \qquad \frac{\{x \stackrel{l}{\nrightarrow}\}_l \quad y \xrightarrow{m} y'}{x; y \xrightarrow{m} y'}$$

- Sometimes negative premises are needed, e.g. certain priority operators inexpressible using just positive premises [Aceto and Ingólfsdóttir(2008)].

Semantics of Systems with Negative Premises?

- No longer a simple inductive definition of provable transitions.
- Potential pitfalls, e.g. rules like $\dfrac{a \stackrel{l}{\nrightarrow}}{a \stackrel{l}{\longrightarrow} b}$
- Various approaches, that of *well-supported proofs* is a popular & powerful notion [Glabbeek(2004)]
- Is *incomplete* for pathological examples like that above
  - neither $\overline{a \stackrel{l}{\nrightarrow}}$ nor $\overline{a \stackrel{l}{\longrightarrow} b}$ are derivable
  - by restricting attention to complete specifications, one achieves a 2-valued TSS

Towards open formulae

- Well-supported proof only works for closed formulas
  - Asserting provability of $s \xrightarrow{l} s'$ or $s \stackrel{l}{\nrightarrow}$ for closed s,s'.
- We wish to extend the notion to open formulae, with hypotheses are variables. e.g.

$$\frac{\{x \stackrel{l}{\nrightarrow}\}_l \qquad \{y \stackrel{l}{\nrightarrow}\}_l \qquad z \xrightarrow{m} z'}{(x;y);z \xrightarrow{m} z'}$$

Towards open formulae

- Well-supported proof only works for closed formulas
  - Asserting provability of $s \xrightarrow{l} s'$ or $s \stackrel{l}{\nrightarrow}$ for closed s,s'.
- We wish to extend the notion to open formulae, with hypotheses are variables. e.g.

$$\frac{\{x \stackrel{l}{\nrightarrow}\}_l \qquad \{y \stackrel{l}{\nrightarrow}\}_l \qquad z \xrightarrow{m} z'}{(x;y);z \xrightarrow{m} z'}$$

- Why?
  - To support (open) *operational laws* via (fh-)bisimulation which remain valid under disjoint extensions [Mosses et al.(2010)Mosses, Mousavi, and Reniers]
  - e.g. $(x;y);z \sim x;(y;z)$

Contribution

A notion of **well-supported proof for open transition rules** satisfying various desirable properties:

- Consistency ($\overline{s \xrightarrow{l} s'}$ and $\overline{s \overset{l}{\nrightarrow}}$ can't both be provable)
- Instantiation closure (if $\overline{s}$ is provable then so is $\overline{\sigma(s)}$)
- Agrees with original notion on closed terms
- Modularity (under disjoint extensions, old proofs remain valid)
- Conservativity (under disjoint extensions, no new proofs of old formulae)

Well-Supported Proofs

Basic Notions

Transition System Specifications have:

- A signature Σ and set of labels L.
- *Formulas* ϕ are of the form $s \xrightarrow{l} s'$ or $s \stackrel{l}{\nrightarrow}$ where s, s' are Σ-terms and $l \in L$.
  - $s \xrightarrow{l} s'$ *denies* $s \stackrel{l}{\nrightarrow}$ and vice-versa.
- A set of deduction rules $\dfrac{H}{s \xrightarrow{l} s'}$ over such formulas.

A *derivation* of a transition rule $\frac{H}{\phi}$ is an inductive proof using rules in D with open leaves/hypotheses (possibly negative) in H.

Ground well-supported proof

A *ground well-supported proof* of $\overline{\phi}$ is a upwardly branching tree labelled by closed formulae and rooted at ϕ, where:

- Positive steps $\dfrac{K}{s \xrightarrow{l} s'}$ are instances of deduction rules
- For negative steps $\dfrac{K}{s \overset{l}{\nrightarrow}}$, it must be the case that:

Each derivation of $\dfrac{N}{s \xrightarrow{l} s'}$, ($N$ negative)
contains some formula which denies a formula in K

Negative steps work by refuting each possible derivation.

Closed-Instance Semantics

- As we will see, the above definition doesn't work for open formulae / transition rules.
- An alternative is *closed-instance semantics*: ϕ holds for open ϕ if all closed instantiations $\sigma(\phi)$ holds.
- But this fails to be *modular*:
  - In a base system with single rule $\frac{x \stackrel{b}{\nrightarrow}}{f(x) \xrightarrow{a} x}$, $\overline{f(x) \xrightarrow{a} x}$ holds.
  - But disjointly adding $\overline{1 \xrightarrow{b} 1}$ invalidates the formula.

Towards open formulae

Example

Consider a TSS with deduction rules $\dfrac{f(x) \stackrel{a}{\nrightarrow}}{g(x) \xrightarrow{a} x}$, $\overline{f(0) \xrightarrow{a} 0}$. *Then:*

- $\overline{f(1) \stackrel{a}{\nrightarrow}}$ *and* $\overline{g(1) \xrightarrow{a} 1}$ *have well-supported proofs.*
- *The derivation* $\overline{f(0) \xrightarrow{a} 0}$ *ensures that neither* $\overline{f(0) \stackrel{a}{\nrightarrow}}$ *nor* $\overline{g(0) \xrightarrow{a} 0}$ *are provable.*
- $\overline{f(x) \stackrel{a}{\nrightarrow}}$ *is provable... shouldn't be, due to the derivation* $\overline{f(0) \xrightarrow{a} 0}$ *which denies an instance of* $f(x) \stackrel{a}{\nrightarrow}$.

Towards open formulae

Example

Consider a TSS with deduction rules $\frac{f(x) \stackrel{a}{\nrightarrow}}{g(x) \xrightarrow{a} x}$, $\overline{f(0) \xrightarrow{a} 0}$. *Then:*

- $\overline{f(1) \stackrel{a}{\nrightarrow}}$ *and* $\overline{g(1) \xrightarrow{a} 1}$ *have well-supported proofs.*
- *The derivation* $\overline{f(0) \xrightarrow{a} 0}$ *ensures that neither* $\overline{f(0) \stackrel{a}{\nrightarrow}}$ *nor* $\overline{g(0) \xrightarrow{a} 0}$ *are provable.*
- $\overline{f(x) \stackrel{a}{\nrightarrow}}$ *is provable... shouldn't be, due to the derivation* $\overline{f(0) \xrightarrow{a} 0}$ *which denies an instance of* $f(x) \stackrel{a}{\nrightarrow}$.

$\Rightarrow$ We must consider counterexamples up to substitution: otherwise, $\overline{g(x) \xrightarrow{a} x}$ provable, but $\overline{g(0) \xrightarrow{a} 0}$ unprovable.

Well-supported proofs for open formulas

We next adapt the notion of well-supported proof to open transition rules $\frac{H}{\phi}$ where H is a context:

- H gives assumptions on variables ($x \xrightarrow{l} s$, $x \stackrel{l}{\nrightarrow}$).

Well-supported proofs for open formulas

A *well-supported proof* of $\frac{H}{\phi}$ is a upwardly branching tree labelled by formulae and rooted at ϕ, where:

- Leaves are in H
- Positive steps $\dfrac{K}{s \xrightarrow{l} s'}$ are instances of deduction rules
- For negative steps $\dfrac{K}{s \stackrel{l}{\nrightarrow}}$, it must be the case that:

Each derivation of $\dfrac{C}{\sigma(s) \xrightarrow{l} s'}$, $\quad$ (C negative + vars)
contains a formula denying $\sigma(k)$ for some $k \in K$

(Differences from closed version:
H hypotheses, substitutive counter examples.)

Basic Results

Instantiation Closure

Theorem (Closure under Instantiating Formulae)

Suppose $\frac{\{\psi_i : i \in I\}}{\phi}$ *has a well-supported proof.*
Let σ *be a substitution so each* $\frac{K}{\sigma(\psi_i)}$ *has a well-supported proof.*
Then $\frac{K}{\sigma(\phi)}$ *has a well-supported proof.*

Instantiation Closure

Theorem (Closure under Instantiating Formulae)

Suppose $\dfrac{\{\psi_i : i \in I\}}{\phi}$ *has a well-supported proof.*

Let σ *be a substitution so each* $\dfrac{K}{\sigma(\psi_i)}$ *has a well-supported proof.*

Then $\dfrac{K}{\sigma(\phi)}$ *has a well-supported proof.*

Proof: Substitution + pasting of proof trees.

Consistency

Theorem (Consistency)

In any TSS, it can't be the case that $\overline{s \xrightarrow{l} s'}$ *and* $\overline{s \overset{l}{\nrightarrow}}$ *both have well-supported proofs.*

Consistency

Theorem (Consistency)

In any TSS, it can't be the case that $\overline{s \xrightarrow{l} s'}$ and $\overline{s \stackrel{l}{\nrightarrow}}$ both have well-supported proofs.

Proof (contradiction): assume minimal proofs of contradicting formulae. use "root derivation" of positive part with negative part to find smaller contradicting proofs.

Consistency

Theorem (Consistency)

In any TSS, it can't be the case that $\dfrac{}{s \xrightarrow{l} s'}$ *and* $\dfrac{}{s \stackrel{l}{\nrightarrow}}$ *both have well-supported proofs.*

Proof (contradiction): assume minimal proofs of contradicting formulae. use "root derivation" of positive part with negative part to find smaller contradicting proofs.

Generalisation: Some consistency assumptions on $H \Rightarrow$
can't prove both $\dfrac{H}{s \xrightarrow{l} s'}$ and $\dfrac{H}{s \stackrel{l}{\nrightarrow}}$

Modularity

Disjoint Extensions, Modularity

A *disjoint extension* of a TSS is:

- An extension of the signature Σ with new symbols Σ' and labels
- An extension of D with new rules D', each of which is of the form $\dfrac{S}{f(s_1, \ldots, s_n) \xrightarrow{l} t}$ for $f \in D'$.

Disjoint Extensions, Modularity

A *disjoint extension* of a TSS is:

- An extension of the signature Σ with new symbols Σ' and labels
- An extension of D with new rules D', each of which is of the form $\dfrac{S}{f(s_1, \ldots, s_n) \xrightarrow{l} t}$ for $f \in D'$.

Important property: If π is a well-supported proof of $\frac{H}{\phi}$ in T, then remains so in $T \uplus T_1$.

For positive steps $\dfrac{K}{s \xrightarrow{l} s'}$, simple.

Modularity for Negative Steps

For negative steps we need:

$$\frac{K}{s \stackrel{l}{\not\rightarrow}} \text{ is valid in } T_0 \Rightarrow \text{valid in } T_0 \uplus T_1.$$

i.e. each counterexample proving $\dfrac{C}{\sigma(s) \xrightarrow{l} s'}$ must be denied for $\sigma \in T_0 \uplus T_1$

Modularity for Negative Steps

For negative steps we need:

$$\frac{K}{s \stackrel{l}{\nrightarrow}} \text{ is valid in } T_0 \Rightarrow \text{valid in } T_0 \uplus T_1.$$

i.e. each counterexample proving $\dfrac{C}{\sigma(s) \xrightarrow{l} s'}$ must be denied for $\sigma \in T_0 \uplus T_1$

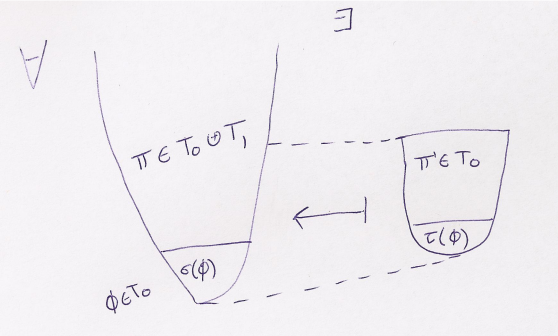
We need to:

- Map potential counterexample derivations in $T_0 \uplus T_1$ back into a T_0 derivation (its "skeleton")

Modularity for Negative Steps

We need to:

- Map potential counterexample derivations in $T_0 \uplus T_1$ back into a T_0 derivation (its "skeleton")



Modularity for well-supported proofs

Theorem (Modularity)

Suppose $T_0 \uplus T_1$ *is a disjoint extension of* T_0 *and let* π *be a well-supported proof for* $\frac{H}{\phi}$ *in* T_0*.*

Then π *is a well-supported proof for* $\frac{H}{\phi}$ *in* $T_0 \uplus T_1$*.*

Conservativity

Source dependence

Now seek to show: in disjoint extensions, no new proofs of old formulae.
Requires *source dependence*:

each variable in a rule can be traced back to a variable in the source of the conclusion (via transitions in the premise)

Ok: $$\frac{x \xrightarrow{l} x'}{x; y \xrightarrow{l} x'; y}$$

Source dependence

Now seek to show: in disjoint extensions, no new proofs of old formulae.
Requires *source dependence*:

each variable in a rule can be traced back to a variable in the source of the conclusion (via transitions in the premise)

Ok: $\dfrac{x \xrightarrow{l} x'}{x; y \xrightarrow{l} x'; y}$

Example

Consider a TSS $\dfrac{x \xrightarrow{b} 1}{0 \xrightarrow{a} 1}$. *Then* $\overline{0 \xrightarrow{a} 1}$ *not provable.*

Extend by constant 2 *with* $\overline{2 \xrightarrow{b} 1}$. *Then* $\overline{0 \xrightarrow{a} 1}$ *is provable.*

Conservativeness for Disjoint Extensions

Theorem (Conservativeness for Disjoint Extensions)

Let $T_0 \uplus T_1$ be a disjoint extension of T_0, where T_0 is source-dependent, and let $\phi \in T_0$. Let π be a well-supported proof of $\frac{H}{\phi}$ in $T_0 \uplus T_1$. Then π is a well-supported proof of $\frac{H}{\phi}$ in T_0.

Proof: induction using "source dependence measure" for positive steps. For negative steps, uses modularity result to move counterexamples from T_0 to $T_0 \uplus T_1$.

Soundness over Closed-instance Semantics

Theorem

For closed ϕ, if $\overline{\phi}$ has a well-supported proof then it has a ground well-supported proof.

Proof: Follows from the fact that $\overline{\phi}$ has a closed well-supported proof (instantiation closure).

Conservativity over Closed-instance Semantics

Needs source dependence:

Example

Consider TSS T with deduction rule $\dfrac{x \xrightarrow{b} 1}{0 \xrightarrow{a} 1}$.
Then $\overline{0 \overset{a}{\nrightarrow}}$ *has a ground well-supported proof (no valid derivations concluding* $0 \xrightarrow{a} \_$*)*
But no well-supported proof in T.

Conservativity over Closed-instance Semantics

Theorem

In a source dependent system and closed ϕ, if $\overline{\phi}$ has a ground well-supported proof then it has a well-supported proof.

Proof: Follows from the fact that each derivation of $s \xrightarrow{l} s'$ for closed s is closed.

Conclusions

Contribution

Our notion satisfies:

- Consistency ($\overline{s \xrightarrow{l} s'}$ and $\overline{s \stackrel{l}{\nrightarrow}}$ can't both be provable)
- Instantiation closure (if $\overline{s}$ is provable then so is $\overline{\sigma(s)}$)
- Modularity (under disjoint extensions, old proofs remain valid)

Assuming source dependent rules:

- Agrees with original notion on closed terms
- Conservativity (under disjoint extensions, no new proofs of old formulae)

Open Algebraic Laws

Consider an algebraic law, like

$$(x; y); z \sim x; (y; z)$$

As the language is (disjointly) extended, the domain of quantification (x,y,z) increases. Ideal:

- we prove such laws in the "minimal subsystem" containing just the rules for ;
- guaranteed to hold in any extension = any system containing this notion of ;

Fh-bisimulation

To prove such laws, we need to consider a notion of bisimulation for open terms satisfying this modularity property.

fh-bisimulation is such a notion:

- if $s\ R\ t$ and $\dfrac{H}{s \xrightarrow{l} s'}$ then $\dfrac{H}{t \xrightarrow{l} t'}$ with $s'\ R\ t'$

(usual 'step' condition, but under arbitrary hypotheses on variables.)

This notion *is* modular – preserved by disjoint extensions. [Mosses et al.(2010)Mosses, Mousavi, and Reniers]

...with negative premises

- The work here can be used to adapt fh-bisimulation to the negative setting.
- Modularity of the underlying well-supported proofs leads to modularity for the proved equations.
- Another key issue: compositionality (bisimulation as a congruence, via rule formats) [Mousavi et al.(2007)Mousavi, Reniers, and Groote]

PLanCompS vision

- A growing repository of fundamental constructs (like ;) specified independently
- Laws about such constructs can be proved once and for all
  - e.g. associativity/commutativity/unit laws
- Formal semantics can be given in an accessible manner by *translation* into funcons
  - Tool support – e.g. running programs
- Computational effects via the mechanics of *Modular SOS* [Mosses(2004), Churchill and Mosses(2013)]

`www.plancomps.org`

Conclusions

We:

- Extended well-supported proofs to open transition rules
- Proved consistency, instantiation, modularity, conservativity results

Further directions:

- Use these results to support modularity of equational laws
- Consider compositionality of fh-bisimulation based on these notions
- ...

Thank You.

Luca Aceto and Anna Ingólfsdóttir.
On the expressibility of priority.
Inf. Process. Lett., 109(1):83–85, 2008.

Martin Churchill and PeterD. Mosses.
Modular bisimulation theory for computations and values.
In Frank Pfenning, editor, *Foundations of Software Science and Computation Structures*, volume 7794 of *Lecture Notes in Computer Science*, pages 97–112. Springer Berlin Heidelberg, 2013.
ISBN 978-3-642-37074-8.
doi: 10.1007/978-3-642-37075-5_7.
URL http://dx.doi.org/10.1007/978-3-642-37075-5_7.

Robert Jan (Rob) van Glabbeek.
The meaning of negative premises in transition system specifications II.
Journal of Logic and Algebraic Programming (JLAP), 60-61:229–258, 2004.

Peter D. Mosses.
Modular structural operational semantics.
J. Log. Algebr. Program., 60-61:195–228, 2004.
doi: 10.1016/j.jlap.2004.03.008.

Peter D. Mosses, Mohammad Reza Mousavi, and Michel A. Reniers.
Robustness of equations under operational extensions.
In Sibylle B. Fröschle and Frank D. Valencia, editors, *EXPRESS'10*, volume 41 of *EPTCS*, pages 106–120, 2010.

MohammadReza Mousavi, Michel A. Reniers, and Jan Friso Groote.
SOS rule formats and meta-theory: 20 years after.
Theoretical Computer Science, 373:238–272, 2007.