Realizability, Testing and Game Semantics

GaLoP 2014 (Grenoble)

Rodolphe Lepigre - LAMA, UMR 5127
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

\[ t, u, v ::= x \mid \lambda x . t \mid u \, v \mid \text{cc} \]

Four kinds of terms:
- Variable
- \( \lambda \)-abstraction
- Function application
- Call/cc
Simple types

\[ A, B, C ::= \lambda \mid A \to B \]

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:
\[ \Gamma \vdash t : A \]
Typing rules

\[ \Gamma, x : A \vdash t : B \quad \Rightarrow_i \quad \Gamma \vdash \lambda x.t : A \rightarrow B \]

\[ \Gamma \vdash u : A \rightarrow B \quad \Gamma \vdash v : A \quad \Rightarrow_e \quad \Gamma \vdash u \cdot v : B \]

\[ \Gamma, x : A \vdash x : A \quad \Rightarrow_{Ax} \]

\[ \Gamma \vdash cc : ((A \rightarrow B) \rightarrow A) \rightarrow A \quad \Rightarrow_{cc} \]
A closure is a couple $\langle t, \sigma \rangle$ where:

- $t$ is a term
- $\sigma$ is an environment

$\sigma$ maps free variables of $t$ to closures

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

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

\[
\text{let } \text{succ} = \text{fun } n \rightarrow \text{if } \text{true } \text{then } n + 1 \text{ else } \text{false}
\]

Realizability:
- Another way of identifying correct programs
- Based on the notion of evaluation
- Compatible with typing
Stacks and processes

\[ \pi, \rho ::= \varepsilon \mid c.\pi \]

Stacks are built:
- Using the empty stack \( \varepsilon \)
- By pushing a closure \( c \) on a stack \( \pi \)

A process is a couple \( c \star \pi \) where:
- \( c \) is a closure
- \( \pi \) is a stack

\[ \vdash \varepsilon : \mathcal{X} \]

\[ \vdash c : A \quad \vdash \pi : B \]

\[ \vdash c.\pi : (A \rightarrow B) \]

\[ \vdash c : A \quad \vdash \pi : \mathcal{A} \]

\[ \vdash c \star \pi : \perp \]
Stacks as “first class” objects

Stacks can be seen as execution contexts

Classical computation amounts to manipulating stacks (call/cc)

A stack \( \pi \) is a closed object:
- It can be seen as a constant that we denote \( k_\pi \)
- \( k_\pi \) is a new form of closure

One more typing rule:

\[
\begin{align*}
\vdash \pi : A^\bot \\
\vdash k_\pi : A \rightarrow B
\end{align*}
\]
Summary of the syntax

\[ \begin{align*}
  t, u, v & ::= \; x \; | \; \lambda x.t \; | \; u \; v \; | \; \mathsf{cc} \\
  c & ::= \; \langle t, \sigma \rangle \; | \; \mathsf{k}_\pi \\
  \pi, \rho & ::= \; \varepsilon \; | \; c.\pi \\
  p, q & ::= \; c \star \pi
\end{align*} \]
Reduction relation

\[ \langle x, \sigma \rangle \star \pi \quad \rightarrow \quad \sigma(x) \star \pi \]

\[ \langle \lambda x. t, \sigma \rangle \star c. \pi \quad \rightarrow \quad \langle t, \sigma + \{ x \mapsto c \} \rangle \star \pi \]

\[ \langle t \ u, \sigma \rangle \star \pi \quad \rightarrow \quad \langle t, \sigma \rangle \star \langle u, \sigma \rangle. \pi \]

\[ \langle c c, \sigma \rangle \star c. \pi \quad \rightarrow \quad c \star k_{\pi}. \pi \]

\[ k_{\pi} \star c. \pi' \quad \rightarrow \quad c \star \pi \]
Pole, falsity values and truth values

Parameters:
- A set of processes $\bot$ (closed under anti-reduction)
- An interpretation $I$ for base types

Falsity values (set of stacks):
$$
||X||_\bot = I_X \quad ||A \rightarrow B||_\bot = \{c.\pi \mid c \in |A|_\bot, \pi \in ||B||_\bot\}
$$

Truth values (set of closures):
$$
|A|_\bot = \{c \in A \mid \forall \pi \in ||A||_\bot \ c \star \pi \in \bot\}
$$

The realizability relation ($\models_\bot$) is defined as:
$$
c \models_\bot A \iff c \in |A|_\bot$$
Soundness (adequacy)

**Theorem 1.**

Let $\perp$ be a pole. If we have:

- $\Gamma \vdash t : \Lambda$
- $\sigma \models_{\perp} \Gamma$

then $\langle t, \sigma \rangle \models_{\perp} \Lambda$.

**Corollary 1.**

Let $\perp$ be pole. If $\vdash p : \perp$, then $p \in \perp$. 
New terms: channels

A channel is a term \([\Delta \Rightarrow X]\) where
- \(\Delta\) is a context
- \(X\) is an atomic type

\[
\frac{\Delta \subseteq \Gamma}{\Gamma \vdash [\Delta \Rightarrow X] : X}_{\text{Ch}}
\]
Realizability with channels

Channel substitution $\Sigma$:
- Replace every channel $\alpha = [\Delta \Rightarrow X]$ by a term $t_\alpha$
- With $\langle t_\alpha, \sigma \rangle \vdash X$ for every $\sigma \vdash \Delta$

**Theorem 2.**
Let $\perp$ be a pole, and $\Sigma$ be a channel substitution. If we have:
- $\Gamma \vdash t : \Lambda$
- $\sigma \vdash \Gamma$
then $\langle t\Sigma, \sigma \rangle \vdash \Lambda$.

**Corollary 2.**
Let $\perp$ be a pole, and $\Sigma$ be a channel substitution. If $\vdash p : \perp$, then $p\Sigma \in \perp$. 
The “good”, the “bad” and the “channel”

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

They can be of three kinds:
- “Channel” states: processes of the form \(\langle \Delta \Rightarrow X \rangle, \sigma \star \pi\)
- “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 \(\mathcal{C}, \mathcal{B}, \text{ and } \mathcal{C}\)
Normalization

Theorem 3.
If \( p \) is a process such that \( \vdash p : \bot \) then
- either \( p \rightarrow^* q \in \mathcal{G} \)
- or \( p \rightarrow^* q \in \mathcal{E} \).

Proof. (by realizability)
Theorem 3.

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

- either \( p \rightarrow^* q \in \mathcal{G} \)
- or \( p \rightarrow^* q \in \mathcal{C} \).

Proof. (by realizability)

- We consider the pole \( \bot_{\mathcal{N}} = \{ p \mid p \rightarrow^* q \in \mathcal{G} \cup \mathcal{C} \} \)
Normalization

Theorem 3.
If $p$ is a process such that $\vdash p : \bot$ then
- either $p \rightarrow^* q \in \mathcal{G}$
- or $p \rightarrow^* q \in \mathcal{C}$.

Proof. (by realizability)
- We consider the pole $\bot_{\mathcal{N}} = \{ p \mid p \rightarrow^* q \in \mathcal{G} \cup \mathcal{C} \}$
- Since $\mathcal{C} \subseteq \bot_{\mathcal{N}}$ we have $\langle [\Delta \Rightarrow X], \sigma \rangle \Downarrow_{\bot_{\mathcal{N}}} X$
Normalization

**Theorem 3.**

If $p$ is a process such that $\vdash p : \bot$ then
- either $p \rightarrow^* q \in \mathcal{G}$
- or $p \rightarrow^* q \in \mathcal{C}$.

**Proof.** (by realizability)
- We consider the pole $\bot_N = \{ p \mid p \rightarrow^* q \in \mathcal{G} \cup \mathcal{C} \}$
- Since $\mathcal{C} \subseteq \bot_N$ we have $\langle [\Delta \Rightarrow X], \sigma \rangle \models_{\bot_N} X$
- $\Sigma_{id}$ is a channel substitution for $\bot_N$

□
## Normalization

**Theorem 3.**
If \( p \) is a process such that \( \vdash p : \bot \) then
- either \( p \rightarrow^* q \in \mathcal{G} \)
- or \( p \rightarrow^* q \in \mathcal{C} \).

**Proof.** (by realizability)
- We consider the pole \( \bot_\mathcal{N} = \{ p \mid p \rightarrow^* q \in \mathcal{G} \cup \mathcal{C} \} \)
- Since \( \mathcal{C} \subseteq \bot_\mathcal{N} \) we have \( \langle [\Delta \Rightarrow X], \sigma \rangle \models_{\bot_\mathcal{N}} X \)
- \( \Sigma_{id} \) is a channel substitution for \( \bot_\mathcal{N} \)
- Since \( \vdash p : \bot \) we obtain that \( p\Sigma_{id} = p \in \bot_\mathcal{N} \) \( \square \)
What about reducing channels?

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

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

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

- $z$
- $s[\Delta \Rightarrow N]$

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

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

- $f \lambda x.[\Gamma, x : X \Rightarrow X]$
- Which might be reduced further to $f \lambda x.x$
The reduction of channels

\[
\text{ANF}(\Delta \Rightarrow X) = \{ x t_1 \ldots t_k \mid \Delta(x) = (\overrightarrow{A_1 \rightarrow X_1}) \ldots (\overrightarrow{A_k \rightarrow X_k}) \rightarrow X \}
\]

Where \( t_i = \lambda x_i. [\Delta, x_i : \overrightarrow{A_i \Rightarrow X_i}] \)

We define \((\rightarrow)\) to be the smallest relation such that:
- \((\rightarrow) \subseteq (\rightarrow)\)
- For all \( a \in \text{ANF}(\Delta \Rightarrow X)\),

\[
\langle [\Delta \Rightarrow X], \sigma \rangle \star \pi \rightarrow \langle a, \sigma \rangle \star \pi
\]
What was our goal again?

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

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

When a channel is reached, the Opponent takes over

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

**Conjecture 1.**

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

- Stop on a “bad” final state
- Contain an infinite sequence of ($\rightarrow$) reductions
Subject reduction

Theorem 4.
If $p$ and $q$ are processes such that:

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

then $\vdash q : \bot$. 
Reduction to a “bad” state

Theorem 5.
If $\vdash p : \bot$, then it is not possible that $p \rightarrow^* q \in \mathcal{B}$.

Proof. (by contradiction)
Reduction to a “bad” state

Theorem 5. If $\vdash p : \bot$, then it is not possible that $p \rightarrow^* q \in \mathcal{B}$.

Proof. (by contradiction)
- We suppose that $p \rightarrow^* q \in \mathcal{B}$
Reduction to a “bad” state

**Theorem 5.**

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

**Proof.** (by contradiction)

- We suppose that $p \rightarrow^* q \in \mathcal{B}$
- $\vdash p : \bot \Rightarrow \vdash q : \bot$ (subject reduction)
Reduction to a “bad” state

**Theorem 5.**

If \( \vdash p : \bot \), then it is not possible that \( p \rightarrow^* q \in B \).

**Proof.** (by contradiction)

- We suppose that \( p \rightarrow^* q \in B \)
- \( \vdash p : \bot \Rightarrow \vdash q : \bot \) (subject reduction)
- \( q \rightarrow^* q' \in G \cup C \) (normalization theorem)
Reduction to a “bad” state

**Theorem 5.**  
If \( \vdash p : \bot \), then it is not possible that \( p \rightarrow^* q \in \mathcal{B} \).

**Proof.** (by contradiction)  
- We suppose that \( p \rightarrow^* q \in \mathcal{B} \)  
- \( \vdash p : \bot \Rightarrow \vdash q : \bot \) (subject reduction)  
- \( q \rightarrow^* q' \in \mathcal{G} \cup \mathcal{C} \) (normalization theorem)  
- \( q' = q \) (q is a final state)

\[ \square \]
Reduction to a “bad” state

**Theorem 5.**

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

**Proof.** (by contradiction)
- We suppose that $p \rightarrow^* q \in \mathcal{B}$
- $\vdash p : \bot \Rightarrow \vdash q : \bot$ (subject reduction)
- $q \rightarrow^* q' \in \mathcal{G} \cup \mathcal{C}$ (normalization theorem)
- $q' = q$ (q is a final state)
- Contradiction: $\mathcal{B} \cap (\mathcal{G} \cup \mathcal{C}) = \emptyset$
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 ($\Rightarrow$). The run $R$ should go through infinitely many “channel” states.

Proof. (by contradiction)
Infinite reduction, infinite interaction

Theorem 6.
We consider ⊢ p : ⊥ and suppose that there exists an infinite run R of the machine starting from p using (→). 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 \( (\rightarrow) \). 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 $(\rightarrow)$. 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 $p' \rightarrow q'$ (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 $(\rightarrow)$. 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 $p' \rightarrow q'$ (otherwise $R$ was not infinite)
- Since $p \rightarrow^* q'$, $\vdash q' : \bot$ (subject reduction)
Infinite reduction, infinite interaction

Theorem 6.
We consider ⊨ p : ⊥ and suppose that there exists an infinite run R of the machine starting from p using (⇒). 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' ⇒ q' (otherwise R was not infinite)
- Since p ⇒* q', ⊨ q' : ⊥ (subject reduction)
- q' ⇒* q ∈ G ∪ C (normalization theorem)
Infinite reduction, infinite interaction

**Theorem 6.**

We consider ⊢ p : ⊥ and suppose that there exists an infinite run R of the machine starting from p using (⇒). 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' ⇒ q' (otherwise R was not infinite)
- Since p ⇒* q', ⊢ q' : ⊥ (subject reduction)
- q' ⇒* q ∈ G ∪ C (normalization theorem)
  - If q ∈ G then R was not infinite
Infinite reduction, infinite interaction

Theorem 6.
We consider ⊨ p : ⊥ and suppose that there exists an infinite run R of the machine starting from p using (⇒). 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' → q' (otherwise R was not infinite)
- Since p →* q', ⊨ q' : ⊥ (subject reduction)
- q' →* q ∈ \mathcal{G} ∪ \mathcal{C} (normalization theorem)
  - If q ∈ \mathcal{G} then R was not infinite
  - If q ∈ \mathcal{C} then R would contain more than n “channels”
Without subject reduction?

We need a pole:
- Closed under $(\rightarrow)^{-1}$
- Containing $\mathcal{G}$
- Not containing any element of $\mathcal{B}$
- Closed under $(\rightarrow)$
- In which channels realize their type
Thank you!