Classical realizability in the CPS target language

Jonas Frey

Piriapolis, 20 July 2016

article:
https://sites.google.com/site/jonasfreysite/mfps.pdf

Negative and CPS translation

- Glivenko (1929): A classically provable iff $\neg\neg A$ intuitionistically provable (CBV, works for all connectives except $\forall$)
- Plotkin (1975) uses continuation passing style (CPS) translations to simulate different evaluation strategies (CBN, CBV) within another
- Felleisen et al. (1980ies) relate CPS translations and **control operatos** (like call/cc) on abstract machines
- Griffin (1989) recognizes correspondence between CPS and negative translations via CH
- in particular, the natural type of call/cc is **Peirce's law** (PL)

$$((A \Rightarrow B) \Rightarrow A) \Rightarrow A$$

- since PL axiomatizes classical logic, we get an extension of CH to classical logic – the foundation of Krivine's realizability interpretation

Classical 2nd order logic with proof terms

- same language as int. 2nd order logic
- proof system extended by one rule for PL

$$\frac{}{\Gamma, a : A, \Delta \vdash a : A} \qquad \frac{}{\Gamma \vdash \text{œ} : ((A \Rightarrow B) \Rightarrow A) \Rightarrow A}$$

$$\frac{\Gamma, a : A \vdash t : B}{\Gamma \vdash \lambda a \,.\, t : A \Rightarrow B} \qquad \frac{\Gamma \vdash t : A \Rightarrow B \qquad \Gamma \vdash u : A}{\Gamma \vdash tu : B}$$

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash t : \forall x \,.\, A} \qquad \frac{\Gamma \vdash t : \forall x \,.\, A}{\Gamma \vdash t : A[\tau / x]}$$

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash t : \forall X^n \,.\, A} \qquad \frac{\Gamma \vdash t : \forall X^n \,.\, A}{\Gamma \vdash t : A[B[\vec{t}/\vec{x}]/X(\vec{t})]}$$

- realizability model based on operational model for λ-calculus + call/cc : the **Krivine machine** (KAM)

The Krivine Machine

Syntax:

Terms:	t	$::=$	$x \mid \lambda x.t \mid tt \mid \text{æ} \mid \mathsf{k}_\pi \mid \ldots$ *(non-logical instructions)*
Stacks:	π	$::=$	$\varepsilon \mid t{\cdot}\pi$ (t closed)
Processes:	p	$::=$	$t \star \pi$ (t closed)

reduction relation on processes:

$$
\begin{array}{lrcl}
\text{(push)} & tu \star \pi & \succ & t \star u{\cdot}\pi \\
\text{(pop)} & (\lambda x\,.\,t[x]) \star u{\cdot}\pi & \succ & t[u] \star \pi \\
\text{(save)} & \text{æ} \star t{\cdot}\pi & \succ & t \star \mathsf{k}_\pi{\cdot}\pi \\
\text{(restore)} & \mathsf{k}_\pi \star t{\cdot}\rho & \succ & t \star \pi
\end{array}
$$

- non-logical instructions necessary for non-trivial realizability models
- Λ set of closed terms
- Π set of stacks
- $\Lambda{\star}\Pi$ set of processes
- $PL \subseteq \Lambda$ set of **quasiproofs**, i.e. terms w/o non-logical instructions

Classical realizability

- **pole** : set $\perp\!\!\!\perp \subseteq \Lambda{\star}\Pi$ of processes closed under inverse reduction
- truth values are sets $S, T \subseteq \Pi$ of **stacks**
- realizability relation between closed terms and truth values

$$t \Vdash S \quad \text{iff} \quad \forall \pi \in S \,.\, t \star \pi \in \perp\!\!\!\perp$$

- predicates are functions $\varphi, \psi : \mathbb{N}^k \to P(\Pi)$ (more generally $J \to P(\Pi)$)
- interpretation $[\![A]\!]_\rho \in \Sigma$ of formulas defined relative to valuations (assigning individuals to 1st order vars and predicates to relation vars)

$$\begin{aligned}
[\![X(\vec{t})]\!]_\rho &= \rho(X)([\![\vec{t}]\!]_\rho) \\
[\![A \Rightarrow B]\!]_\rho &= \{t{\cdot}\pi \mid t \Vdash [\![A]\!]_\rho,\ \pi \in [\![B]\!]_\rho\} \\
[\![\forall x \,.\, A]\!]_\rho &= \textstyle\bigcup_{k \in \mathbb{N}} [\![A]\!]_{\rho(x \mapsto k)} \\
[\![\forall X^n \,.\, A]\!]_\rho &= \textstyle\bigcup_{\varphi : \mathbb{N}^n \to \Sigma} [\![A]\!]_{\rho(X^n \mapsto \varphi)}
\end{aligned}$$

Theorem (Adequation)

If $\vec{x} : \vec{A} \vdash t : B$ is derivable and $\vec{u} \Vdash [\![\vec{A}]\!]_\rho$ then $t[\vec{u}/\vec{x}] \Vdash [\![B]\!]_\rho$.
In particular, if B is closed and $\vdash t : B$ then $t \Vdash [\![B]\!]$.

Consistency

- two ways of degeneracy
- model arising from $\perp\!\!\!\perp = \varnothing$ equivalent to standard model
- $\perp\!\!\!\perp = \Lambda \star \Pi$ inconsistent (all formulas realized)
- more generally we have

Lemma

$\perp\!\!\!\perp$ gives rise to a consistent model iff every process $t \star \pi \in \perp\!\!\!\perp$ contains a non-logical instruction.

The termination pole

- one non-logical instruction end denoting termination

Terms:	$t ::= x \mid \lambda x.t \mid t\,t \mid \text{œ} \mid \mathsf{k}_\pi \mid \mathsf{end}$	
Stacks:	$\pi ::= \varepsilon \mid t{\cdot}\pi$	t closed
Processes:	$p ::= t \star \pi$	t closed

- notation: $p{\downarrow} \quad \Leftrightarrow \quad \exists \rho\,.\, t \star \pi \succ^* \mathsf{end} \star \rho$ ('p terminates')
- termination pole: $\mathfrak{T} = \{p \in \Lambda{\star}\Pi \mid p{\downarrow}\}$ set of terminating processes
- for $f : \mathbb{N} \to \{0, 1\}$, consider the formula

$$\Phi \quad \equiv \quad \forall x\,.\,\mathrm{Int}(x) \Rightarrow f(x) \neq 0 \Rightarrow f(x) \neq 1 \Rightarrow \bot.$$

- Φ equivalent to $\forall x\,.\,\mathrm{Int}(x) \Rightarrow f(x) = 0 \vee f(x) = 1$, holds in standard model

Theorem

In the model arising from $\mathfrak{T}$, Φ is realized iff it f is computable.

The PTIME pole

- To define a pole of 'PTIME processes', we augment the syntax with a special variable α:

Terms:	$t ::= x \mid \lambda x.t \mid t\,t \mid \text{cc} \mid \mathsf{k}_\pi \mid \mathsf{end} \mid \alpha$	
Stacks:	$\pi ::= \varepsilon \mid t \cdot \pi$	t closed
Processes:	$p ::= t \star \pi$	t closed

- α never bound, 'closed' means 'no free vars except α'
- $PL = \{t \in \Lambda \mid \mathsf{end} \notin t\}$ (α may appear in proof-like terms)
- PTIME pole given by

$$\mathfrak{P} = \{p \mid \exists P \in \mathbb{N}[X]\ \forall \sigma \in \{0,1\}^* .\ p[\overline{\sigma}/\alpha]\downarrow^{\leq P(|\sigma|)}\}$$

Classical realizability in the CPS target language

Motivation

- use explicit negative translation instead of $\mathcal{CC}$
- negative tranlsation doesn't need full int. logic as target language
- disjunction & minimal negation (w/o ex falso) sufficient
- CPS target language is a term calculus for a system based on n-ary negated multi-disjunction like $\neg(A_1 \vee \cdots \vee A_n)$ but with **labels** and written $\langle \ell_1(A_1), \ldots, \ell_n(A_n) \rangle$

$\mathcal{L}$ countable set of labels, $\ell_1, \ldots, \ell_n, \ell \in \mathcal{L}$.

Expressions:

$$\begin{array}{lrcl} \textit{Terms:} & s, t, u & ::= & x \mid \langle \ell_1(x.\, p_1), \ldots, \ell_n(x.\, p_n) \rangle \\ \textit{Programs:} & p, q & ::= & t_\ell u \mid \ldots \textit{(non-logical instructions)} \end{array}$$

Reduction of programs:

$$\langle \ldots, \ell(x.\, p), \ldots \rangle_\ell t \quad \succ \quad p[t/x]$$

2nd order CPS target logic

language consists of

- individual variables $x, y, z, \ldots$
- n-ary relation variables $X^n, Y^n, Z^n, \ldots$ for each $n \geq 0$
- arithmetic constants and operations $0, S, \ldots$
- formulas: $A \ ::= \ X^n(\vec{t}) \mid \exists x \,.\, A \mid \exists X^n \,.\, A \mid \left\langle \ell_1(A_1), \ldots, \ell_n(A_n) \right\rangle \quad n \geq 0$

proof system with proof terms:

$$\text{(Var)} \ \frac{}{\Gamma \vdash x_i : A_i} \qquad \text{(App)} \ \frac{\Gamma \vdash t : \left\langle \ldots, \ell(B), \ldots \right\rangle \qquad \Gamma \vdash u : B}{\Gamma \vdash t_\ell u}$$

$$\text{(Abs)} \ \frac{\Gamma, y : B_1 \vdash p_1 \qquad \cdots \qquad \Gamma, y : B_m \vdash p_m}{\Gamma \vdash \langle \ell_1(y.\, p_1), \ldots, \ell_m(y.\, p_m) \rangle : \left\langle \ell_1(B_1), \ldots, \ell_m(B_m) \right\rangle}$$

$$(\exists\text{-I}) \ \frac{\Gamma \vdash t : A[u/x]}{\Gamma \vdash t : \exists x \,.\, A} \qquad (\exists\text{-E}) \ \frac{\Gamma \vdash t : \exists x \,.\, A \qquad \Gamma, x : A \vdash p[x]}{\Gamma \vdash p[t]}$$

$$(\exists\text{-I}) \ \frac{\Gamma \vdash t : A[B[\vec{u}/\vec{x}]/X(\vec{u})]}{\Gamma \vdash t : \exists X^n \,.\, A} \qquad (\exists\text{-E}) \ \frac{\Gamma \vdash t : \exists X^n \,.\, A \qquad \Gamma, x : A \vdash p[x]}{\Gamma \vdash p[t]}$$

Admissible rules & subject reduction

Admissible rules:

(Cut)
$$\frac{\Gamma \vdash s : A \qquad \Gamma, x : A \vdash p}{\Gamma \vdash p[s/x]} \qquad \frac{\Gamma \vdash s : A \qquad \Gamma, x : A \vdash t : B}{\Gamma \vdash t[s/x] : B}$$

(Sym)
$$\frac{\Gamma \vdash p}{\sigma(\Gamma) \vdash p} \qquad \frac{\Gamma \vdash t : B}{\sigma(\Gamma) \vdash t : B}$$

(Weak)
$$\frac{\Gamma \vdash p}{\Gamma, x : A \vdash p} \qquad \frac{\Gamma \vdash t : B}{\Gamma, x : A \vdash t : B}$$

(Contr)
$$\frac{\Gamma, x : A, y : A \vdash p}{\Gamma, x : A \vdash p[x/y]} \qquad \frac{\Gamma, x : A, y : A \vdash t : B}{\Gamma, x : A \vdash t[x/y] : B}$$

Lemma (Subject reduction)

If $\Gamma \vdash \langle \dots, \ell(x.\, p), \dots \rangle_\ell t$ *is derivable, then so is* $\Gamma \vdash p[t/x]$.

Simplified notation suppressing labels

- Assume $\mathcal{L} = \mathbb{N}$
- Write $\neg(A_0, \ldots, A_{n-1})$ and $\langle x_1 \,.\, p_0, \ldots, x_1 \,.\, p_{n-1}\rangle$ for record types and terms indexed by $\{0, \ldots, n-1\}$
- if indexing set is not an initial segment of $\mathbb{N}$, write $-$ for undefined entries

CBV translation of classical 2nd order logic into 2nd order target language

I give translation for types only, terms left as an exercise.

- $(A \Rightarrow B)^\top = \neg\neg(\neg A^\top, B^\top)$
- $(\forall x \,.\, A)^\top = \neg \exists x \,.\, \neg A^\top$
- $(\forall X^n \,.\, A)^\top = \neg \exists X^n \,.\, \neg A^\top$

Theorem

$A_1, \ldots, A_n \vdash A$ classically provable iff $A_1^\top, \ldots, A_n^\top \vdash \neg\neg B^\top$ provable in target language.

Realizability in the CPS target language

- $\mathbb{T}$ set of closed terms, $\mathbb{T}_0$ set of *pure* closed terms (prooflike terms)
- $\mathbb{P}$ set of closed programs
- pole : $⫫ \subseteq \mathbb{P}$ closed under inverse $\succ$
- truth values : $S, T \subseteq \mathbb{T}$
- interpretation $[\![A]\!]_\rho \subseteq \mathbb{T}$ of formulas defined relative to valuations

$$
\begin{aligned}
[\![X(\vec{t})]\!]_\rho &= \rho(X)([\![\vec{t}]\!]_\rho) \\
[\![\langle \ell_1(A_1), \ldots, \ell_n(A_n) \rangle]\!]_\rho &= \{t \in \mathbb{T} \mid \forall i \in \{1, \ldots, n\}\ \forall s \in [\![A_i]\!]_\rho \,.\, t_{\ell_i} s \in ⫫\} \\
[\![\exists x \,.\, A]\!]_\rho &= \bigcup_{k \in \mathbb{N}} [\![A]\!]_{\rho(x \mapsto k)} \\
[\![\exists X^n \,.\, A]\!]_\rho &= \bigcup_{\varphi : \mathbb{N}^n \to \Sigma} [\![A]\!]_{\rho(X^n \mapsto \varphi)}
\end{aligned}
$$

Adequation/Soundness

- If $\vec{x} : \vec{A} \vdash s : B$ and $\vec{t} \in [\![\vec{A}]\!]_\rho$ then $s[\vec{t}/\vec{x}] \in [\![B]\!]_\rho$
- If $\vec{x} : \vec{A} \vdash p$ and $\vec{t} \in [\![\vec{A}]\!]_\rho$ then $p[\vec{t}/\vec{x}] \in ⫫$

Combined with negative translation

If $\vec{x} : \vec{A} \vdash s : B$ is classically provable and $\vec{t} \in [\![\vec{A}^\top]\!]_\rho$ then $s^\top[\vec{t}/\vec{x}] \in [\![\neg\neg B^\top]\!]_\rho$.

Ordering on predicates

- $\perp\!\!\!\perp$ fixed pole
- generalize predicates to arbitrary carrier sets: a predicate on $J \in \mathbf{Set}$ is a function $\varphi : J \to P(\mathbb{T})$
- predicates on J can be ordered

$$\varphi \leq \psi \quad \text{iff} \quad \exists t[a,b] \in \mathbb{T}_0[a,b] \;\; \forall j \in J \;\; \forall u \in \varphi(j) \;\; \forall v \in \neg\psi(i) \;\; . \;\; t[u,v] \in \perp\!\!\!\perp$$

- intuitively : the judgment $\varphi(j), \neg\psi(j) \vdash$ is realized

Predicates form a Boolean tripos

- The assignment $J \ \mapsto \ (P(\Pi)^J, \leq)$ extends to an **indexed preorder**, i.e. a functor

$$\mathcal{K}_{\perp\!\!\!\perp} : \mathbf{Set}^{\mathrm{op}} \to \mathbf{Ord}$$

Theorem

$\mathcal{K}_{\perp\!\!\!\perp}$ *is a* ***Boolean tripos****, i.e.*

- *fibers* $\mathcal{K}_{\perp\!\!\!\perp}(J)$ *are Boolean prealgebra for all* $J \in \mathbf{Set}$
- *reindexing maps* $\mathcal{K}_{\perp\!\!\!\perp}(f) : \mathcal{K}_{\perp\!\!\!\perp}(I) \to \mathcal{K}_{\perp\!\!\!\perp}(J)$ *preserve Boolean prealgebra structure for all* $f : J \to I$
- *reindexing maps have right adjoints* $\mathcal{K}_{\perp\!\!\!\perp}(f) \dashv \forall_f : \mathcal{K}_{\perp\!\!\!\perp}(J) \to \mathcal{K}_{\perp\!\!\!\perp}(I)$, *and*

  for all pullback squares $\begin{array}{ccc} L & \xrightarrow{q} & K \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle g} \\ J & \xrightarrow{f} & I \end{array}$ *we have* $\mathcal{K}_{\perp\!\!\!\perp}(g) \circ \forall_f \cong \forall_q \circ \mathcal{K}_{\perp\!\!\!\perp}(p)$
- *there exists* $\mathrm{tr} \in \mathcal{P}(\mathrm{Prop})$ *such that for every* $I \in \mathbf{Set}$ *and* $\varphi \in \mathcal{P}(I)$ *there exists* $f : I \to \mathrm{Prop}$ *with* $\mathcal{K}_{\perp\!\!\!\perp}(f)(\mathrm{tr}) \cong \varphi$

Internal logic of a tripos

We can use **(higher order) predicate logic** as notation and calculational tool for constructions in $\mathcal{P}$.

E.g. for $\varphi \in \mathcal{P}(A \times B), \psi \in \mathcal{P}(B \times C)$, write

$$\theta(x,z) \;\equiv\; \exists y\,.\,\varphi(x,y) \wedge \psi(y,z)$$

instead of

$$\theta \;=\; \exists_{\partial_1}(\partial_2{}^*\varphi \wedge \partial_0{}^*\psi).$$

$$\begin{tikzcd} & A \times B & \\ & A \times B \times C \arrow[u, "\partial_2"'] \arrow[r, "\partial_1"] \arrow[d, "\partial_0"] & A \times C \\ & B \times C & \end{tikzcd}$$

Given **predicates** $\varphi_1, \ldots, \varphi_n, \psi \in \mathcal{P}(A_1 \times \ldots \times A_k)$, say that the **judgment**

$$\varphi_1(\vec{x}), \ldots, \varphi_n(\vec{x}) \vdash_{\vec{x}} \psi(\vec{x})$$

is **valid**, if

$$\varphi_1 \wedge \cdots \wedge \varphi_n \leq \psi \quad \text{in} \quad \mathcal{P}(A_1 \times \ldots \times A_k).$$

More generally, $\varphi_1 \ldots \varphi_n, \psi$ can be **formulas** instead of (atomic) predicates.

Validity relation closed under deduction rules for classical predicate logic.

Lawvere: Equality predicate on A is given by $\exists_\delta \top$, where $\delta : A \to A \times A$

The tripos-to-topos construction

For any tripos $\mathcal{P} : \mathbf{Set}^{\mathrm{op}} \to \mathbf{Ord}$ we define a category $\mathbf{Set}[\mathcal{P}]$ as follows.

Definition

$\mathbf{Set}[\mathcal{P}]$ is the category where

- **objects** are pairs $(A \in \mathbf{Set}, \rho \in \mathcal{P}(A \times A))$ such that

$$\begin{array}{rl} \textit{(sym)} & \rho(x, y) \vdash \rho(y, x) \\ \textit{(trans)} & \rho(x, y), \rho(y, z) \vdash \rho(x, z) \end{array}$$

- **morphisms** $(A, \rho) \to (B, \sigma)$ are (equivalence classes of) predicates $\phi \in \mathcal{P}(A \times B)$ such that

$$\begin{array}{rll} \textit{(strict)} & \phi(x, y) \vdash \rho x \wedge \sigma y & \qquad [\text{short for } \rho(x, x) \wedge \sigma(y, y)] \\ \textit{(cong)} & \rho(x, x'), \phi(x', y), \sigma(y, y') \vdash \phi(x, y') & \\ \textit{(sv)} & \phi(x, y), \phi(x, y') \vdash \sigma(y, y') & \\ \textit{(tot)} & \rho x \vdash \exists y \,.\, \phi(x, y) & \end{array}$$

- $\phi, \phi' \in \mathcal{P}(A \times B)$ are identified as morphisms, if $\phi \cong \phi'$
- composition is relational composition

Lemma

For any tripos $\mathcal{P} : \mathbf{Set}^{\mathrm{op}} \to \mathbf{Ord}$, $\mathbf{Set}[\mathcal{P}]$ is a topos with a ***natural numbers object***

Conjunction as intersection

- tripos-to-topos construction only uses $\wedge, \exists$
- $\exists$ has easy representation, but encoding of $\wedge$ involves double-dualization, complicating computations
- for reasonable poles, there is an easier representation as **intersection type**

Syntactic order, support

Definition

Given a record

$$t = \langle \ell(x.\,p) \mid \ell \in F \rangle$$

and a set $M \subseteq \mathcal{L}$ of labels, define the *restriction of t to M* to be the record

$$t|_M \;=\; \langle \ell(x.\,p) \mid \ell \in F \cap M \rangle.$$

The *syntactic order* $\sqsubseteq$ on terms and programs is the reflexive-transitive and compatible closure of the set of all pairs $(t|_M, t)$

Definition

A *pole* $\perp\!\!\!\perp$ is called *strongly closed*, if it satisfies the conditions

$$p \to_\beta q, q \in \perp\!\!\!\perp \;\Rightarrow\; p \in \perp\!\!\!\perp \quad \text{and}$$
$$p \sqsubseteq q, p \in \perp\!\!\!\perp \;\Rightarrow\; q \in \perp\!\!\!\perp.$$

A *truth value* $S \subseteq \mathbb{T}$ is called *strongly closed*, if it satisfies

$$t \to_\beta u, u \in S \;\Rightarrow\; t \in S \quad \text{and}$$
$$t \sqsubseteq u, t \in S \;\Rightarrow\; u \in S.$$

Support, intersection

Definition

A truth value S is said to be *supported* by a set $M \subseteq \mathcal{L}$ of labels, if we have $s|_M \in S$ for every $s \in S$. More generally, a predicate $\varphi \in P(\mathbb{T})^J$ is said to be supported by M, if $\varphi(j)$ is supported by M for all $j \in J$.

Theorem

Let $\varphi, \psi \in P(\mathbb{T})^J$ be predicates that are both pointwise strongly closed, and supported by disjoint finite sets F and G of labels, respectively. Then the predicate $\varphi \cap \psi$, which is defined by $(\varphi \cap \psi)(j) = \varphi(j) \cap \psi(j)$, is a meet of φ and ψ and is supported by $F \cup G$.

If $\perp\!\!\!\perp$ is strongly closed, then every predicate is equivalent to a finitely supported strongly closed predicate, and they are closed under the logical operations.

Thanks for your attention!