Realizability, Testing and Game Semantics

GaLoP 2014 (Grenoble)

Rodolphe Lepigre - LAMA, UMR 5127

Introduction

Operational framework for game semantics (P. Clairambault)

A play is an interactive program in a Krivine's Abstract Machine

Implements a winning strategy for typed terms

Aim: give a direct proof that the execution of such terms is well-behaved

Syntax

$$t\,,\,u\,,\,v \quad ::= \quad x \quad | \quad \lambda x.t \quad | \quad u\,v \quad | \quad \mathtt{cc}$$

Four kinds of terms:

- Variable
- λ-abstraction
- Function application
- Call/cc

Simple types

$$A, B, C \quad ::= \quad X \quad | \quad A \to B$$

Types are built using:

- Base types (Atomic types)
- Functions

Context:

- Finite set of type declarations
- $\Gamma = x_1 : A_1, \ldots, x_n : A_n$

Typing judgement:

$$\Gamma \quad \vdash \quad t \quad : \quad A$$

Typing rules

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \to B}\to_i \qquad \frac{\Gamma \vdash u : A \to B \quad \Gamma \vdash v : A}{\Gamma \vdash u\,v : B}\to_e$$

$$\frac{}{\Gamma, x : A \vdash x : A}\text{Ax} \qquad \frac{}{\Gamma \vdash \mathfrak{cc} : ((A \to B) \to A) \to A}\mathfrak{cc}$$

Working with closures

A closure is a couple $\langle t\,, \sigma\rangle$ where:

- t is a term
- σ is an environment

σ maps free variables of t to closures

Notation (extend): $\sigma + \{x \mapsto c\}$

$$\frac{}{\vdash \emptyset : \emptyset}\,\sigma_{\emptyset}$$

$$\frac{\vdash \sigma : \Gamma \quad \vdash c : A}{\vdash \sigma + \{x \mapsto c\} : \Gamma, x : A}\,\sigma_{+}$$

$$\frac{\vdash \sigma : \Gamma \quad \Gamma \vdash t : A}{\vdash \langle t\,, \sigma\rangle : A}\,{<>}_{i}$$

Classical Realizability

Typing:

- A way to identify correct programs
- Based on the syntax
- Many working programs are rejected

```
let succ = fun n -> if true then n + 1 else false
```

Realizability:

- Another way of identifying correct programs
- Based on the notion of evaluation
- Compatible with typing

Stacks and processes

$$\pi, \rho \quad ::= \quad \varepsilon \quad | \quad c.\pi$$

$$\dfrac{}{\vdash \varepsilon : X^{\perp}}\,\varepsilon$$

Stacks are built:

- Using the empty stack ε
- By pushing a closure c on a stack π

$$\dfrac{\vdash c : A \qquad \vdash \pi : B^{\perp}}{\vdash c.\pi : (A \to B)^{\perp}}\,\pi$$

A process is a couple $c \star \pi$ where:

- c is a closure
- π is a stack

$$\dfrac{\vdash c : A \qquad \vdash \pi : A^{\perp}}{\vdash c \star \pi : \perp}\,\star$$

Stacks as "first class" objects

Stacks can be seen as execution contexts

Classical computation amounts to manipulating stacks (call/cc)

A stack π is a closed object:

- It can be seen as a constant that we denote k_π
- k_π is a new form of closure

One more typing rule:

$$\frac{\vdash \pi : A^\perp}{\vdash k_\pi : A \to B}\, k_\pi$$

Summary of the syntax

$$t\,,u\,,v \quad ::= \quad x \quad | \quad \lambda x.t \quad | \quad u\,v \quad | \quad cc$$

$$c \quad ::= \quad \langle t\,,\sigma\rangle \quad | \quad k_\pi$$

$$\pi\,,\rho \quad ::= \quad \varepsilon \quad | \quad c.\pi$$

$$p\,,q \quad ::= \quad c \star \pi$$

Reduction relation

$$\langle x, \sigma \rangle \star \pi \quad \succ \quad \sigma(x) \star \pi$$

$$\langle \lambda x.t, \sigma \rangle \star c \cdot \pi \quad \succ \quad \langle t, \sigma + \{x \mapsto c\} \rangle \star \pi$$

$$\langle t\, u, \sigma \rangle \star \pi \quad \succ \quad \langle t, \sigma \rangle \star \langle u, \sigma \rangle \cdot \pi$$

$$\langle \mathfrak{cc}, \sigma \rangle \star c \cdot \pi \quad \succ \quad c \star k_\pi \cdot \pi$$

$$k_\pi \star c \cdot \pi' \quad \succ \quad c \star \pi$$

Pole, falsity values and truth values

Parameters:

- A set of processes $⫫$ (closed under anti-reduction)
- An interpretation I for base types

Falsity values (set of stacks):

$$\|X\|_{⫫} = I_X \qquad \|A \to B\|_{⫫} = \left\{c.\pi \mid c \in |A|_{⫫}, \pi \in \|B\|_{⫫}\right\}$$

Truth values (set of closures):

$$|A|_{⫫} = \left\{c \in \Lambda \mid \forall \pi \in \|A\|_{⫫}\ c \star \pi \in ⫫\right\}$$

The realizability relation ($\Vdash_{⫫}$) is defined as:

$$c \Vdash_{⫫} A \qquad \Leftrightarrow \qquad c \in |A|_{⫫}$$

Soundness (adequacy)

Theorem 1.

Let $⫫$ be a pole. If we have:

- $\Gamma \vdash t : A$
- $\sigma \Vdash_{⫫} \Gamma$

then $\langle t, \sigma \rangle \Vdash_{⫫} A$.

Corollary 1.

Let $⫫$ be pole. If $\vdash p : \bot$, then $p \in ⫫$.

New terms: channels

A channel is a term $[\Delta \Rightarrow X]$ where

- Δ is a context
- X is an atomic type

$$\frac{\Delta \subseteq \Gamma}{\Gamma \vdash [\Delta \Rightarrow X] : X}\,\text{Ch}$$

Realizabiliy with channels

Channel substitution Σ:

- Replace every channel $\alpha = [\Delta \Rightarrow X]$ by a term t_α
- With $\langle t_\alpha , \sigma \rangle \Vdash_{\perp\!\!\!\perp} X$ for every $\sigma \Vdash_{\perp\!\!\!\perp} \Delta$

Theorem 2.

Let $\perp\!\!\!\perp$ be a pole, and Σ be a channel substitution. If we have:

- $\Gamma \vdash t : A$
- $\sigma \Vdash_{\perp\!\!\!\perp} \Gamma$

then $\langle t\Sigma , \sigma \rangle \Vdash_{\perp\!\!\!\perp} A$.

Corollary 2.

Let $\perp\!\!\!\perp$ be a pole, and Σ be a channel substitution. If $\vdash p : \bot$, then $p\Sigma \in \perp\!\!\!\perp$.

The "good", the "bad" and the "channel"

Final states are processes that cannot be reduced further using $(\rightarrowtriangle)$

They can be of three kinds:

- "Channel" states: processes of the form $\langle [\Delta \Rightarrow X], \sigma \rangle \star \pi$
- "Bad" final states: processes of the form
  - $\langle \lambda x.t, \sigma \rangle \star \varepsilon$
  - $k_\pi \star \varepsilon$
- "Good" final states: final states that are neither of the above

We denote the corresponding sets $\mathscr{C}$, $\mathscr{B}$ and $\mathscr{G}$

Normalization

Theorem 3.

If p is a process such that $\vdash p : \bot$ then

- either $p \twoheadrightarrow^* q \in \mathscr{G}$
- or $p \twoheadrightarrow^* q \in \mathscr{C}$.

Proof. (by realizability) □

Normalization

Theorem 3.

If p is a process such that $\vdash p : \bot$ then

- either $p \rightarrow^* q \in \mathscr{G}$
- or $p \rightarrow^* q \in \mathscr{C}$.

Proof. (by realizability)

- We consider the pole $\perp\!\!\!\perp_{\mathscr{N}} = \{p \mid p \rightarrow^* q \in \mathscr{G} \cup \mathscr{C}\}$

□

Normalization

Theorem 3.

If p is a process such that $\vdash p : \bot$ then

- either $p \rightarrow^* q \in \mathscr{G}$
- or $p \rightarrow^* q \in \mathscr{C}$.

Proof. (by realizability)

- We consider the pole $\perp\!\!\!\perp_{\mathscr{N}} = \{p \mid p \rightarrow^* q \in \mathscr{G} \cup \mathscr{C}\}$
- Since $\mathscr{C} \subseteq \perp\!\!\!\perp_{\mathscr{N}}$ we have $\langle [\Delta \Rightarrow X], \sigma \rangle \Vdash_{\perp\!\!\!\perp_{\mathscr{N}}} X$

□

Normalization

Theorem 3.

If p is a process such that $\vdash p : \bot$ then

- either $p \rightarrow^* q \in \mathscr{G}$
- or $p \rightarrow^* q \in \mathscr{C}$.

Proof. (by realizability)

- We consider the pole $\perp\!\!\!\perp_{\mathscr{N}} = \{p \mid p \rightarrow^* q \in \mathscr{G} \cup \mathscr{C}\}$
- Since $\mathscr{C} \subseteq \perp\!\!\!\perp_{\mathscr{N}}$ we have $\langle [\Delta \Rightarrow X], \sigma \rangle \Vdash_{\perp\!\!\!\perp_{\mathscr{N}}} X$
- Σ_{id} is a channel substitution for $\perp\!\!\!\perp_{\mathscr{N}}$

□

Normalization

Theorem 3.

If p is a process such that $\vdash p : \bot$ then

- either $p \rightarrow^* q \in \mathscr{G}$
- or $p \rightarrow^* q \in \mathscr{C}$.

Proof. (by realizability)

- We consider the pole $\perp\!\!\!\perp_{\mathscr{N}} = \{p \mid p \rightarrow^* q \in \mathscr{G} \cup \mathscr{C}\}$
- Since $\mathscr{C} \subseteq \perp\!\!\!\perp_{\mathscr{N}}$ we have $\langle [\Delta \Rightarrow X], \sigma \rangle \Vdash_{\perp\!\!\!\perp_{\mathscr{N}}} X$
- Σ_{id} is a channel substitution for $\perp\!\!\!\perp_{\mathscr{N}}$
- Since $\vdash p : \bot$ we obtain that $p\Sigma_{\text{id}} = p \in \perp\!\!\!\perp_{\mathscr{N}}$ □

What about reducing channels?

A channel $[\Delta \Rrightarrow X]$ should reduce to terms t such that $\Delta \vdash t : X$

Let $\Delta = s : N \to N, z : N$ be a context

We want $[\Delta \Rrightarrow N]$ to reduce to either of:

- z
- $s\,[\Delta \Rrightarrow N]$

Let $\Gamma = f : (X \to X) \to X$ be a context

We want $[\Gamma \Rrightarrow X]$ to reduce to:

- $f\,\lambda x.[\Gamma, x : X \Rrightarrow X]$
- Which might be reduced further to $f\,\lambda x.x$

The reduction of channels

$$\mathrm{ANF}(\Delta \Rightarrow X) = \left\{ x\, t_1 \ldots t_k \mid \Delta(x) = \left(\overrightarrow{A_1} \to X_1\right) \ldots \left(\overrightarrow{A_k} \to X_k\right) \to X \right\}$$

Where $t_i = \lambda \overrightarrow{x_i}.\left[\Delta, \overrightarrow{x_i} : \overrightarrow{A_i} \Rightarrow X_i\right]$

We define $(\twoheadrightarrow)$ to be the smallest relation such that:

- $(\rightarrowtriangle) \subseteq (\twoheadrightarrow)$
- For all $a \in \mathrm{ANF}(\Delta \Rightarrow X)$,

$$\langle [\Delta \Rightarrow X], \sigma\rangle \star \pi \qquad \twoheadrightarrow \qquad \langle a, \sigma \rangle \star \pi$$

What was our goal again?

A play consists of a run of a process p in the machine

The Player reduces the term using ($\rightarrowtriangle$)

When a channel is reached, the Opponent takes over

Opponent move: one step of ($\twoheadrightarrow$) reduction

Conjecture 1.

If p is a process such that $\vdash p : \bot$, a run of p using ($\twoheadrightarrow$) cannot:

- Stop on a "bad" final state
- Contain an infinite sequence of ($\rightarrowtriangle$) reductions

Subject reduction

Theorem 4.

If p and q are processes such that:

- $\vdash p : \bot$
- $p \twoheadrightarrow q$

then $\vdash q : \bot$.

Reduction to a “bad” state

Theorem 5.

If $\vdash p : \bot$, then it is not possible that $p \twoheadrightarrow^* q \in \mathscr{B}$.

Proof. (by contradiction) □

Reduction to a “bad” state

Theorem 5.

If $\vdash p : \bot$, then it is not possible that $p \twoheadrightarrow^* q \in \mathscr{B}$.

Proof. (by contradiction)

- We suppose that $p \twoheadrightarrow^* q \in \mathscr{B}$

□

Reduction to a "bad" state

Theorem 5.

If $\vdash p : \bot$, then it is not possible that $p \twoheadrightarrow^* q \in \mathscr{B}$.

Proof. (by contradiction)

- We suppose that $p \twoheadrightarrow^* q \in \mathscr{B}$
- $\vdash p : \bot \Rightarrow \vdash q : \bot$ (subject reduction)

□

Reduction to a "bad" state

Theorem 5.

If $\vdash p : \bot$, then it is not possible that $p \twoheadrightarrow^* q \in \mathscr{B}$.

Proof. (by contradiction)

- We suppose that $p \twoheadrightarrow^* q \in \mathscr{B}$
- $\vdash p : \bot \Rightarrow \vdash q : \bot$ (subject reduction)
- $q \rightarrowtriangle^* q' \in \mathscr{G} \cup \mathscr{C}$ (normalization theorem)

□

Reduction to a "bad" state

Theorem 5.

If $\vdash p : \bot$, then it is not possible that $p \twoheadrightarrow^* q \in \mathscr{B}$.

Proof. (by contradiction)

- We suppose that $p \twoheadrightarrow^* q \in \mathscr{B}$
- $\vdash p : \bot \Rightarrow \vdash q : \bot$ (subject reduction)
- $q \rightarrowtriangle^* q' \in \mathscr{G} \cup \mathscr{C}$ (normalization theorem)
- $q' = q$ (q is a final state)

□

Reduction to a “bad” state

Theorem 5.

If $\vdash p : \bot$, then it is not possible that $p \twoheadrightarrow^* q \in \mathscr{B}$.

Proof. (by contradiction)

- We suppose that $p \twoheadrightarrow^* q \in \mathscr{B}$
- $\vdash p : \bot \Rightarrow \vdash q : \bot$ (subject reduction)
- $q \rightarrow^* q' \in \mathscr{G} \cup \mathscr{C}$ (normalization theorem)
- $q' = q$ (q is a final state)
- Contradiction: $\mathscr{B} \cap (\mathscr{G} \cup \mathscr{C}) = \emptyset$ □

Infinite reduction, infinite interaction

Theorem 6.

We consider $\vdash p : \bot$ and suppose that there exists an infinite run R of the machine starting from p using ($\twoheadrightarrow$). The run R should go through infinitely many "channel" states).

Proof. (by contradiction) $\square$

Infinite reduction, infinite interaction

Theorem 6.
We consider $\vdash p : \bot$ and suppose that there exists an infinite run R of the machine starting from p using $(\twoheadrightarrow)$. The run R should go through infinitely many "channel" states).

Proof. (by contradiction)

- We suppose that R goes through exactly n "channel" states

□

Infinite reduction, infinite interaction

Theorem 6.

We consider $\vdash p : \bot$ and suppose that there exists an infinite run R of the machine starting from p using ($\twoheadrightarrow$). The run R should go through infinitely many "channel" states).

Proof. (by contradiction)

- We suppose that R goes through exactly n "channel" states
- We consider p', the n-th "channel" state in the reduction of p

□

Infinite reduction, infinite interaction

Theorem 6.

We consider $\vdash p : \bot$ and suppose that there exists an infinite run R of the machine starting from p using ($\twoheadrightarrow$). The run R should go through infinitely many "channel" states).

Proof. (by contradiction)

- We suppose that R goes through exactly n "channel" states
- We consider p', the n-th "channel" state in the reduction of p
- There is q' such that $p' \twoheadrightarrow q'$ (otherwise R was not infinite)

□

Infinite reduction, infinite interaction

Theorem 6.

We consider $\vdash p : \bot$ and suppose that there exists an infinite run R of the machine starting from p using $(\twoheadrightarrow)$. The run R should go through infinitely many "channel" states).

Proof. (by contradiction)

- We suppose that R goes through exactly n "channel" states
- We consider p', the n-th "channel" state in the reduction of p
- There is q' such that $p' \twoheadrightarrow q'$ (otherwise R was not infinite)
- Since $p \twoheadrightarrow^* q'$, $\vdash q' : \bot$ (subject reduction)

□

Infinite reduction, infinite interaction

Theorem 6.

We consider $\vdash p : \bot$ and suppose that there exists an infinite run R of the machine starting from p using ($\twoheadrightarrow$). The run R should go through infinitely many "channel" states).

Proof. (by contradiction)

- We suppose that R goes through exactly n "channel" states
- We consider p', the n-th "channel" state in the reduction of p
- There is q' such that $p' \twoheadrightarrow q'$ (otherwise R was not infinite)
- Since $p \twoheadrightarrow^* q'$, $\vdash q' : \bot$ (subject reduction)
- $q' \rightarrowtriangle^* q \in \mathscr{G} \cup \mathscr{C}$ (normalization theorem)

□

Infinite reduction, infinite interaction

Theorem 6.
We consider $\vdash p : \bot$ and suppose that there exists an infinite run R of the machine starting from p using ($\twoheadrightarrow$). The run R should go through infinitely many "channel" states).

Proof. (by contradiction)

- We suppose that R goes through exactly n "channel" states
- We consider p′, the n-th "channel" state in the reduction of p
- There is q' such that $p' \twoheadrightarrow q'$ (otherwise R was not infinite)
- Since $p \twoheadrightarrow^* q'$, $\vdash q' : \bot$ (subject reduction)
- $q' \rightarrowtriangle^* q \in \mathscr{G} \cup \mathscr{C}$ (normalization theorem)
  - If $q \in \mathscr{G}$ then R was not infinite

□

Infinite reduction, infinite interaction

Theorem 6.
We consider $\vdash p : \bot$ and suppose that there exists an infinite run R of the machine starting from p using ($\twoheadrightarrow$). The run R should go through infinitely many "channel" states).

Proof. (by contradiction)

- We suppose that R goes through exactly n "channel" states
- We consider p', the n-th "channel" state in the reduction of p
- There is q' such that $p' \twoheadrightarrow q'$ (otherwise R was not infinite)
- Since $p \twoheadrightarrow^* q'$, $\vdash q' : \bot$ (subject reduction)
- $q' \rightarrowtail^* q \in \mathscr{G} \cup \mathscr{C}$ (normalization theorem)
  - If $q \in \mathscr{G}$ then R was not infinite
  - If $q \in \mathscr{C}$ then R would contain more than n "channels" □

Without subject reduction?

We need a pole:

- Closed under $(\rightarrowtriangle)^{-1}$
- Containing $\mathscr{G}$
- Not containing any element of $\mathscr{B}$
- Closed under $(\twoheadrightarrow)$
- In which channels realize their type

Thank you!