Stateful Structural Operational Semantics

$[\![-]\!]$

Stefan Milius
joint work with Sergey Goncharov, Lutz Schröder, Stelios Tsampas, Henning Urbat

Friedrich-Alexander-Universität Erlangen-Nürnberg

IFIP WG 1.3, Lipari, Sept. 6, 2022

Structural Operational Semantics [Plotkin 1981]

Idea: Specify program/process behaviour by inductive transition rules.

$$\frac{p \xrightarrow{a} p'}{p \,||\, q \xrightarrow{a} p' \,||\, q} \qquad \frac{q \xrightarrow{a} q'}{p \,||\, q \xrightarrow{a} p \,||\, q'}$$

Key issue: **compositionality** – is behavioural equivalence a congruence?

$$\underbrace{p_i \sim q_i \quad (i = 1, \ldots, n) \quad \Longrightarrow \quad \mathsf{f}(p_1, \ldots, p_n) \sim \mathsf{f}(q_1, \ldots, q_n) \qquad (\mathsf{f} \in \Sigma)}_{\text{Typically long and complex proof } ☹}$$

Goal: Rule formats that guarantee compositionality!

GSOS

GSOS rules [Bloom, Istrail & Mayer 1995]:

$$\frac{\{p_i \xrightarrow{a} q_{ij}\}_{i,j,a} \quad \{p_i \stackrel{b}{\not\to}\}_{i,b}}{\mathsf{f}(p_1,\ldots,p_n) \xrightarrow{c} t(\ldots,p_i,\ldots,q_{ij}^a,\ldots)} \qquad (f \in \Sigma)$$

...guarantee compositionality with respect to bisimilarity.

Categorically [Turi & Plotkin 1997]: Natural Transformations

$$\underbrace{\Sigma(X \times (\mathcal{P}_\mathsf{f} X)^L)}_{\text{premisses}} \longrightarrow \underbrace{(\mathcal{P}_\mathsf{f}\Sigma^* X)^L}_{\text{conclusion}} \qquad (X \in \mathsf{Set})$$

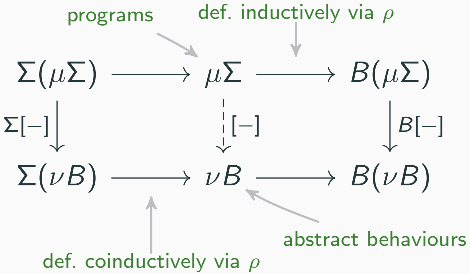
Abstract GSOS law of $\Sigma\colon \mathcal{C} \to \mathcal{C}$ over $B\colon \mathcal{C} \to \mathcal{C}$

$$\Sigma(X \times BX) \longrightarrow B\Sigma^* X \qquad (X \in \mathcal{C})$$

Abstract GSOS [Turi & Plotkin 1997]

$$\rho_X \colon \Sigma(X \times BX) \longrightarrow B\Sigma^* X \qquad (X \in \mathcal{C})$$

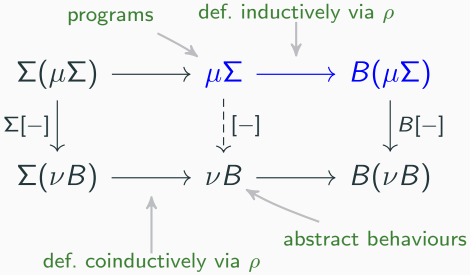
Operational model, denotational model, semantics for free!



Abstract GSOS [Turi & Plotkin 1997]

$$\rho_X \colon \Sigma(X \times BX) \to B\Sigma^* X \qquad (X \in \mathcal{C})$$

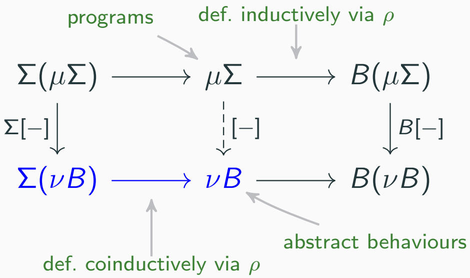
Operational model, denotational model, semantics for free!



Abstract GSOS [Turi & Plotkin 1997]

$$\rho_X \colon \Sigma(X \times BX) \longrightarrow B\Sigma^* X \qquad (X \in \mathcal{C})$$

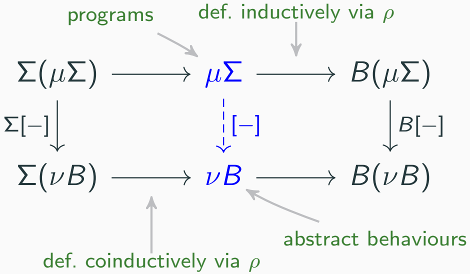
Operational model, denotational model, semantics for free!



Abstract GSOS [Turi & Plotkin 1997]

$$\rho_X \colon \Sigma(X \times BX) \to B\Sigma^* X \qquad (X \in \mathcal{C})$$

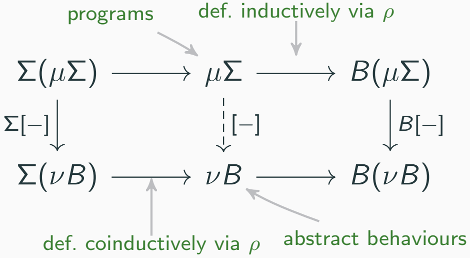
Operational model, denotational model, semantics for free!



Abstract GSOS [Turi & Plotkin 1997]

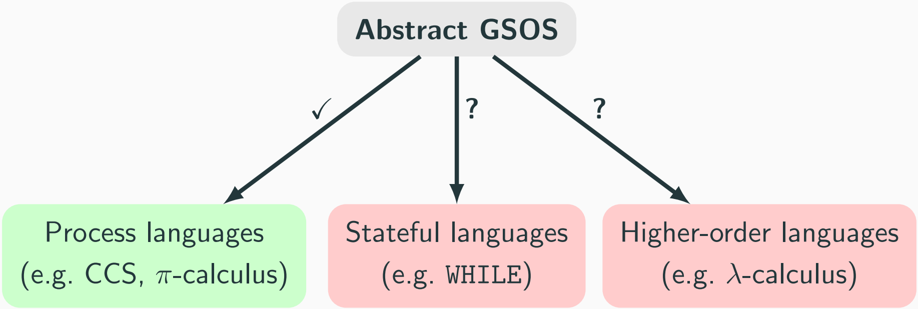
$$\rho_X \colon \Sigma(X \times BX) \to B\Sigma^* X \qquad (X \in \mathcal{C})$$

Operational model, denotational model, semantics for free!

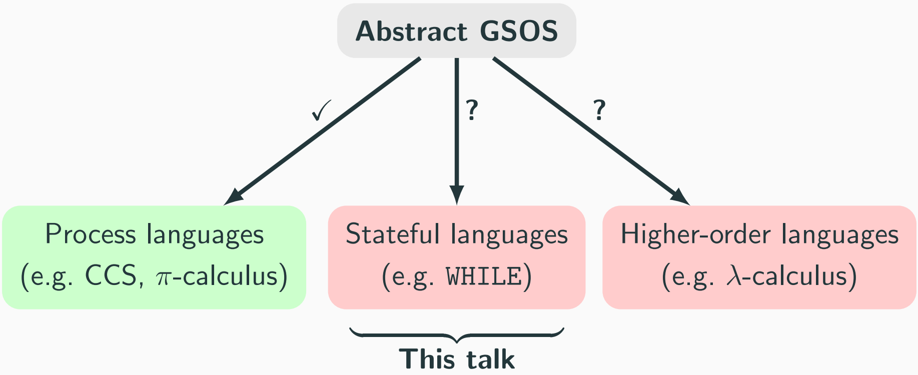


Compositionality for free: $[-]$ is a Σ-algebra morphism!

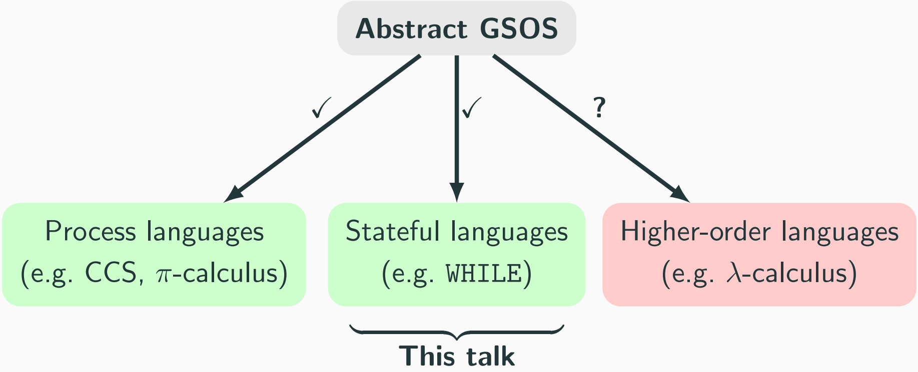
Abstract GSOS: Applications



Abstract GSOS: Applications



Abstract GSOS: Applications



WHILE Language: SOS Specification

$$\texttt{skip}\ \frac{}{s, \texttt{skip} \downarrow s}$$

$$\texttt{asn}\ \frac{}{s, (x := e) \downarrow s_{[x \leftarrow [e]_s]}}$$

$$\texttt{while1}\ \frac{}{s, \texttt{while}\ e\ p \downarrow s}\ [e]_s = 0$$

$$\texttt{while2}\ \frac{}{s, \texttt{while}\ e\ p \rightarrow s, (p;\ \texttt{while}\ e\ p)}\ [e]_s \neq 0$$

$$\texttt{seq1}\ \frac{s, p \downarrow s'}{s, (p;\ q) \rightarrow s', q}$$

$$\texttt{seq2}\ \frac{s, p \rightarrow s', p'}{s, (p;\ q) \rightarrow s', (p';\ q)}$$

with finite support
$\{x \in \mathsf{Vars} : s(x) \neq 0\}$

$$s, s' \in \mathsf{States} \quad (= \mathsf{Vars} \rightarrow \mathbb{N})$$

Stateful SOS

Σ (signature), $\quad S$ (set of states)

A **stateful SOS specification** is a set of rules of the form

$$\frac{\{s, p_i \to s_i, q_i\}_{i \in W} \quad \{s, p_i \downarrow s_i\}_{i \notin W}}{s, \mathsf{f}(p_1, \ldots, p_n) \to s', t(\ldots, p_i, q_i, \ldots) \textbf{ or } \downarrow s'}$$

(exactly one rule for each $\mathsf{f} \in \Sigma$, states $s, s_1, \ldots, s_n$ and $W \subseteq \{1, \ldots, n\}$).

Categorically: stateful SOS laws

$$\lambda_X : \underbrace{S \times \Sigma(X \times S \times (X + 1))}_{\text{premisses}} \longrightarrow \underbrace{S \times (\Sigma^* X + 1)}_{\text{conclusion}} \qquad (X \in \mathrm{Set}).$$

$\texttt{WHILE}$ Language: SOS Specification

$$\texttt{skip}\ \frac{}{s, \texttt{skip} \downarrow s}$$

$$\texttt{asn}\ \frac{}{s, (x := e) \downarrow s_{[x \leftarrow [e]_s]}}$$

$$\texttt{while1}\ \frac{}{s, \texttt{while}\ e\ p \downarrow s}\ [e]_s = 0$$

$$\texttt{while2}\ \frac{}{s, \texttt{while}\ e\ p \to s, (p;\ \texttt{while}\ e\ p)}\ [e]_s \neq 0$$

$$\texttt{seq1}\ \frac{s, p \downarrow s'}{s, (p;\ q) \to s', q}$$

$$\texttt{seq2}\ \frac{s, p \to s', p'}{s, (p;\ q) \to s', (p';\ q)}$$

Stateful SOS specification (up to completing premisses)

From Stateful SOS to Abstract GSOS

$$\lambda_X : S \times \Sigma(X \times S \times (X+1)) \to S \times (\Sigma^* X + 1)$$

induces abstract GSOS law

$$\rho_X \colon \Sigma(X \times BX) \to B\Sigma^* X \quad \text{where} \quad BX = (S \times (X+1))^S$$

Operational model ($\mu\Sigma$), denotational model (νB), compositionality

$$\begin{array}{ccccc}
\Sigma(\mu\Sigma) & \longrightarrow & \mu\Sigma & \longrightarrow & B(\mu\Sigma) \\
{\scriptstyle \Sigma[-]}\downarrow & & \downarrow{\scriptstyle [-]} & & \downarrow{\scriptstyle B[-]} \\
\Sigma(\nu B) & \longrightarrow & \nu B & \longrightarrow & B(\nu B)
\end{array}$$

Resumption Semantics

$$\begin{array}{ccccc} \Sigma(\mu\Sigma) & \longrightarrow & \mu\Sigma & \longrightarrow & B(\mu\Sigma) \\ {\scriptstyle \Sigma[-]}\downarrow & & \downarrow{\scriptstyle [-]} & & \downarrow{\scriptstyle B[-]} \\ \Sigma(\nu B) & \longrightarrow & \nu B & \longrightarrow & B(\nu B) \end{array}$$

For $BX = (S \times (X + 1))^S$:

$$\nu B = |S|\text{-branching } S\text{-labelled possibly infinite trees.}$$

This yields a **resumption semantics**: programs run in an environment that can observe and modify intermediate states.

Example (`WHILE`)

$$[\![\mathrm{x} := 1;\ \mathrm{x} := \mathrm{x} + 1]\!] \quad \neq \quad [\![\mathrm{x} := 1;\ \mathrm{x} := \mathrm{x} * 2]\!]$$

Resumption Semantics

$$\begin{array}{ccccc}
\Sigma(\mu\Sigma) & \longrightarrow & \mu\Sigma & \longrightarrow & B(\mu\Sigma) \\
\Sigma[-]\downarrow & & \downarrow [-] & & \downarrow B[-] \\
\Sigma(\nu B) & \longrightarrow & \nu B & \longrightarrow & B(\nu B)
\end{array}$$

For $BX = (S \times (X + 1))^S$:

$$\nu B = |S|\text{-branching } S\text{-labelled possibly infinite trees.}$$

This yields a **resumption semantics**: programs run in an environment that can observe and modify intermediate states.

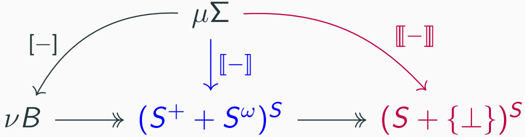
Example (WHILE)

$$\left[\mathrm{x} := 1;\ \mathrm{x} := \mathrm{x} + 1\right] \quad \neq \quad \left[\mathrm{x} := 1;\ \mathrm{x} := \mathrm{x} * 2\right]$$

Usually too fine-grained! Coarser semantic domains?

Semantic Domains for Stateful SOS

Every stateful SOS specification yields three semantics (def. coinductively):



Resumption semantics: Env. can observe/modify intermediate states.

Trace semantics: Env. can observe intermediate states.

Termination semantics: Env. can only observe the final state (if any).

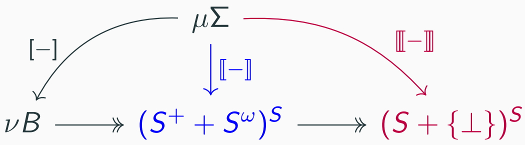
Example (WHILE)

$$[\![x := 1;\ x := x + 1]\!] \quad = \quad [\![x := 1;\ x := x * 2]\!]$$

$$[\![x := 1;\ x := 2]\!] \quad \neq \quad [\![x := 2;\ x := 2]\!]$$

$$[\![x := 1;\ x := 2]\!] \quad = \quad [\![x := 2;\ x := 2]\!]$$

Semantic Domains for Stateful SOS



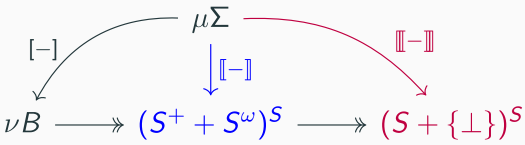
Are these three semantics compositional?

$$[p_i] = [q_i] \quad (i = 1, \ldots, n) \quad \stackrel{?}{\Longrightarrow} \quad [\mathsf{f}(p_1, \ldots, p_n)] = [\mathsf{f}(q_1, \ldots, q_n)]$$

$$[\![p_i]\!] = [\![q_i]\!] \quad (i = 1, \ldots, n) \quad \stackrel{?}{\Longrightarrow} \quad [\![\mathsf{f}(p_1, \ldots, p_n)]\!] = [\![\mathsf{f}(q_1, \ldots, q_n)]\!]$$

$$[\![\![p_i]\!]\!] = [\![\![q_i]\!]\!] \quad (i = 1, \ldots, n) \quad \stackrel{?}{\Longrightarrow} \quad [\![\![\mathsf{f}(p_1, \ldots, p_n)]\!]\!] = [\![\![\mathsf{f}(q_1, \ldots, q_n)]\!]\!]$$

Semantic Domains for Stateful SOS



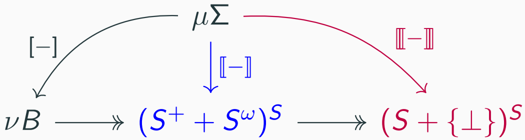
Are these three semantics compositional?

$$[p_i] = [q_i] \quad (i = 1, \dots, n) \quad \overset{\checkmark}{\underset{\text{TP'97}}{\Longrightarrow}} \quad [\mathsf{f}(p_1, \dots, p_n)] = [\mathsf{f}(q_1, \dots, q_n)]$$

$$[\![p_i]\!] = [\![q_i]\!] \quad (i = 1, \dots, n) \quad \overset{\times}{\Longrightarrow} \quad [\![\mathsf{f}(p_1, \dots, p_n)]\!] = [\![\mathsf{f}(q_1, \dots, q_n)]\!]$$

$$[\![\![p_i]\!]\!] = [\![\![q_i]\!]\!] \quad (i = 1, \dots, n) \quad \overset{\times}{\Longrightarrow} \quad [\![\![\mathsf{f}(p_1, \dots, p_n)]\!]\!] = [\![\![\mathsf{f}(q_1, \dots, q_n)]\!]\!]$$

Compositionality



Example (Compositionality fails for for $[\![-]\!]$ and $[\![\![-]\!]\!]$)

Extend `WHILE` by adding a unary operator $u(\cdot)$ with

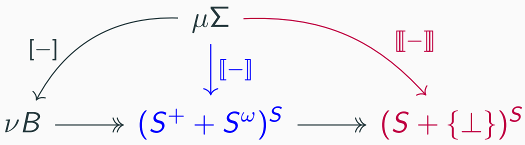
$$\frac{s, p \to s', p'}{s, u(p) \to 0, u(p')} \qquad \frac{s, p \downarrow s'}{s, u(p) \downarrow s'}$$

For $t_1 = \big(\mathrm{x} := 1;\ \mathrm{x} := \mathrm{x} + 1\big)$ and $t_2 = \big(\mathrm{x} := 1;\ \mathrm{x} := \mathrm{x} * 2\big)$ we have

$$[\![t_1]\!] = [\![t_2]\!] \qquad \text{but} \qquad [\![u(t_1)]\!] \neq [\![u(t_2)]\!],$$

$$[\![\![t_1]\!]\!] = [\![\![t_2]\!]\!] \qquad \text{but} \qquad [\![\![u(t_1)]\!]\!] \neq [\![\![u(t_2)]\!]\!].$$

Compositionality



Theorem

Compositionality is undecidable for $[\![-]\!]$ and $[\![\![-]\!]\!]$.

Proof (reduction from halting problem): Form stateful SOS spec.

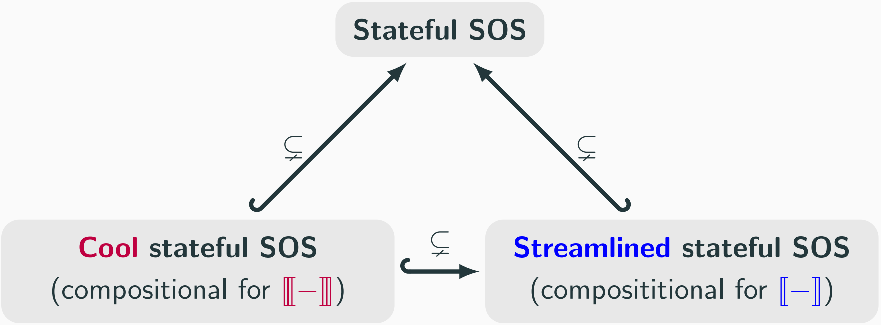
'composition'

$\mathcal{S} \quad = \quad$ Spec. of run of TM $\xrightarrow{\circ}$ non-compositional spec.

Then TM halts $\iff$ $\mathcal{S}$ non-compositional. $\square$

Streamlining and Cooling Stateful SOS

We devise two restrictions of stateful SOS that guarantee compositionality:



cf. van Glabbeek 2005, Abou-Saleh & Pattinson 2011

Streamlined Stateful SOS

Streamlined Stateful SOS

Stateful SOS

$$\frac{\{s, p_i \to s_i, q_i\}_{i \in W} \quad \{s, p_i \downarrow s_i\}_{i \notin W}}{s, \mathrm{f}(p_1, \ldots, p_n) \to s', t(\ldots, p_i, q_i, \ldots) \textbf{ or } \downarrow s'}$$

Passive operator f $\in \Sigma$**:** given by rule of the form

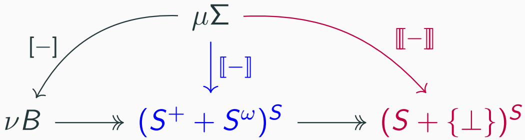
$$\frac{}{s, \mathrm{f}(p_1, \ldots, p_n) \to s', t(p_1, \ldots, p_n) \textbf{ or } \downarrow s'}$$

Streamlined spec.: For active f, rules have the following forms (j fixed):

$$\frac{\cdots \quad s, p_j \to s_j, q_j \quad \cdots}{s, \mathrm{f}(p_1, \ldots, p_j, \ldots, p_n) \to s_j, \mathrm{f}(p_1, \ldots, q_j, \ldots, p_n) \ \textbf{ or } \ s_j, q_j}$$

$$\frac{\{s, p_i \to s_i, q_i\}_{i \in W} \quad \{s, p_i \downarrow s_i\}_{i \notin W}}{s, \mathrm{f}(p_1, \ldots, p_j, \ldots, p_n) \to s', t(p_1, \ldots, \sout{p_j}, \ldots, p_n) \textbf{ or } \downarrow s'}$$

Compositionality



Example (Compositionality fails for $[\![-]\!]$)

Extend `WHILE` by adding a unary operator $u(\cdot)$ with

$$\frac{s, p \to s', p'}{s, u(p) \to 0, u(p')} \qquad \frac{s, p \downarrow s'}{s, u(p) \downarrow s'}$$

Not streamlined!

For $t_1 = \big(\mathrm{x} := 1;\ \mathrm{x} := \mathrm{x} + 1\big)$ and $t_2 = \big(\mathrm{x} := 1;\ \mathrm{x} := \mathrm{x} * 2\big)$ we have

$$[\![t_1]\!] = [\![t_2]\!] \qquad \text{but} \qquad [\![u(t_1)]\!] \neq [\![u(t_2)]\!].$$

WHILE Language: SOS Specification

$$\texttt{skip}\ \frac{}{s, \texttt{skip} \downarrow s}$$

$$\texttt{asn}\ \frac{}{s, (x := e) \downarrow s_{[x \leftarrow [e]_s]}}$$

$$\texttt{while1}\ \frac{}{s, \texttt{while}\ e\ p \downarrow s}\ [e]_s = 0$$

$$\texttt{while2}\ \frac{}{s, \texttt{while}\ e\ p \rightarrow s, (p;\ \texttt{while}\ e\ p)}\ [e]_s \neq 0$$

$$\texttt{seq1}\ \frac{s, p \downarrow s'}{s, (p;\ q) \rightarrow s', q}$$

$$\texttt{seq2}\ \frac{s, p \rightarrow s', p'}{s, (p;\ q) \rightarrow s', (p';\ q)}$$

Streamlined!

Streamlined Stateful SOS

Theorem (Compositionality of trace semantics)

For every streamlined stateful SOS specification,

$$[\![p_i]\!] = [\![q_i]\!] \quad (i = 1, \ldots, n) \quad \Longrightarrow \quad [\![\mathsf{f}(p_1, \ldots, p_n)]\!] = [\![\mathsf{f}(q_1, \ldots, q_n)]\!]$$

Streamlined Stateful SOS

Theorem (Compositionality of trace semantics)

For every streamlined stateful SOS specification,

$$[\![p_i]\!] = [\![q_i]\!] \quad (i = 1, \ldots, n) \quad \Longrightarrow \quad [\![\mathsf{f}(p_1, \ldots, p_n)]\!] = [\![\mathsf{f}(q_1, \ldots, q_n)]\!]$$

Example

`WHILE` is streamlined, thus compositional w.r.t. trace semantics.

Example (Interrupt handling)

Extend `WHILE` with an interrupt flag `i` and modify rules to

$$\frac{s, p \to s', p'}{s, (p;\ q) \to s', (p';\ q)}[\mathtt{i}]_s = 0 \qquad \frac{s, p \to s', p'}{s, (p;\ q) \to s', q}[\mathtt{i}]_s \neq 0$$

Still streamlined, thus compositional w.r.t. trace semantics!

Cool Stateful SOS

Cool Stateful SOS

Stateful SOS

$$\frac{\{s, p_i \to s_i, q_i\}_{i \in W} \quad \{s, p_i \downarrow s_i\}_{i \notin W}}{s, \mathsf{f}(p_1, \ldots, p_n) \to s', t(\ldots, p_i, q_i, \ldots) \textbf{ or } \downarrow s'}$$

Passive operator $\mathsf{f} \in \Sigma$**:** given by rule of the form

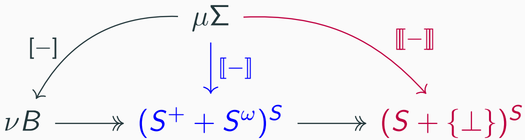
$$\frac{}{s, \mathsf{f}(p_1, \ldots, p_n) \to s', t(p_1, \ldots, p_n) \textbf{ or } \downarrow s'}$$

Cool spec.: For active f, rules have the following forms (for fixed j):

$$\frac{s, p_j \to s_j, q_j}{s, \mathsf{f}(p_1, \ldots, p_j, \ldots, p_n) \to s_j, \mathsf{f}(p_1 \ldots, q_j, \ldots, p_n)}$$

$$\frac{s, p_j \downarrow s'}{s, \mathsf{f}(p_1, \ldots, p_j, \ldots, p_n) \to \underbrace{s'', t}_{\text{depend on } s' \text{ but not } s}(p_1, \ldots, \not{p_j}, \ldots, p_n) \textbf{ or } \downarrow s''}$$

Compositionality



Example (Compositionality fails for $[\![-]\!]$)

Extend `WHILE` by adding a unary operator $u(\cdot)$ with

Uncool!

$$\frac{s, p \to s', p'}{s, u(p) \to 0, u(p')} \qquad \frac{s, p \downarrow s'}{s, u(p) \downarrow s'}$$

For $t_1 = \big(\mathrm{x} := 1;\ \mathrm{x} := \mathrm{x} + 1\big)$ and $t_2 = \big(\mathrm{x} := 1;\ \mathrm{x} := \mathrm{x} * 2\big)$ we have

$$[\![t_1]\!] = [\![t_2]\!] \qquad \text{but} \qquad [\![u(t_1)]\!] \neq [\![u(t_2)]\!].$$

$\texttt{WHILE}$ Language: SOS Specification

$$\texttt{skip}\ \frac{}{s, \texttt{skip} \downarrow s}$$

$$\texttt{asn}\ \frac{}{s, (x := e) \downarrow s_{[x \leftarrow [e]_s]}}$$

$$\texttt{while1}\ \frac{}{s, \texttt{while}\ e\ p \downarrow s}\ [e]_s = 0$$

$$\texttt{while2}\ \frac{}{s, \texttt{while}\ e\ p \rightarrow s, (p\texttt{;}\ \texttt{while}\ e\ p)}\ [e]_s \neq 0$$

$$\texttt{seq1}\ \frac{s, p \downarrow s'}{s, (p\texttt{;}\ q) \rightarrow s', q}$$

$$\texttt{seq2}\ \frac{s, p \rightarrow s', p'}{s, (p\texttt{;}\ q) \rightarrow s', (p'\texttt{;}\ q)}$$

Cool!

Cool Stateful SOS

Theorem (Compositionality of termination semantics)

For every cool stateful SOS specification,

$$[\![p_i]\!] = [\![q_i]\!] \quad (i = 1, \ldots, n) \quad \Longrightarrow \quad [\![\mathsf{f}(p_1, \ldots, p_n)]\!] = [\![\mathsf{f}(q_1, \ldots, q_n)]\!]$$

Cool Stateful SOS

Theorem (Compositionality of termination semantics)

For every cool stateful SOS specification,

$$[\![p_i]\!] = [\![q_i]\!] \quad (i = 1, \ldots, n) \quad \Longrightarrow \quad [\![\mathsf{f}(p_1, \ldots, p_n)]\!] = [\![\mathsf{f}(q_1, \ldots, q_n)]\!]$$

Example

`WHILE` is cool, thus compositional w.r.t. termination semantics.

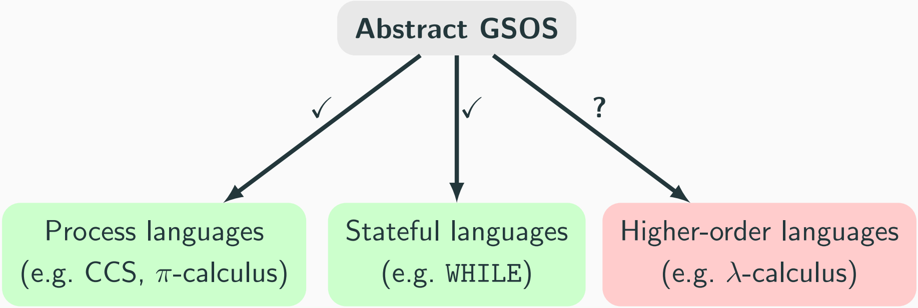
Example (Interrupt handling)

Extend `WHILE` with an interrupt flag `i` and modify rules of `;` to

$$\frac{s, p \to s', p'}{s, (p;\ q) \to s', (p';\ q)}\,[\mathtt{i}]_s = 0 \qquad \frac{s, p \to s', p'}{s, (p;\ q) \to s', q}\,[\mathtt{i}]_s \neq 0$$

Uncool! (but compositional for trace semantics)

Conclusion and Future Work



Stateful SOS

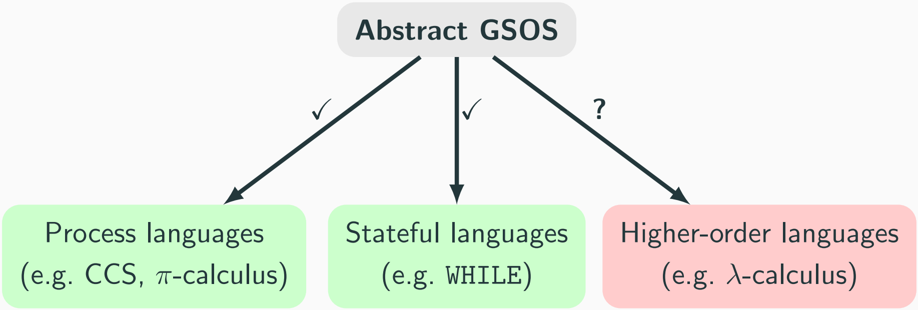
+

Coarser Domains

+

Coolness

Conclusion and Future Work

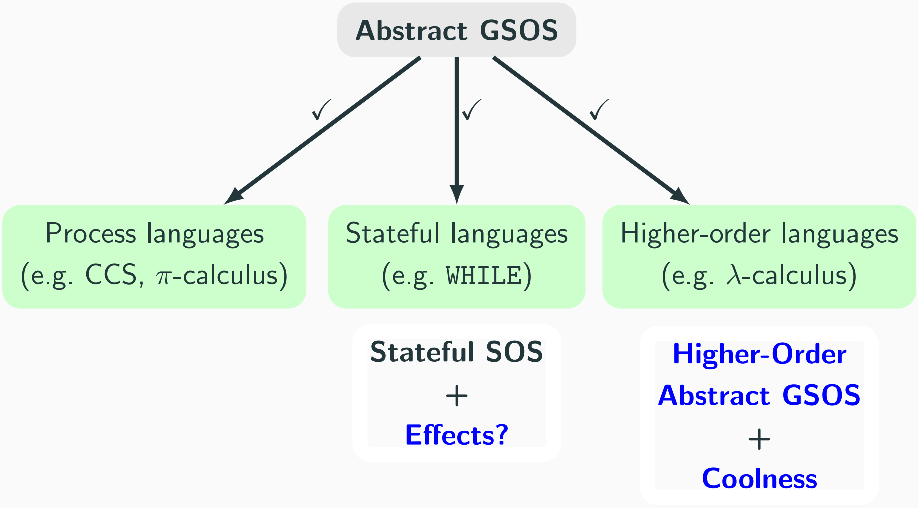


Stateful SOS

$+$

Effects?

Conclusion and Future Work



Appendix

Cool Stateful SOS: Towards a Categorical View

Stateful SOS

$$\frac{\{s, p_i \to s_i, q_i\}_{i \in W} \quad \{s, p_i \downarrow s_i\}_{i \notin W}}{s, \mathsf{f}(p_1, \ldots, p_n) \to s', t(\ldots, p_i, q_i, \ldots) \textbf{ or } \downarrow s'}$$

Passive operator $\mathsf{f} \in \Sigma$**:** given by rule of the form

$$\frac{}{s, \mathsf{f}(p_1, \ldots, p_n) \to s', t(p_1, \ldots, p_n) \textbf{ or } \downarrow s'}$$

Thus, rules for f determined by a natural transformation

$$\pi_X^{\mathsf{f}} \colon S \times X^n \to S \times (\Sigma^* X + 1) \qquad (X \in \mathsf{Set}).$$

Cool Stateful SOS: Towards a Categorical View

Cool spec.: For active f, rules have the following forms (for fixed j):

$$\frac{s, p_j \to s_j, q_j}{s, \mathsf{f}(p_1, \ldots, p_j, \ldots, p_n) \to s_j, \mathsf{f}(p_1 \ldots, q_j, \ldots, p_n)}$$

$$\frac{s, p_j \downarrow s'}{s, \mathsf{f}(p_1, \ldots, p_j, \ldots, p_n) \to \underbrace{s'', t}_{\text{depend on } s' \text{ but not } s}(p_1, \ldots, \cancel{p_j}, \ldots, p_n) \textbf{ or } \downarrow s''}$$

Thus, rules for active f determined by a natural transformation

$$\alpha^{\mathsf{f}}_X \colon S \times X^{j-1} \times 1 \times X^{n-j} \to S \times (\Sigma^* X + 1) \qquad (X \in \mathrm{Set}).$$

Natural transformations α^{f}_X and π^{f}_X (for f passive) yield stateful SOS law

$$\lambda_X \colon S \times \Sigma(X \times S \times (X + 1)) \to S \times (\Sigma^* X + 1) \qquad (X \in \mathrm{Set}).$$

Categorical proof/generalization of compositionality results?