Operational Game Semantics (OGS) formally: Let's talk about chattering

Peio Borthelle, LAMA, Univ. Savoie Mont Blanc, CNRS, France
Tom Hirschowitz, LAMA, Univ. Savoie Mont Blanc, CNRS, France
Guilhem Jaber, LS2N, Nantes Université, France
Yannick Zakowski, LIP, ENS de Lyon, Inria, France

GALOP'24 — 2024/01/14

A bit of context

Original motivation: interactive semantics for FFI

Step 1: use OGS, prove soundness…

A bit of context

Original motivation: interactive semantics for FFI

Step 1: use OGS, prove soundness…

… formally (programming is the only way I like math)

A bit of context

Original motivation: interactive semantics for FFI

Step 1: use OGS, prove soundness…

… formally (programming is the only way I like math)

… this is actually kind of tricky?! (me, one year in)

$$\frac{[\![p]\!]_{\mathrm{OGS}} \approx [\![q]\!]_{\mathrm{OGS}}}{\forall E, \gamma,\ \mathrm{eval}(E[p[\gamma]]) \equiv_{\mathrm{res}} \mathrm{eval}(E[q[\gamma]])}\ \text{soundness}$$

Formalization challenges

Syntax and operational semantics are tedious.

$\Rightarrow$ Just enough precision (not more).

OGS requires subtle coinductive reasoning.

$\Rightarrow$ Answer in this talk.

Key choices

Traces in intrinsically typed and scoped De-Bruijn.

Axiomatize what makes OGS sound.

Copattern- and coalgebra-based presentation.

Outline

1. Our flavor of Operational game semantics.
2. Composition and the mystery hypothesis.
3. Concluding with eventual guardedness.

Our flavor of Operational Game Semantics

Observations*

What can you ask to a...

function?	$\cdot\mathtt{app}(v, \kappa)$
pair?	$\cdot\mathtt{fst}(\kappa)$, $\cdot\mathtt{snd}(\kappa)$
stream?	$\cdot\mathtt{head}(\kappa)$, $\cdot\mathtt{tail}(\kappa)$
continuation?	$\cdot\mathtt{ret}(v)$

* also called “copattern”

In practice

Partiality: the delay monad

$$\mathcal{D}(X) \coloneqq \nu A.\, A + X$$

Operational semantics: sequent calculus-style

$$\mathsf{Val} \colon \mathsf{Ctx} \to \mathsf{Typ} \to \mathsf{Set} \qquad \mathsf{Conf} \colon \mathsf{Ctx} \to \mathsf{Set} \qquad \mathsf{Obs} \colon \mathsf{Typ} \to \mathsf{Set}$$

$$\mathsf{eval} \colon \forall \Gamma, \mathsf{Conf}\, \Gamma \to \mathcal{D}(\mathsf{Nf}\, \Gamma) \qquad \mathsf{holes} \colon \mathsf{Obs}\, \tau \to \mathsf{Ctx}$$

$$\mathsf{Nf}\, \Gamma \coloneqq (x \colon \tau \in \Gamma) \times (o \colon \mathsf{Obs}\, \tau) \times (\gamma \colon \mathsf{holes}(o) \to_{\mathsf{Val}} \Gamma)$$

$$c \approx_{\mathsf{ctx}} d \coloneqq \forall \gamma, \mathsf{eval}\ (c[\gamma]) \equiv_{\mathsf{Obs}} \mathsf{eval}\ (d[\gamma])$$

Strategies: Set families S^{+}, S^{-}, equipped with:

$$\mathrm{play} \colon S^{+}\ (\Gamma, \Delta) \to \mathcal{D}\left((o \colon \mathsf{Obs}^{\bullet}\ \Gamma) \times S^{-}\ (\Gamma, \Delta + \mathsf{holes}(o))\right)$$
$$\mathrm{coplay} \colon S^{-}\ (\Gamma, \Delta) \to (o \colon \mathsf{Obs}^{\bullet}\ \Delta) \to S^{+}\ (\Gamma + \mathsf{holes}(o), \Delta)$$

Strategies: Set families S^+, S^-, equipped with:

$$\mathsf{play}\colon S^+\;(\Gamma,\Delta) \to \mathcal{D}\left((o\colon \mathsf{Obs}^\bullet\;\Gamma) \times S^-\;(\Gamma,\Delta + \mathsf{holes}(o))\right)$$
$$\mathsf{coplay}\colon S^-\;(\Gamma,\Delta) \to (o\colon \mathsf{Obs}^\bullet\;\Delta) \to S^+\;(\Gamma + \mathsf{holes}(o),\Delta)$$

The "operational strategy"

$$S^+(\Gamma,\Delta) \coloneqq (c\colon \mathsf{Conf}\;\Gamma) \times (\gamma\colon \Delta \to_{\mathsf{Val}} \Gamma)$$
$$S^-(\Gamma,\Delta) \coloneqq \Delta \to_{\mathsf{Val}} \Gamma$$
$$\mathsf{play} \coloneqq \text{“eval then hide arguments”}$$
$$\mathsf{coplay} \coloneqq \text{“apply observation”}$$

Levy & Staton: Transition systems over games

Xia *et al.*: Interaction trees

Composition and the *mystery* hypothesis

Why composition?

OGS soundness in a nutshell

1. Composition respects bisimilarity: congruence.
2. Composition simulates substitution: adequacy.

Given $[\![c]\!] \approx [\![d]\!]$, for any γ,

$$
\begin{aligned}
\mathrm{eval}(c[\gamma]) &\approx [\![c]\!] \parallel [\![\gamma]\!] && \text{(by 2)} \\
&\approx [\![d]\!] \parallel [\![\gamma]\!] && \text{(by 1)} \\
&\approx \mathrm{eval}(d[\gamma]) && \text{(by 2)}
\end{aligned}
$$

Characterizing composition

$$-\|- : \forall \Phi,\ S^{+}\ \Phi \to S^{-}\ \Phi \to \mathcal{D}(\mathsf{Res})$$

$$(c, \gamma) \parallel \delta \;\coloneqq\; \mathsf{let}\ x{\cdot}o(\varphi) \leftarrow \mathsf{eval}(c)\,;\ \mathsf{case}\ x \begin{cases} \mathsf{final} & \mapsto \mathsf{ret}(x{\cdot}o) \\ \mathsf{shared} & \mapsto (\delta(x){\cdot}o(\mathsf{fresh}), \delta) \parallel (\gamma + \varphi) \end{cases}$$

Characterizing composition

$$-\|- : \forall \Phi,\ S^{+}\ \Phi \to S^{-}\ \Phi \to \mathcal{D}(\mathrm{Res})$$

$$(c, \gamma) \parallel \delta \ \coloneqq\ \mathrm{let}\ x{\cdot}o(\varphi) \leftarrow \mathrm{eval}(c)\,;\ \mathrm{case}\ x \begin{cases} \mathrm{final} & \mapsto \mathrm{ret}(x{\cdot}o) \\ \mathrm{shared} & \mapsto (\delta(x){\cdot}o(\mathrm{fresh}), \delta) \parallel (\gamma + \varphi) \end{cases}$$

This is not a coinductive definition 

Chattering, *or, why everything always falls apart*

A bad looping example

$$(c, \gamma) \parallel \delta \qquad \Gamma, \Delta \coloneqq [\neg\mathsf{Bool}]$$

$$c \coloneqq \langle \mathsf{true} \parallel x \rangle \qquad \gamma \coloneqq y \mapsto x \qquad \delta \coloneqq x \mapsto y$$

🚨 Looping without ever doing a reduction step. 🚨

Chattering, *or, why everything always falls apart*

A bad looping example

$$(c, \gamma) \parallel \delta \qquad \Gamma, \Delta := [\neg \mathrm{Bool}]$$

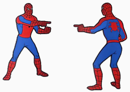
$$c := \langle \mathrm{true} \parallel x \rangle \qquad \gamma := y \mapsto x \qquad \delta := x \mapsto y$$

🚨 Looping without ever doing a reduction step. 🚨

Two live processes sharing a channel

Fine: Stop interacting with the world.

Not Fine: Pointing fingers.



Revisiting OGS positions

An order on variables

Arguments should only mention *older* variables.

Γ and Δ should form an acyclic bipartite graph.

Better types

An interleaving of the two scopes: $\Phi \coloneqq \Gamma_0, \Delta_0, \Gamma_1, \Delta_1, \ldots$

$$\text{my}(\Phi) \coloneqq \Gamma_0, \Gamma_1, \ldots$$

$$\text{your}(\Phi) \coloneqq \Delta_0, \Delta_1, \ldots$$

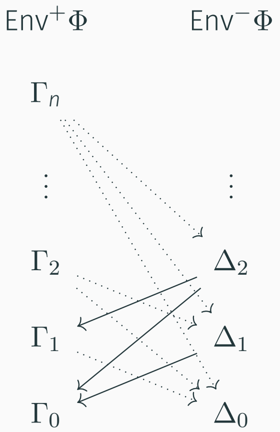
Revisiting assignments

Replace $\Gamma \to_{\mathsf{Val}} \Delta$ with some funny pair of mutual inductives.

Refine OGS states.

$S^{+}\ \Phi := \mathsf{Conf}\ (\mathsf{my}\ \Phi) \times \mathsf{Env}^{+}\ \Phi$

$S^{-}\ \Phi := \mathsf{Env}^{-}\ \Phi$



Finite chattering

Eventually, either

1. Interaction ends.
2. Some (head) variable is replaced by a non-variable value.

Finite chattering

Eventually, either

1. Interaction ends.
2. Some (head) variable is replaced by a non-variable value.

Not enough!

$$\langle\, x \,\|\, y \,\rangle \xrightarrow{chatter} \langle\, x \,\|\, \cdot\mathrm{app}(true, z) \,\rangle \xrightarrow{chatter} \langle\, \lambda a.t \,\|\, \cdot\mathrm{app}(true, z) \,\rangle$$

Two chatters for a redex.

Repeatedly instanciating the head variable of a normal-form by a non-variable value eventually leads to a redex.

$$- \triangleright - : \mathrm{Obs} \to \mathrm{Obs} \to \mathrm{Prop} \qquad \frac{\mathrm{eval}\ (v \cdot o_1(\gamma)) \approxeq \mathrm{ret}\ (x \cdot o_2(\delta))}{o_1 \triangleright o_2}$$

"Finite redexes"

$- \triangleright -$ is well-founded.

Concluding with eventual guardedness

Eventual guardedness

Recursive equations

$$e \colon \overbrace{X \to \mathcal{D}(X}^{\text{variables}} + Y)$$

$$e \colon X \to \mathcal{D}(\underbrace{X}_{\text{recursive calls}} + \underbrace{Y}_{\text{constants}})$$

Guardedness criteria

$e\ x$ is guarded if $e\ x \neq \mathrm{ret}(\mathrm{inl}(x))$.

$e\ x$ is eventually guarded if there exists an n such that $e^n\ x$ is guarded.

Pointwise (eventually) guarded equations admit unique fixpoints (w.r.t. strong bisimilarity).

Conclusion

Contributions

- Formalized generic soundness theorem for OGS.
- OGS for several $\mu\tilde{\mu}$ and λ-calculi.
- New? interesting family of guard conditions.

Future work ideas

- Coq: more flexible language interface.
- Expand: effectful languages.
- Adjacent: completeness, normal form bisimulations.