Toposes for Time Complexity Classes

Jonas Frey

joint work with Jakob Grue Simonsen

Developments in Implicit Computational Complexity (DICE)

Eindhoven, 3 April 2016

Summary

- aim: construct realizability toposes from complexity classes, and use internal logic and geometric arguments for analysis
- one possibly : number realizability style, restrict complexity of realizers
- works, but does not yield toposes
- instead use Krivine's **classical realizability**, and represent complexity class by the 'pole'

Part I
Categorical Krivine realizability

Syntax:

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

reduction relation on processes:

(push)	$tu \star \pi$	$\succ$	$t \star u{\cdot}\pi$
(pop)	$(\lambda x\,.\,t[x]) \star u{\cdot}\pi$	$\succ$	$t[u] \star \pi$
(save)	$\mathfrak{cc} \star t{\cdot}\pi$	$\succ$	$t \star \mathsf{k}_\pi{\cdot}\pi$
(restore)	$\mathsf{k}_\pi \star t{\cdot}\rho$	$\succ$	$t \star \pi$

- non-logical instructions necessary for non-trivial realizability models

Krivine's classical realizability – basic ideas

Guiding intuitions:

- Combination of **Kleene realizability** and **negative translation**
- Syntax with **continuations** instead of **CPS translation**
- **Negation** replaced by $(-) \Rightarrow R$, for convenient R ('pole')
- different R give different **realizability models**

Notation, Terminology

- Λ set of closed terms
- Π set of stacks
- $\Lambda \star \Pi = \Lambda \times \Pi$ set of processes
- $QP \subseteq \Lambda$ set of **quasi-proofs** – 'pure' terms not containing any 'non-logical instructions' (continuations k_π allowed)

Definition

A **pole** is a set $\perp\!\!\!\perp \subseteq \Lambda \star \Pi$ of processes closed under inverse reduction, i.e.

$$t \star \pi \succ u \star \rho, \quad u \star \rho \in \perp\!\!\!\perp \quad \Rightarrow \quad t \star \pi \in \perp\!\!\!\perp$$

- Different poles $\perp\!\!\!\perp$ give different realizability models
- Example: termination pole

Example: The termination pole

- constant end (‘termination’) as only non-logical instruction
- define

$$(t \star \pi)\downarrow \quad \Leftrightarrow \quad \exists \rho \,.\, t \star \pi \succ^{*} \mathsf{end} \star \rho.$$
$$\mathfrak{T} \quad = \quad \{t \star \pi \in \Lambda \star \Pi \mid (t \star \pi)\downarrow\}$$

Truth values, ordering

- Fix a pole $\perp\!\!\!\perp$
- **Truth values** are subsets $P \subseteq \Pi$, elements are 'refutations'
- For $t \in \Lambda$, $P, Q \in \mathcal{P}(\Pi)$ define

$$\begin{array}{lcll} t \Vdash P & \Leftrightarrow & \forall \pi \in P \,.\, t \star \pi \in \perp\!\!\!\perp & (\text{'}t \text{ realizes } P\text{'}) \\ P^{\perp\!\!\!\perp} & = & \{t \in \Lambda \mid \forall \pi \in P \,.\, t \star \pi \in \perp\!\!\!\perp\} & (\text{'realizers'}) \\ P \Rightarrow Q & = & \{u \cdot \pi \mid u \Vdash P, \pi \in Q\} & \end{array}$$

- For $L \subseteq \Lambda$ define

$$L_{\perp\!\!\!\perp} = \{\pi \in \perp\!\!\!\perp \mid \forall t \in L \,.\, t \star \pi \in \perp\!\!\!\perp\}$$

- Define **ordering** on set $\mathcal{P}(\Pi)$ of truth values by

$$S \leq T \quad :\Leftrightarrow \quad \exists t \in QP \,.\, t \Vdash S \Rightarrow T$$

for $S, T \subseteq \Pi$ (restriction to *quasi-proofs* to avoid degeneracy)

Ordering on predicates

- **Predicates** are families of truth values, i.e. functions $\varphi, \psi : J \to \mathcal{P}(\Pi)$
- Define **ordering** on set $\mathcal{P}(\Pi)^J$ of predicates on J by

$$\varphi \leq \psi \quad :\Leftrightarrow \quad \exists t \in QP\, \forall j \in J\, .\, t \Vdash \varphi(j) \Rightarrow \psi(j)$$

- in Krivine's terminology, this would mean that the formula

$$\forall j : J\, .\, \varphi(j) \Rightarrow \psi(j)$$

  is realized by a quasi-proof
- ordering **uniform** – compare with pointwise ordering

$$\varphi \leq \psi \quad :\Leftrightarrow \quad \forall j \in J\, \exists t \in QP\, .\, t \Vdash \varphi(j) \Rightarrow \psi(j)$$

Predicates form a Boolean tripos

- The assignment $J \mapsto (\mathcal{P}(\Pi)^J, \leq)$ 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* $\mathcal{K}_{\perp\!\!\!\perp}(f) \vdash \forall_f : \mathcal{K}_{\perp\!\!\!\perp}(J) \to \mathcal{K}_{\perp\!\!\!\perp}(I)$*, 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* $\mathcal{K}_{\perp\!\!\!\perp}(f)(\mathrm{tr}) \cong \varphi$

We can use **(higher order) predicate logic 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

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

$$\begin{array}{ccc} A \times B & & \\ \uparrow{\scriptstyle \partial_2} & & \\ A \times B \times C & \xrightarrow{\partial_1} & A \times C \\ \downarrow{\scriptstyle \partial_0} & & \\ B \times C & & \end{array}$$

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 $\delta : A \to A \times A$

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

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

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

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

- $\phi, \phi' \in \mathcal{P}(A \times B)$ 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***

The constant objects functor

Definition

For a tripos $\mathcal{P}$, define the **constant objects functor**

$$\Delta \;:\; \mathbf{Set} \;\to\; \mathbf{Set}[\mathcal{P}]$$

by

$$\begin{array}{ccc} A & \mapsto & (A, =) \\ \downarrow f & \mapsto & \downarrow [\phi] \\ B & \mapsto & (B, =) \end{array} \qquad \text{where} \quad \phi(x, y) \;\equiv\; f(x) = y$$

The natural numbers object (NNO) of $\mathbf{Set}[\mathcal{P}]$ is given by the subobject of $\Delta(\mathbb{N})$ corresponding to the predicate

$$\mathrm{nat}(x) \;\equiv\; \forall X : P(\mathbb{N}) \,.\, X(0) \Rightarrow (\forall y \,.\, X(y) \Rightarrow X(y+1)) \Rightarrow X(x)$$

For **Grothendieck toposes**, the natural numbers object is simply $\Delta(\mathbb{N})$ (since Δ is a left adjoint)

Consistency

- Falsity is the set Π of *all* stacks
- $\mathcal{K}_{\perp\!\!\perp}$ is **consistent**, if there is no quasi-proof realizing Π

$$\begin{aligned} & \neg\exists t \in QP \,.\, t \Vdash \Pi \\ \Leftrightarrow \quad & \neg\exists t \in QP \,\forall \pi \in \Pi \,.\, t \star \pi \in \perp\!\!\perp \\ \Leftrightarrow \quad & \forall t \in QP \,\exists \pi \in \Pi \,.\, t \star \pi \notin \perp\!\!\perp \end{aligned}$$

Theorem

$\perp\!\!\perp \subseteq \Lambda\star\Pi$ *is consistent iff every* $t * \pi \in \perp\!\!\perp$ *contains a non-logical instruction.*

Proof.

If all elements of $\perp\!\!\perp$ contain non-logical instructions, then $t \star \varepsilon \notin \perp\!\!\perp$ for any quasi-proof t.
Conversely, if $t \star \pi \in \perp\!\!\perp$ is 'pure', then $\mathsf{k}_\pi t$ is a quasi-proof-realizing Π. □

- $\perp\!\!\perp$ is inconsistent iff **Set**$[\mathcal{K}_{\perp\!\!\perp}]$ is equivalent to the terminal category $\mathbf{1}$
- termination pole $\mathfrak{T}$ is consistent

Part II
Poles from complexity classes

- idea: represent complexity class (say PTIME) by the pole, i.e. take $\perp\!\!\!\perp$ to be set of processes of 'polynomial complexity'
- to make asymptotic statements about a single process, need input/arguments/data
- first approach was to use I/O instructions
- simpler approach leads to models that are easier to analyze

The PTIME pole

- syntax comprises non-logical constant end, and a special variable α representing input

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

- 'closed' means 'no free vars except α'
- $QP = \{t \in \Lambda \mid \mathsf{end} \notin t\}$ (α may appear in quasi-proofs)
- For $\sigma \in \{0,1\}^*$, let $\overline{\sigma}$ be the System F encoding of σ
- PTIME pole given by

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

- relation to computational complexity since the Krivine machine is a *reasonable model*

Truth values from sets of strings

For $U \subseteq \{0,1\}^*$ define truth value

$$A_U = \left\{ t \cdot \varepsilon \in \Pi \mid \exists P \in \mathbb{N}[X]\ \forall \sigma \in U\,.\,(t \star \varepsilon)[\overline{\sigma}/\alpha]{\downarrow}^{\leq P(|\sigma|)} \right\} \subseteq \Pi$$

Theorem

For $U \subseteq \{0,1\}^*$, we have

1. $A_{U^{\complement}} \leq \neg A_U$
2. $\neg A_U \leq A_{U^{\complement}}$ *iff U is decidable in polynomial time.*

in $(P(\mathfrak{P}), \leq)$.

Part III
Functors between classical realizability toposes

- Idea: construct functor **Set**$[\mathfrak{T}] \to$ **Set**$[\mathfrak{P}]$ from inclusion of terms w/o α in terms with α

$$\Lambda \subset \Lambda_\alpha$$

- mapping on truth values given by

$$\Delta : P(\Pi) \to P(\Pi), \qquad S \mapsto (S^{\mathfrak{T}})_{\mathfrak{P}}.$$

- problem: monotonicity of construction relies on following conjecture

Conjecture

For all $K, L \subseteq \Lambda_\alpha$ and $S \subseteq \Pi_\alpha$ we have $K \bot_{\mathfrak{P}} L \cdot S \;\Leftrightarrow\; K \bot_{\mathfrak{P}} (L_{\mathfrak{P}})^{\mathfrak{P}} \cdot S$.

- conjecture remains unresolved, but problem disappears when using a different syntax!

The CPS target language

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:

$$\langle \ell_1(x.\, p_1), \ldots, \ell_n(x.\, p_n) \rangle_{\ell_i} t \quad \succ \quad p_i[t/x] \qquad \text{if } 1 \leq i \leq n$$

Types:

$$A \quad ::= \quad X \mid \langle \ell_1(A_1), \ldots, \ell_n(A_n) \rangle \qquad n \geq 0$$

Typing rules:

$$\text{(Var)} \quad \frac{}{\Gamma \vdash x_i : A_i} \quad \Gamma \equiv x_1 : A_1, \ldots, x_n : A_n, \;\; 1 \leq i \leq n$$

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

$$\text{(Elim)} \quad \frac{\Gamma \vdash t : \langle \ell_1(B_1), \ldots, \ell_m(B_m) \rangle \qquad \Gamma \vdash u : B_i}{\Gamma \vdash t_{\ell_i}\, u} \quad 1 \leq i \leq m$$

Fix shorthands

$$\top \equiv \langle\rangle \qquad \neg A \equiv \langle \mathsf{k}(A) \rangle \qquad \neg(A, B) \equiv \langle \mathsf{l}(A), \mathsf{r}(B) \rangle$$

Define classical conjunction

$$A \wedge B \equiv \neg(\neg A, \neg B)$$

- For formulas A in $(\neg, \wedge)$-fragment of prop. logic define $A^\top$ by expanding connectives according to above
- Translate classical into CPS sequents

$$(A_1, \ldots, A_n \vdash B_1, \ldots, B_m)^\top \quad = \quad (A_1^\top, \ldots, A_n^\top, \neg B_1^\top, \ldots, \neg B_m^\top \vdash)$$

- $(\Gamma \vdash \Delta)$ provable in classical logic iff $(\Gamma \vdash \Delta)^\top$ provable in CPS logic

Classical realizability in the CPS target language

- $\mathbb{T}$ set of closed terms, $\mathbb{T}_0$ set of *pure* closed terms
- $\mathbb{P}$ set of closed programs
- $\perp\!\!\!\perp \subseteq \mathbb{P}$ closed under inverse $\succ$
- Truth values are sets $S, T \subseteq \mathbb{T}$ of closed terms
- For labels $\ell_1, \ldots, \ell_n$ and truth values $S_1, \ldots, S_n$ set

$$\langle \ell_1(S_1), \ldots, \ell_n(S_n) \rangle = \{ t \in \mathbb{T} \mid \forall i \in \{1, \ldots, n\}\ \forall s \in S_i \,.\, t_{\ell_i} s \in \perp\!\!\!\perp \}\,.$$

Thanks for your attention!