Classical Realizability

Jaap van Oosten

Department of Mathematics, Utrecht University

Cambridge Category Seminar, March 6, 2012

Classical Realizability was developed in the middle of the 1990s by Jean-Louis Krivine.
Its aim is twofold:

- Give new models for classical theories (in particular, set theory)
- Understand classical truth in terms which have computational meaning

In this talk, we concentrate on the first aspect.

Outline of the talk:

1) Description of Krivine's classical realizability
2) Krivine realizability as a tripos/topos construction
3) A connection with relative realizability

Sources:

1) Papers by Jean-Louis Krivine, see Krivine's home page: `http://www.pps.jussieu.fr/~krivine/`
2) Paper *Krivine's Classical Realizability from a Categorical Perspective* by Thomas Streicher (to appear in MSCS); available at Streicher's home page: `http://www.mathematik.tu-darmstadt.de/~streicher/`
3) Lecture Notes by Alexandre Miquel for 'Proofs and Programs' week at Luminy, Feb 13–17, 2012: available at `http://li2012.univ-mrs.fr/programme/week3/talks/` Strongly recommended, and shamelessly plagiarized in this talk
4) Some work by my student Wouter Stekelenburg (as yet unpublished)

There are two kinds of objects: *terms* (denoted $t, t', s, u, \ldots$) and *stacks* (denoted π, π').
We may have *stack constants* (basic stacks) from a set Π_0; we think of a stack as a sequence of closed terms ended by a stack constant. Given a closed term t and a stack π, we have a new stack $t.\pi$.
The terms come from a λ-calculus enriched with extra constants.
In this talk, we shall only consider the following extra constants:

> For every stack π there is a constant k_π (sometimes called *continuation constants*)
>
> There is a constant $\mathfrak{cc}$ (*call/cc*)

If we denote the set of stacks by Π and the set of terms by Λ, we have therefore the following formal syntax:

$\Pi ::= \alpha | t.\pi$ ($\alpha \in \Pi_0$, $t \in \Lambda$, t closed)

$\Lambda ::= x | \lambda x.t | tu | \mathfrak{cc} | k_\pi$ ($\pi \in \Pi$)

An element of $\Lambda \times \Pi$ (typically written as $t * \pi$) is called a *process*. There is a *reduction relation* on processes, generated by the following one-step reductions:

$$\begin{array}{ll} \text{Push} & tu * \pi \succ t * u.\pi \\ \text{Grab} & \lambda x.t * u.\pi \succ t[u/x] * \pi \\ \text{Save} & \mathfrak{cc} * u.\pi \succ u * k_\pi.\pi \\ \text{Restore} & k_\pi * u.\pi' \succ u * \pi \end{array}$$

This is called *Krivine's Abstract Machine*. Note that the first two rules implement *weak head reduction*:

$$(\lambda x_1 \cdots x_n.t)M_1 \cdots M_n * \pi \succ\succ t[M_1/x_1, \ldots, M_n/x_n] * \pi$$

A set of $\mathcal{U}$ processes is *saturated* if $t * \pi \in \mathcal{U}$ whenever $t * \pi \succ t' * \pi'$ and $t' * \pi' \in \mathcal{U}$.
We fix a saturated set of processes: a *pole* $\perp\!\!\!\perp$.
We also fix a set of terms: the set PL of *proof-like* terms. Krivine stipulates: PL is the set of closed terms which don't contain a continuation constant k_π (this may be too strict).

Logic

Consider a language in second-order logic: we have certain first-order constants, function symbols and relation symbols; first-order varables $x, y, \ldots$, second-order variables $X, Y, \ldots$ (of each arity ≥ 0), and the logical symbols $\rightarrow, \forall x, \forall X$.

We have the usual definitions:

$$\begin{array}{rcl} \bot & \equiv & \forall X.X \\ \neg A & \equiv & A \rightarrow \bot \\ A \wedge B & \equiv & \forall X.(A \rightarrow (B \rightarrow X)) \rightarrow X \\ A \vee B & \equiv & \forall X.(A \rightarrow X) \rightarrow ((B \rightarrow X) \rightarrow X) \\ \exists x A & \equiv & \forall X.(\forall x(A \rightarrow X) \rightarrow X) \\ \text{etc.} & & \end{array}$$

Curry Howard for Classical second-order logic

Define a derivation system of typing judgements $\Gamma \vdash t : A$ where Γ is a variable declaration $x_1 : A_1, \ldots, x_n : A_n$, the A_i are second-order formulas and t is a term:

$$\frac{}{\Gamma \vdash x : A}\ (x : A) \in \Gamma$$

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \to B}$$

$$\frac{\Gamma \vdash t : A \to B \qquad \Gamma \vdash u : A}{\Gamma \vdash tu : B}$$

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash t : \forall x A}\ x \notin FV(\Gamma)$$

$$\frac{\Gamma \vdash t : \forall x A}{\Gamma \vdash t : A[e/x]}$$

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash t : \forall X.A}\ X \notin FV(\Gamma)$$

$$\frac{\Gamma \vdash t : \forall X.A}{\Gamma \vdash t : A[P/X]}$$

And one classical rule (Peirce's Law):

$$\frac{}{\Gamma \vdash \text{cc} : ((A \to B) \to A) \to A}$$

Examples of derivable judgements:

$$\begin{array}{rcll} \textbf{pair} & \equiv & \lambda xyz.zxy & : \quad \forall XY.X \to (Y \to X \wedge Y) \\ \textbf{fst} & \equiv & \lambda z.z(\lambda xy.x) & : \quad \forall XY.X \wedge Y \to X \\ \textbf{left} & \equiv & \lambda xuv.ux & : \quad \forall XY.X \to X \vee Y \\ \textbf{right} & \equiv & \lambda yuv.vy & : \quad \forall XY.Y \to X \vee Y \end{array}$$

and also

$$\textbf{EM} \equiv \text{cc}(\lambda k.\textbf{right}(\lambda x.k(\textbf{left}x))) : \forall X.X \vee \neg X$$

Realizability

Suppose we are given a set U of individuals. Relative to an assignment of variables, where elements of U are assigned to first-order variables and functions $U^k \to \mathcal{P}(\Pi)$ are assigned to k-ary predicate variables, we now assign to any formula A a set of stacks $\|A\|$, a set of "witnesses against A". The set of *realizers of* A, written $|A|$, is defined as

$$|A| = \{t \in \Lambda \mid \forall \pi \in \|A\| \; t * \pi \in \perp\!\!\!\perp\}$$

The definition is simple:

$$\begin{array}{rcl} \|A \to B\| & = & |A|.\|B\| = \{t.\pi \mid t \in |A|, \pi \in \|B\|\} \\ \|\forall x A\| & = & \bigcup_{u \in U} \|A(u)\| \\ \|\forall X.A\| & = & \bigcup_{F : U^k \to \mathcal{P}(\Pi)} \|A(F)\| \end{array}$$

Then $|\forall x A| = \bigcap_{u \in U} |A(u)|$, etc.

A complication: if the pole $\perp\!\!\!\perp$ is empty, we always have: $|A| = \emptyset$ or $|A| = \Lambda$. We have classical, two-valued semantics.
On the other hand, if the pole contains one process, say $t * \pi$, then by the rule (Restore) we have $k_\pi * t.\pi' \in \perp\!\!\!\perp$ for any π'; whence by (Push), $k_\pi t * \pi' \in \perp\!\!\!\perp$ for any π'; which means that $k_\pi t \in |A|$ for any A, in particular for $A \equiv \forall X.X$.
Therefore we say: a closed formula A is *true* under this realizability, if its set $|A|$ of realizers contains an element of PL, the set of proof-like terms.
Strong Soundness Theorem Suppose the typing judgement $x_1 : A_1, \ldots, x_n : A_n \vdash t : B$ is derivable; suppose that relative to an assignment ρ we have $u_1 \in |A_1[\rho]|, \ldots, u_n \in |A_n[\rho]|$. Then

$$t[u_1/x_1, \ldots, u_n/x_n] \in |B[\rho]|$$

Note that the hypothesis implies that t is proof-like; so if $u_1, \ldots, u_n$ are proof-like, so is $t(u_1, \ldots, u_n)$.

Examples

1. For any A, B and term t:

$$t \in |A \to B| \;\Rightarrow\; \forall u(u \in |A| \Rightarrow tu \in |B|)$$

For, suppose $\pi \in \|B\|$, $u \in |A|$. Then $u.\pi \in \|A \to B\|$ so $t * u.\pi \in \perp\!\!\!\perp$; by (Push), $tu * \pi \in \perp\!\!\!\perp$.

2. For any A and B: if $\pi \in \|A\|$ then $k_\pi \in |A \to B|$. For, suppose $\pi \in \|A\|$, $u.\rho \in \|A \to B\|$ so $u \in |A|$, $\rho \in \|B\|$. Then $u * \pi \in \perp\!\!\!\perp$ whence by (Restore), $k_\pi * u.\rho \in \perp\!\!\!\perp$.

3. Let us see that $\mathfrak{cc}$ realizes Peirce's Law: suppose $t.\pi \in \|((A \to B) \to A) \to A\|$, so $t \in |(A \to B) \to A|$, $\pi \in \|A\|$. Then $k_\pi \in |A \to B|$, so $k_\pi.\pi \in \|(A \to B) \to A\|$. Hence $t * k_\pi.\pi \in \perp\!\!\!\perp$. By (Save), $\mathfrak{cc} * t.\pi \in \perp\!\!\!\perp$. we conclude that $\mathfrak{cc} \in |((A \to B) \to A) \to A|$

Equality and the natural numbers

Given a set X of individuals we can put for $e, e' \in X$:

$$\begin{aligned} \|e \asymp e'\| &= \bigcup_{F:X\to\mathcal{P}(\Pi)} \|F(e) \to F(e')\| \\ &= \|\forall X.X(e) \to X(e')\| \end{aligned}$$

If $X = \mathbb{N}$ and we have function symbols for the basic functions on $\mathbb{N}$, we can realize most of the Peano axioms:

$$\forall x \neg(x = 0)$$
$$\forall xy(s(x) = s(y) \to x = y)$$
$$\text{etc.}$$

but not induction. For induction to work, we have to relativise the quantifiers to a predicate N, defined by:

$$N(x) \equiv \forall X.(X(0) \wedge \forall y(X(y) \to X(s(y))) \to X(x)$$

So far the treatment of Krivine/Miquel. Can we understand this interpretation in terms of categorical logic?

Definition. A tripos on Set is a pseudofunctor $P : \mathrm{Set}^{\mathrm{op}} \to \mathrm{Preord}$, satisfying:

a) For each set X the preorder PX is endowed with a binary operation $(\cdot) \to (\cdot)$ which obeys the laws of intuitionistic implicational logic (e.g., $\phi \leq \psi \to \phi$, $\theta \to (\phi \to \psi) \leq (\theta \to \phi) \to (\theta \to \psi)$);

b) For every function $f : X \to Y$ of sets, the map $Pf : PY \to PX$ preserves $\to$ up to isomorphism. Moreover, Pf has a right adjoint $\forall f$, which satisfies the Beck condition and the condition that for $\phi \in PX$, $\psi \in PY$,

$$\forall f(Pf(\psi) \to \phi) \simeq \psi \to \forall f(\phi)$$

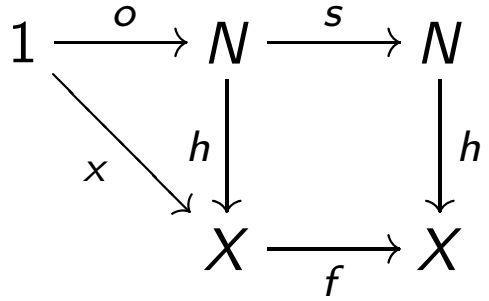
c) There is a *generic predicate*: a set Σ and an element $\sigma \in P\Sigma$ with the property that for every $\phi \in PX$ there is a function $\{\phi\} : X \to \Sigma$ such that $P\{\phi\}(\sigma) \simeq \phi$.

Every tripos on Set gives rise to a model of second-order logic.
Formulas with parameters from a set X are interpreted as elements of PX
Second-order (unary) predicates are interpreted as elements of Σ^X (where Σ is the carrier of a chosen generic predicate)
The element relation must be an element of $P(\Sigma^X \times X)$: it can be taken as $P(\mathrm{ev})(\sigma)$ where $\mathrm{ev} : \Sigma^X \times X \to \Sigma$ is the evaluation map.
A closed formula is interpreted as an alement of $P1$ (1 a fixed one-element set); it is *true* if its interpretation is the top element in this preorder.

For a tripos P on Set we can construct a topos $\mathrm{Set}[P]$:
Objects are pairs $(X, \sim)$ where $\sim$ is an element of $P(X \times X)$ such that the statements

$$\forall xy(x \sim y \to y \sim x)\ ,\ \forall xyz(x \sim y \wedge y \sim z \to x \sim z)$$

are true in the tripos P
A morphism $(X, \sim) \to (Y, \sim')$ is an equivalence class of a "functional relation": an element of $P(X \times Y)$ for which statements saying that it is extensional w.r.t. $\sim$ and $\sim'$, single-valued and total, are true in the tripos P
The topos $\mathrm{Set}[P]$ has a *natural numbers object*: an object N together with morphisms $1 \xrightarrow{o} N$ and $N \xrightarrow{s} N$ such that for every diagram $1 \xrightarrow{x} X \xrightarrow{f} X$ there is a unique map $h : N \to X$ making the following diagram commute:



To construct a natural numbers object in $\mathrm{Set}[P]$, take any set M with an element m and an injective function $M \xrightarrow{\tau} M$ for which $m \notin \mathrm{rge}(\tau)$. Define a predicate on M in the tripos P (i.e., an element of PM):

$$N(x) \equiv \forall X.(m \in X \wedge \forall y(y \in X \to \tau(y) \in X) \to x \in X$$

Now if one defines $\sim \in P(M \times M)$ by

$$x \sim y \equiv N(x) \wedge x \asymp y$$

then $(M, \sim)$ is a natural numbers object in $\mathrm{Set}[P]$

Krivine's realizability defines a Boolean tripos $\mathcal{K}$ on Set: for a set X, let $\mathcal{K}X$ be the set of functions $X \to \mathcal{P}(\Pi)$. Given such a function ϕ, we define $|\phi(x)|$ by

$$|\phi(x)| \;=\; \{t \in \Lambda \,|\, \forall \pi \in \phi(x)\, t * \pi \in \perp\!\!\!\perp\}$$

Define $\to$ on $\mathcal{K}X$ by

$$(\phi \to \psi)(x) \;=\; \{t.\pi \,|\, t \in |\phi(x)|,\ \pi \in \psi(x)\}$$

The order is given by: $\phi \leq \psi$ if and only if $\bigcap_x |(\phi \to \psi)(x)|$ contains a proof-like term.
For $f : X \to Y$, $\mathcal{K}f : \mathcal{K}Y \to \mathcal{K}X$ is given by composition with f. So $\mathcal{K}f$ preserves $\to$ and is order-preserving. Its right adjoint $\forall f$ is given by

$$\forall f(\phi)(y) \;=\; \|\forall x(f(x) \asymp y \to \phi(x)\|$$

Recall that $\|\forall x(f(x) \asymp y \to \phi(x)\| =$
$\bigcup_{x \in X} \{t.\pi \,|\, t \in |f(x) \asymp y|,\ \pi \in \phi(x)\}$

For any tripos P on Set, the equality $\asymp$ gives rise to a functor $\nabla : \mathrm{Set} \to \mathrm{Set}[P]$: send X to $(X, \asymp)$.
The natural numbers object N is a subobject of $\nabla(\mathbb{N})$
Sometimes, N is isomorphic to $\nabla(\mathbb{N})$. In traditional intuitionistic realizability examples, $\nabla(\mathbb{N})$ has 0 and a successor map but no discernable arithmetical structure.
Miquel has investigated the inclusion $N \subset \nabla(\mathbb{N})$ in a particular model (i.e., choice of pole) of Krivine realizability. There is very interesting structure there! Somewhat of the flavour of nonstandard arithmetic/analysis.

Thomas Streicher has given a reformulation of Krivine's realizability in terms reminiscent of combinatory logic.
An *abstract Krivine structure* consists of:

- a set Λ of "terms", with elements K, S and $\mathfrak{cc}$
- a subset PL of Λ: the 'proof-like terms'
- a set Π of "stacks"
- an application operation $t, s \mapsto ts : \Lambda \times \Lambda \to \Lambda$
- an operation $t, \pi \mapsto t.\pi : \Lambda \times \Pi \to \Pi$
- an operation $k_{(\_)} : \Pi \to \Lambda$
- and a 'pole', a saturated subset $\perp\!\!\!\perp$ of $\Lambda \times \Pi$

As usual, we write elements of $\Lambda \times \Pi$ as $t * \pi$

The saturatedness of $\perp\!\!\!\perp$ means that the following axioms are satisfied:

$$
\begin{array}{ll}
(\mathrm{S1}) & \text{if } t * s.\pi \in \perp\!\!\!\perp \text{ then } ts * \pi \in \perp\!\!\!\perp \\
(\mathrm{S2}) & \text{if } t * \pi \in \perp\!\!\!\perp \text{ then } K * t.s.\pi \in \perp\!\!\!\perp \\
(\mathrm{S3}) & \text{if } tu(su) * \pi \in \perp\!\!\!\perp \text{ then } S * t.s.u.\pi \in \perp\!\!\!\perp \\
(\mathrm{S4}) & \text{if } t * k_\pi.\pi \in \perp\!\!\!\perp \text{ then } \mathfrak{cc} * t.\pi \in \perp\!\!\!\perp \\
(\mathrm{S5}) & \text{if } t * \pi \in \perp\!\!\!\perp \text{ then } k_\pi * t.\pi' \in \perp\!\!\!\perp
\end{array}
$$

Again, we have a tripos: $PX = \mathcal{P}(\Pi)^X$
$\phi \leq \psi$ if and only if $\bigcap_{x \in X} |\phi(x) \to \psi(x)|$ contains a proof-like element, where:
$|\chi(x)| = \{t \in \Lambda \,|\, \forall \pi \in \chi(x)\; t * \pi \in \perp\!\!\!\perp\}$
$\phi(x) \to \psi(x) = \{t.\pi \,|\, t \in |\phi(x)|, \pi \in \psi(x)\}$

Streicher's formulation facilitates drawing a parallel with 'relative realizability'.

A *partial combinatory algebra* (pca) is a set A with a *partial* application function $t, s \mapsto ts : A \times A \rightharpoonup A$, and elements k, s satisfying:

$$\begin{aligned} kxy &= x \\ sxyz &\simeq xz(yz) \end{aligned}$$

Given a pca A we have a tripos P_A, the *realizability tripos* on A: $P_A X = \mathcal{P}(A)^X$; $\phi \leq \psi$ iff $\bigcap_{x \in X} \phi(x) \to \psi(x)$ is nonempty, where for $U, V \subseteq A$: $U \to V = \{a \in A \,|\, \forall x \in U ax \in V\}$

In a pca one can define λ-terms. For example, $\lambda x.x = SKK$

Examples of pcas:

$\mathbb{N}$ with $nm = \{n\}m$

$\mathbb{N}^{\mathbb{N}}$ with 'partial continuous application'

Relative realizability triposes:
now we consider an inclusion $A^\sharp \subset A$ of pcas such that the application on $A^\sharp$ is the restriction of the one on A, and $A^\sharp$ contains elements k and s which satisfy the axioms for both A and $A^\sharp$.
Prime example: $A = \mathbb{N}^\mathbb{N}$, $A^\sharp$ is the set of total recursive functions (this gives the notion of 'Kleene-Vesley' realizability).
We have a relative realizability tripos $P_{A^\sharp,A}$:
$P_{A^\sharp,A}X = \mathcal{P}(A)^X$
$\phi \leq \psi$ iff $\bigcap_x \phi(x) \to \psi(x)$ contains an element of $A^\sharp$.

In the case of a realizability tripos P_A, the preorder $P_A 1$ is equivalent to the total order on two elements.
In the case of $P_{A^\sharp,A}$, $P_{A^\sharp,A}1$ can be very complicated. In our prime example ($A = \mathbb{N}^{\mathbb{N}}$, $A^\sharp$ the set of recursive functions), $P_{A^\sharp,A}1$ is equivalent to the (opposite of the) *lattice of Medvedev degrees*.
Fix a subset $\mathcal{U}$ of $A - A^\sharp$ (a nontrivial Medvedev degree).
We shall define an abstract Krivine structure à la Streicher.
Let $\Lambda = A$, and Π the set of coded finite sequences of elements of A (in any pca, one has a coding of such sequences). Let $a.\pi$ be the code of the sequence obtained by appending a to the sequence coded by π.

Define a pole $\perp\!\!\!\perp$ by:

$$\perp\!\!\!\perp = \{t * \pi \mid t\pi \text{ is defined and an element of } \mathcal{U}\}$$

define a new, total, application on A by:

$$a \cdot b = \lambda\pi.a(b.\pi)$$

Our set PL of proof-like terms is $A^\sharp$.
For the rest of the structure, let $\pi_{\geq k}$ be a code of the sequence $\pi_k, \pi_{k+1}, \ldots$, if π is code of the sequence $\pi_0, \pi_1, \ldots$. Then define:

$$\begin{array}{rcl} K & = & \lambda\pi.\pi_0(\pi_{\geq 2}) \\ S & = & \lambda\rho.\rho_0(\rho_2.[\lambda\nu.\rho_1(\rho_2.\nu)].\rho_{\geq 3}) \\ k_\pi & = & \lambda\rho.\rho_0\pi \\ \text{cc} & = & \lambda\rho.\rho_0(k_{\rho_{\geq 1}}.\rho_{\geq 1}) \end{array}$$

We have: (S1) if $t * s.\pi \in \perp\!\!\!\perp$, then $t(s.\pi) \in \mathcal{U}$, so $(t \cdot s)\pi \in \mathcal{U}$, therefore $t \cdot s * \pi \in \perp\!\!\!\perp$, etc.

The tripos obtained from this abstract Krivine structure can equivalently be described as follows:
define a new preorder on the sets $P_{A^\sharp,A}X$, by putting:
$\phi \leq \psi$ iff the set $\bigcap_x \phi(x) \to [(\psi(x) \to \mathcal{U}) \to \mathcal{U}]$ contains an element of $A^\sharp$.
The topos one constructs from this tripos is the Booleanization of a cosed subtopos of $\mathrm{Set}[P_{A^\sharp,A}]$