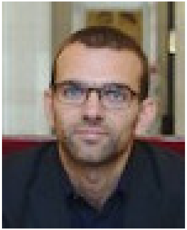
Normalization by realizability

Pierre-Évariste Dagand, Lionel Rieg, **Gabriel Scherer**

April 30, 2021



In this work

We study the

computational meaning

of the *adequacy lemma* of

classical realizability

without using extraction, but direct

dependently-typed programming

using Curien-Herbelin

$$\mu\tilde{\mu}$$

calculi as our realizer language.

Section 1

Classical realizability

Classical realizability: minimal history

Classical realizability is a *realizability* interpretation of logics where formulas are "realized" by λ-calculus abstract machines.

Introduced in the 1990s by Jean-Louis Krivine, providing a simple approach to "realize" classical axioms as control operators.

Later work focused on realizing more "classical" axioms, in particular the family of axioms of choice.

To a programming-language-research person, classical realizability looks like a unary logical relation defined in a systematic, symmetric way.

Classical realizability: overview

A soundness technique for *abstract machines* formed of a pair $\langle t \mid e \rangle$ (in $\mathbb{M}$) of a *term* t (in $\mathbb{T}$) and a *co-term* (context) e (in $\mathbb{E}$).

Classical realizability: overview

A soundness technique for *abstract machines* formed of a pair $\langle\, t \mid e \,\rangle$ (in $\mathbb{M}$) of a *term* t (in $\mathbb{T}$) and a *co-term* (context) e (in $\mathbb{E}$).

For the right definitions, we prove an *adequacy lemma* saying that:

- well-typed terms $t : A$ belong to a set of *truth witnesses* $|A|$
- well-typed co-terms $e : A$ belong to a set of *falsity witnesses* $\|A\|$
- well-typed machines $\langle\, t \mid e \,\rangle$ belong to a *pole* $\perp\!\!\!\perp$.

Those sets capture *good* (sound) terms/coterms/machines.
Here, we define $\perp\!\!\!\perp$ as the set of machines that reduce to a valid machine in normal form.

Classical realizability: overview

A soundness technique for *abstract machines* formed of a pair $\langle t \mid e \rangle$ (in $\mathbb{M}$) of a *term* t (in $\mathbb{T}$) and a *co-term* (context) e (in $\mathbb{E}$).

For the right definitions, we prove an *adequacy lemma* saying that:

- well-typed terms $t : A$ belong to a set of *truth witnesses* $|A|$
- well-typed co-terms $e : A$ belong to a set of *falsity witnesses* $\|A\|$
- well-typed machines $\langle t \mid e \rangle$ belong to a *pole* $\perp\!\!\!\perp$.

Those sets capture *good* (sound) terms/coterms/machines.
Here, we define $\perp\!\!\!\perp$ as the set of machines that reduce to a valid machine in normal form.

We will define $|A|$ and $\|A\|$ such that
$t \in |A|$ and $e \in \|A\|$ imply $\langle t \mid e \rangle \in \perp\!\!\!\perp$.

Orthogonality is central to this:

$$\mathcal{T}^{\perp} \triangleq \{e \mid \forall t \in \mathcal{T},\ \langle t \mid e \rangle \in \perp\!\!\!\perp\} \qquad \mathcal{E}^{\perp} \triangleq \{t \mid \forall e \in \mathcal{E},\ \langle t \mid e \rangle \in \perp\!\!\!\perp\}$$

Classical realizability: abstract machines

λ-terms:

$$t \triangleq x \mid \lambda x.\, t \mid t\ u \qquad\qquad (\lambda x.\, t)\ u \rightsquigarrow t[u/x]$$

Abstract machines (for now):

$$\begin{array}{rcl} e & \triangleq & \star \mid u \cdot e \\ t & \triangleq & x \mid \lambda x.\, t \mid t\ u \\ m & \triangleq & \langle\, t \,|\, e \,\rangle \end{array} \qquad\qquad \begin{array}{rcl} \langle\, t\ u \,|\, e \,\rangle & \rightsquigarrow & \langle\, t \,|\, u \cdot e \,\rangle \\ \langle\, \lambda x.\, t \,|\, u \cdot e \,\rangle & \rightsquigarrow & \langle\, t[u/x] \,|\, e \,\rangle \end{array}$$

Simulation: if $\langle\, \lfloor t \rfloor \,|\, \star \,\rangle \rightsquigarrow^* \langle\, \lfloor u \rfloor \,|\, \star \,\rangle \not\rightsquigarrow$ then $t \rightsquigarrow^* u \not\rightsquigarrow$.

Classical realizability: abstract machines

λ-terms:

$$t \triangleq x \mid \lambda x.\, t \mid t\ u \qquad\qquad (\lambda x.\, t)\ u \rightsquigarrow t[u/x]$$

Abstract machines (for now):

$$\begin{array}{rcl} e & \triangleq & \star \mid u \cdot e \\ t & \triangleq & x \mid \lambda x.\, t \mid t\ u \\ m & \triangleq & \langle\, t \mid e \,\rangle \end{array} \qquad \begin{array}{rcl} \langle\, t\ u \mid e \,\rangle & \rightsquigarrow & \langle\, t \mid u \cdot e \,\rangle \\ \langle\, \lambda x.\, t \mid u \cdot e \,\rangle & \rightsquigarrow & \langle\, t[u/x] \mid e \,\rangle \end{array}$$

Simulation: if $\langle\, \lfloor t \rfloor \mid \star \,\rangle \rightsquigarrow^* \langle\, \lfloor u \rfloor \mid \star \,\rangle \not\rightsquigarrow$ then $t \rightsquigarrow^* u \not\rightsquigarrow$.

$$\begin{array}{rcl} \langle\, (\lambda x.\, t)\ u \mid \star \,\rangle & \rightsquigarrow & \langle\, \lambda x.\, t \mid u \cdot \star \,\rangle \\ & \rightsquigarrow & \langle\, t[u/x] \mid \star \,\rangle \end{array}$$

Classical realizability: realizability structure

A *realizability structure* is a triple $(\mathbb{T}, \mathbb{E}, \perp\!\!\!\perp)$ where

- $\mathbb{T}$ is a set of machine terms
- $\mathbb{E}$ is a set of machine contexts
- $\perp\!\!\!\perp$ is a set of machines

such that:

- $\mathbb{T}, \mathbb{E}$ are closed by terms and context constructors, for example:

$$\star \in \mathbb{E} \qquad\qquad t \in \mathbb{T} \;\wedge\; e \in \mathbb{E} \implies (t \cdot e) \in \mathbb{E}$$

- $\perp\!\!\!\perp$ is closed by anti-reduction:

$$\left\langle\, t' \,\middle|\, e' \,\right\rangle \in \perp\!\!\!\perp \quad \wedge \quad \langle\, t \,|\, e \,\rangle \rightsquigarrow \left\langle\, t' \,\middle|\, e' \,\right\rangle \quad \implies \quad \langle\, t \,|\, e \,\rangle \in \perp\!\!\!\perp$$

Classical realizability: truth and falsity witnesses

The function type $A \to B$ is a *negative* type.
It is determined by its *falsity witnesses* that are *values*: $\|A \to B\|_V$.
The rest follows by orthoginality. For example:

$$\begin{aligned} \|A \to B\|_V &\triangleq |A| \cdot \|B\|_V \\ |A \to B| &\triangleq \|A \to B\|_V^{\perp} \\ \|A \to B\| &\triangleq |A \to B|^{\perp} \end{aligned}$$

For a positive type we could have, for example:

$$|A + B|_V \triangleq |A|_V + |B|_V$$

In general, for positives P and negatives N we have:

$$\begin{aligned} \|P\| &\triangleq |P|_V^{\perp} \\ |P| &\triangleq |P|_V^{\perp\perp} \end{aligned} \qquad \begin{aligned} |N| &\triangleq \|N\|_V^{\perp} \\ \|N\| &\triangleq \|N\|_V^{\perp\perp} \end{aligned}$$

Reminder: $\mathcal{T}^{\perp} \triangleq \{e \mid \forall t \in \mathcal{T},\ \langle\, t \mid e \,\rangle \in \perp\!\!\!\perp\}$

Classical realizability: the adequacy lemma

$$\Gamma \vdash t : A \quad \Longrightarrow \quad \forall \rho \in |\Gamma|,\ \lfloor t \rfloor \in |A|$$

$$\text{where: } \rho \in |\Gamma| \iff \forall (x : A) \in \Gamma,\ \rho(x) \in |A|$$

Example proof case:

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

$$\begin{array}{cll}
 & & (\lambda x.\, t)[\rho] \in |A \to B| = \|A \to B\|_V^{\perp} \\
\iff & \forall e' \in \|A \to B\|_V, & \langle (\lambda x.\, t)[\rho] \mid e' \rangle \in \perp\!\!\!\perp \\
\iff & \forall u \in |A|, e \in \|B\|_V, & \langle (\lambda x.\, t)[\rho] \mid u \cdot e \rangle \in \perp\!\!\!\perp \\
\Leftarrow & \forall u \in |A|, e \in \|B\|_V, & \langle t[\rho, u/x] \mid e \rangle \in \perp\!\!\!\perp \\
\Leftarrow & \forall u \in |A|, e \in \|B\|_V, & t[\rho, u/x] \in |B|, \quad e \in \|B\|_V \\
\Leftarrow & & \text{ind. hyp.}
\end{array}$$

Classical realizability: weak normalization

Let us define:

- $\mathbb{T}$ as the set of *closed* terms
- $\mathbb{E}$ as the set of *closed* contexts (may contain $\star$)
- $\perp\!\!\!\perp$ as the set of weakly-normalizing machines

$$m \in \perp\!\!\!\perp \quad \triangleq \quad \exists m_1, \ldots, m_n, t, \quad m \rightsquigarrow m_1 \rightsquigarrow \ldots \rightsquigarrow m_n = \langle\, \lambda x.\, t \,|\, \star \,\rangle$$

This forms a realizability structure (note: antireduction).
From the adequacy lemma we get weak normalization:

	$\vdash t : A$	
$\Longrightarrow$	$t \in \lvert A \rvert$	adequacy lemma
$\Longrightarrow$	$\langle\, t \,\vert\, \star \,\rangle \in \perp\!\!\!\perp$	$\star \in \lVert A \rVert$
$\Longrightarrow$	t normalizes	simulation

Section 2

Our work: computational content

General approach

To study the computational content of the proof,
we *implement* it in a dependently-typed meta-language.

Note: not program extraction. (Various previous work.)

Relevant definitions

We turn the proposition $\langle\, t \mid e \,\rangle \in \perp\!\!\!\perp$ into a datatype of *concrete evidence*:

$$(\_ \in \perp\!\!\!\perp) : \mathbb{M} \to \mathsf{Type}$$

$$m \in \perp\!\!\!\perp \triangleq \{m_n \in \mathbb{M}_N \mid m \rightsquigarrow m_1 \rightsquigarrow \ldots \rightsquigarrow m_n\}$$

Relevant definitions

We turn the proposition $\langle\, t \mid e \,\rangle \in \perp\!\!\!\perp$ into a datatype of *concrete evidence*:

$$(\_ \in \perp\!\!\!\perp) : \mathbb{M} \to \mathsf{Type}$$

$$m \in \perp\!\!\!\perp \triangleq \{m_n \in \mathbb{M}_N \mid m \rightsquigarrow m_1 \rightsquigarrow \ldots \rightsquigarrow m_n\}$$

Truth and falsity value witnesses have specific shapes:

$$\|A \to B\|_V \triangleq |A| \cdot \|B\|_V$$

$$\pi \in \|A \to B\|_V \triangleq \begin{array}{l} \texttt{match } \pi \texttt{ with} \\ \left| \begin{array}{l} u \cdot e \to u \in |A| \times e \in \|B\| \\ \quad \_ \quad \to \bot \end{array} \right. \end{array}$$

Relevant definitions

We turn the proposition $\langle\, t \,|\, e \,\rangle \in \perp\!\!\!\perp$ into a datatype of *concrete evidence*:

$$(\_ \in \perp\!\!\!\perp) : \mathbb{M} \to \mathsf{Type}$$

$$m \in \perp\!\!\!\perp \triangleq \{m_n \in \mathbb{M}_N \mid m \rightsquigarrow m_1 \rightsquigarrow \ldots \rightsquigarrow m_n\}$$

Truth and falsity value witnesses have specific shapes:

$$\|A \to B\|_V \triangleq |A| \cdot \|B\|_V$$

$$\pi \in \|A \to B\|_V \triangleq \begin{array}{l} \texttt{match } \pi \texttt{ with} \\ \left|\begin{array}{l} u \cdot e \to u \in |A| \times e \in \|B\| \\ \_ \quad\;\; \to \bot \end{array}\right. \end{array}$$

The notion of orthogonality is also made computational:

$$\mathcal{T}^{\perp} \triangleq \{e \mid \forall t \in \mathcal{T},\ \langle\, t \,|\, e \,\rangle \in \perp\!\!\!\perp\}$$

$$e \in |A|^{\perp} \triangleq \forall \{t : \mathbb{T}\}.\, t \in |A| \to \langle\, t \,|\, e \,\rangle \in \perp\!\!\!\perp$$

Conclusion

We are done: the way we defined truth and value witnesses (the shape of values) *completely determines* the evaluation strategy and its implementation.

We found it rather fun – I'll try to show you a bit of it.

Simplification

$m \in \perp\!\!\!\perp$ is dependent on the machine m, $t \in |A|$ on t, etc.
As a first step, we can remove this dependency by defining, for each predicate $\_ \in T$, a non-dependent type $\mathcal{J}(T)$.

$$m \in \perp\!\!\!\perp \triangleq \{m_n \in \mathbb{M}_N \mid m \rightsquigarrow m_1 \rightsquigarrow \ldots \rightsquigarrow m_n\}$$

$$\mathcal{J}(\perp\!\!\!\perp) \triangleq \mathbb{M}_N$$

Simplification

$m \in \perp\!\!\!\perp$ is dependent on the machine m, $t \in |A|$ on t, etc.
As a first step, we can remove this dependency by defining, for each predicate $\_ \in T$, a non-dependent type $\mathcal{J}(T)$.

$$m \in \perp\!\!\!\perp \triangleq \{m_n \in \mathbb{M}_N \mid m \rightsquigarrow m_1 \rightsquigarrow \ldots \rightsquigarrow m_n\}$$

$$\mathcal{J}(\perp\!\!\!\perp) \triangleq \mathbb{M}_N$$

$$u \cdot e \in \|A \to B\|_V \triangleq u \in |A| \times e \in \|B\|$$

$$\mathcal{J}(\|A \to B\|_V) \triangleq \mathcal{J}(|A|) \times \mathcal{J}(\|B\|_V)$$

Simplification

$m \in \perp\!\!\!\perp$ is dependent on the machine m, $t \in |A|$ on t, etc.
As a first step, we can remove this dependency by defining, for each predicate $\_ \in T$, a non-dependent type $\mathcal{J}(T)$.

$$m \in \perp\!\!\!\perp \triangleq \{m_n \in \mathbb{M}_N \mid m \rightsquigarrow m_1 \rightsquigarrow \ldots \rightsquigarrow m_n\}$$

$$\mathcal{J}(\perp\!\!\!\perp) \triangleq \mathbb{M}_N$$

$$u \cdot e \in \|A \to B\|_V \triangleq u \in |A| \times e \in \|B\|$$

$$\mathcal{J}(\|A \to B\|_V) \triangleq \mathcal{J}(|A|) \times \mathcal{J}(\|B\|_V)$$

$$t \in \|A\|^\perp \triangleq \forall \{e : \mathbb{E}\}.\, e \in \|A\| \to \langle\, t \mid e \,\rangle \in \perp\!\!\!\perp$$

$$\mathcal{J}(\|A\|^\perp) \triangleq \mathcal{J}(\|A\|) \to \mathcal{J}(\perp\!\!\!\perp)$$

Adequacy, computationally

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \rho \in |\Gamma| \to t[\rho] \in |A|$$

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \mathcal{J}(|\Gamma|) \to \mathcal{J}(|A|)$$

Adequacy, computationally

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \rightarrow \rho \in |\Gamma| \rightarrow t[\rho] \in |A|$$

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \rightarrow \mathcal{J}(|\Gamma|) \rightarrow \mathcal{J}(|A|)$$

$$\texttt{rea}\,(t^{A\rightarrow B}\ u^{A})\ \bar{\rho}^{|\Gamma|}\ \triangleq\ ? : \mathcal{J}(|B|)$$

$$\mathcal{J}(|B|) = \mathcal{J}(\|B\|_V) \rightarrow \mathcal{J}(\perp\!\!\!\perp)$$

Adequacy, computationally

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \rightarrow \rho \in |\Gamma| \rightarrow t[\rho] \in |A|$$

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \rightarrow \mathcal{J}(|\Gamma|) \rightarrow \mathcal{J}(|A|)$$

$$\texttt{rea}\,(t^{A \rightarrow B}\ u^{A})\,\bar{\rho}^{|\Gamma|} \triangleq \qquad \lambda\bar{\pi} \quad {}^{\|B\|_V}.\ ? : \mathcal{J}(\perp\!\!\!\perp)$$

$$\mathcal{J}(|B|) = \mathcal{J}(\|B\|_V) \rightarrow \mathcal{J}(\perp\!\!\!\perp)$$

Adequacy, computationally

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \rightarrow \rho \in |\Gamma| \rightarrow t[\rho] \in |A|$$

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \rightarrow \mathcal{J}(|\Gamma|) \rightarrow \mathcal{J}(|A|)$$

$$\texttt{rea}\,(t^{A\rightarrow B}\ u^{A})\,\bar{\rho}^{|\Gamma|} \triangleq \qquad \lambda\bar{\pi} \quad ^{\|B\|_V}.\ ? : \mathcal{J}(|A \rightarrow B|) \quad (? : \mathcal{J}(\|A \rightarrow B\|_V))$$

$$\mathcal{J}(|B|) = \mathcal{J}(\|B\|_V) \rightarrow \mathcal{J}(\perp\!\!\!\perp)$$

Adequacy, computationally

$$\mathtt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\} \ \rightarrow \rho \in |\Gamma| \rightarrow t[\rho] \in |A|$$

$$\mathtt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\} \ \rightarrow \mathcal{J}(|\Gamma|) \rightarrow \mathcal{J}(|A|)$$

$$\mathtt{rea}\,(t^{A\rightarrow B}\ u^{A})\,\bar{\rho}^{|\Gamma|} \ \triangleq \qquad \lambda\bar{\pi} \quad ^{\|B\|_V}.\ ?:\mathcal{J}(|A\rightarrow B|) \ \ (?:\mathcal{J}(\|A\rightarrow B\|_V))$$

$$\mathcal{J}(|B|) = \mathcal{J}(\|B\|_V) \rightarrow \mathcal{J}(\perp\!\!\!\perp)$$

Adequacy, computationally

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \rho \in |\Gamma| \to t[\rho] \in |A|$$

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \mathcal{J}(|\Gamma|) \to \mathcal{J}(|A|)$$

$$\texttt{rea}\,(t^{A\to B}\ u^{A})\ \bar{\rho}^{|\Gamma|} \ \triangleq \qquad \lambda\bar{\pi} \quad {}^{\|B\|_V}.\,\texttt{rea}\ t\ \bar{\rho} \qquad\qquad (?:\mathcal{J}(\|A\to B\|_V))$$

$$\mathcal{J}(|B|) = \mathcal{J}(\|B\|_V) \to \mathcal{J}(\perp\!\!\!\perp)$$

Adequacy, computationally

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \rho \in |\Gamma| \to t[\rho] \in |A|$$

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \mathcal{J}(|\Gamma|) \to \mathcal{J}(|A|)$$

$$\texttt{rea}\,(t^{A\to B}\ u^{A})\ \bar{\rho}^{|\Gamma|} \triangleq \qquad \lambda\bar{\pi} \quad {}^{\|B\|_V}.\,\texttt{rea}\ t\ \bar{\rho} \qquad\qquad (? : \mathcal{J}(\|A \to B\|_V))$$

$$\mathcal{J}(|B|) = \mathcal{J}(\|B\|_V) \to \mathcal{J}(\perp\!\!\!\perp) \qquad \mathcal{J}(\|A \to B\|_V) = \mathcal{J}(|A|) \times \mathcal{J}(\|B\|_V)$$

Adequacy, computationally

$$\texttt{rea} : \forall \{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \rho \in |\Gamma| \to t[\rho] \in |A|$$

$$\texttt{rea} : \forall \{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \mathcal{J}(|\Gamma|) \to \mathcal{J}(|A|)$$

$$\texttt{rea}\,(t^{A \to B}\ u^{A})\,\bar{\rho}^{|\Gamma|} \triangleq \qquad \lambda\bar{\pi} \quad ^{\|B\|_V}.\,\texttt{rea}\ t\ \bar{\rho} \qquad\qquad (\texttt{rea}\ u\ \bar{\rho}, \bar{\pi})$$

$$\mathcal{J}(|B|) = \mathcal{J}(\|B\|_V) \to \mathcal{J}(\perp\!\!\!\perp) \qquad \mathcal{J}(\|A \to B\|_V) = \mathcal{J}(|A|) \times \mathcal{J}(\|B\|_V)$$

Adequacy, computationally

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \rho \in |\Gamma| \to t[\rho] \in |A|$$

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \mathcal{J}(|\Gamma|) \to \mathcal{J}(|A|)$$

$$\texttt{rea}\,(t^{A\to B}\ u^{A})\,\bar{\rho}^{|\Gamma|} \triangleq \qquad \lambda\bar{\pi} \quad ^{\|B\|_V}.\,\texttt{rea}\ t\ \bar{\rho} \qquad\qquad (\texttt{rea}\ u\ \bar{\rho}, \bar{\pi})$$

(now let's un-simplify things)

Adequacy, computationally

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \rho \in |\Gamma| \to t[\rho] \in |A|$$

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \mathcal{J}(|\Gamma|) \to \mathcal{J}(|A|)$$

$$\texttt{rea}\,(t^{A\to B}\ u^{A})\,\bar{\rho}^{|\Gamma|} \triangleq \qquad \lambda\bar{\pi} \quad ^{\|B\|_V}.\,\texttt{rea}\ t\ \bar{\rho} \qquad\qquad (\texttt{rea}\ u\ \bar{\rho}, \bar{\pi})$$

$$t \in \|B\|_V^{\perp} \triangleq \forall\{t : \mathbb{T}\}.\, t \in |A| \to \langle\, t \mid e \,\rangle \in \perp\!\!\!\perp$$

Adequacy, computationally

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \rho \in |\Gamma| \to t[\rho] \in |A|$$

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \mathcal{J}(|\Gamma|) \to \mathcal{J}(|A|)$$

$$\texttt{rea}\,(t^{A \to B}\ u^{A})\,\bar{\rho}^{|\Gamma|} \triangleq \qquad \lambda\bar{\pi} \quad {}^{\|B\|_V}.\,\texttt{rea}\ t\ \bar{\rho} \qquad\qquad (\texttt{rea}\ u\ \bar{\rho}, \bar{\pi})$$

$$t \in \|B\|_V^{\perp} \triangleq \forall\{t : \mathbb{T}\}.\, t \in |A| \to \langle\, t \mid e\,\rangle \in \perp\!\!\!\perp$$

Adequacy, computationally

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \rho \in |\Gamma| \to t[\rho] \in |A|$$

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \mathcal{J}(|\Gamma|) \to \mathcal{J}(|A|)$$

$$\texttt{rea}\,(t^{A\to B}\ u^{A})\,\bar{\rho}^{|\Gamma|} \triangleq \lambda\{\pi\}\lambda\bar{\pi}^{\pi\in\|B\|_V}.\,\texttt{rea}\ t\ \bar{\rho} \qquad\qquad (\texttt{rea}\ u\ \bar{\rho}, \bar{\pi})$$

$$t \in \|B\|_V^{\perp} \triangleq \forall\{t : \mathbb{T}\}.\, t \in |A| \to \langle\, t \,|\, e\,\rangle \in \perp\!\!\!\perp$$

Adequacy, computationally

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \rightarrow \rho \in |\Gamma| \rightarrow t[\rho] \in |A|$$

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \rightarrow \mathcal{J}(|\Gamma|) \rightarrow \mathcal{J}(|A|)$$

$$\texttt{rea}\,(t^{A\rightarrow B}\ u^{A})\,\bar{\rho}^{|\Gamma|}\ \triangleq\ \lambda\{\pi\}\lambda\bar{\pi}^{\pi\in\|B\|_V}.\,\texttt{rea}\ t\ \bar{\rho} \qquad\qquad (\texttt{rea}\ u\ \bar{\rho}, \bar{\pi})$$

$$t \in \|B\|_V^{\perp} \triangleq \forall\{t : \mathbb{T}\}.\, t \in |A| \rightarrow \langle\, t \mid e \,\rangle \in \perp\!\!\!\perp$$

Adequacy, computationally

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \rho \in |\Gamma| \to t[\rho] \in |A|$$

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \mathcal{J}(|\Gamma|) \to \mathcal{J}(|A|)$$

$$\texttt{rea}\,(t^{A\to B}\ u^{A})\,\bar{\rho}^{|\Gamma|} \triangleq \lambda\{\pi\}\lambda\bar{\pi}^{\pi\in\|B\|_V}.\,\texttt{rea}\ t\ \bar{\rho} \qquad (\texttt{rea}\ u\ \bar{\rho}, \bar{\pi})$$

$$\langle\, t\ u \,|\, \pi \,\rangle \in \perp\!\!\!\perp$$

$$t \in \|B\|_V^{\perp} \triangleq \forall\{t : \mathbb{T}\}.\, t \in |A| \to \langle\, t \,|\, e \,\rangle \in \perp\!\!\!\perp$$

Adequacy, computationally

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \rho \in |\Gamma| \to t[\rho] \in |A|$$

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \mathcal{J}(|\Gamma|) \to \mathcal{J}(|A|)$$

$$\texttt{rea}\,(t^{A \to B}\ u^{A})\,\bar{\rho}^{|\Gamma|}\ \triangleq\ \lambda\{\pi\}\lambda\bar{\pi}^{\pi \in \|B\|_V}.\,\texttt{rea}\ t\ \bar{\rho} \qquad (\texttt{rea}\ u\ \bar{\rho}, \bar{\pi})$$

$$\langle\, t\ u \,|\, \pi \,\rangle \in \perp\!\!\!\perp \qquad \langle\, t \,|\, u \cdot \pi \,\rangle \in \perp\!\!\!\perp$$

$$t \in \|B\|_V^{\perp} \triangleq \forall\{t : \mathbb{T}\}.\, t \in |A| \to \langle\, t \,|\, e \,\rangle \in \perp\!\!\!\perp$$

Adequacy, computationally

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \rho \in |\Gamma| \to t[\rho] \in |A|$$

$$\texttt{rea} : \forall\{\Gamma\}\ t\ \{A\}\ \{\rho\}.\ \{\Gamma \vdash t : A\}\ \to \mathcal{J}(|\Gamma|) \to \mathcal{J}(|A|)$$

$$\texttt{rea}\,(t^{A \to B}\ u^{A})\,\bar{\rho}^{|\Gamma|} \triangleq \lambda\{\pi\}\lambda\bar{\pi}^{\pi \in \|B\|_V}.\,\texttt{rea}\ t\ \bar{\rho} \qquad (\texttt{rea}\ u\ \bar{\rho}, \bar{\pi})$$

$$\langle\, t\ u \,|\, \pi \,\rangle \in \perp\!\!\!\perp \qquad \rightsquigarrow \qquad \langle\, t \,|\, u \cdot \pi \,\rangle \in \perp\!\!\!\perp$$

(Slightly) more in the paper

We can change the definition of truth and value witnesses. For example:

(old) $\|A \to B\|_V \triangleq |A| \times \|B\|_V$ (new) $\|A \to B\|_V \triangleq |A|_V \times \|B\|_V$

$$|A \times B|_V \triangleq |A| \times |B| \qquad |A \times B|_V \triangleq |A|_V \times |B|_V$$

(Slightly) more in the paper

We can change the definition of truth and value witnesses. For example:

(old) $\|A \to B\|_V \triangleq |A| \times \|B\|_V$ (new) $\|A \to B\|_V \triangleq |A|_V \times \|B\|_V$

$|A \times B|_V \triangleq |A| \times |B|$ $|A \times B|_V \triangleq |A|_V \times |B|_V$

(Slightly) more in the paper

We can change the definition of truth and value witnesses. For example:

$$\text{(old)} \quad \|A \to B\|_V \triangleq |A| \times \|B\|_V \qquad \text{(new)} \quad \|A \to B\|_V \triangleq |A|_V \times \|B\|_V$$

$$|A \times B|_V \triangleq |A| \times |B| \qquad\qquad |A \times B|_V \triangleq |A|_V \times |B|_V$$

It gives us different evaluation strategies: (new) call-by-value arrow.
They are forced by the *typing obligations* of the dependent version.

(Slightly) more in the paper

We can change the definition of truth and value witnesses. For example:

(old) $\|A \to B\|_V \triangleq |A| \times \|B\|_V$ (new) $\|A \to B\|_V \triangleq |A|_V \times \|B\|_V$

$|A \times B|_V \triangleq |A| \times |B|$ $|A \times B|_V \triangleq |A|_V \times |B|_V$

It gives us different evaluation strategies: (new) call-by-value arrow.
They are forced by the *typing obligations* of the dependent version.

When we have both positive and negative types, some definitions are by case-distinction on the polarity.
Hints of a *polarized* evaluation order.

CBN version

$$
\begin{array}{lcl}
\langle \_ \mid \_ \rangle_A & : & \mathcal{J}(|A|) \to \mathcal{J}(\|A\|) \to \mathcal{J}(\perp\!\!\!\perp) \\
\langle \bar{t} \mid \bar{e} \rangle_P & \triangleq & \bar{t}\ \bar{e} \\
\langle \bar{t} \mid \bar{e} \rangle_N & \triangleq & \bar{e}\ \bar{t}
\end{array}
$$

$$
\begin{array}{llcl}
\texttt{rea}\ \ x^A & \bar{\rho} & \triangleq & \bar{\rho}(x) \\
\texttt{rea}\ \ (\lambda x^A.\, t^B) & \bar{\rho} & \triangleq & \lambda(\bar{u}^{|A|}, \bar{e}^{\|B\|}).\, \langle\, \texttt{rea}\ t\ \bar{\rho}[x \mapsto \bar{u}] \mid \bar{e}\,\rangle_B \\
\texttt{rea}\ \ (t^{A\to B}\ u^A) & \bar{\rho} & \triangleq & \lambda\bar{\pi}^{\|B\|_V}.\, \texttt{rea}\ t\ \bar{\rho}\ \left(\texttt{rea}\ u\ \bar{\rho}, \bar{\pi}^{\perp\perp}\right) \\
\texttt{rea}\ \ \left(t^A, u^B\right) & \bar{\rho} & \triangleq & (\texttt{rea}\ t\ \bar{\rho}, \texttt{rea}\ u\ \bar{\rho})^{\perp\perp}
\end{array}
$$

$$
\texttt{rea}\,(\texttt{let}\ (x, y) = t^{A\times B}\ \texttt{in}\ u^C)\ \bar{\rho}\ \triangleq
$$

$$
\lambda\bar{\pi}^{\|C\|_V}.\, \langle\, \texttt{rea}\ t\ \bar{\rho} \mid \lambda(\bar{x}, \bar{y}).\ \texttt{rea}\ u\ \bar{\rho}[x \mapsto \bar{x}, y \mapsto \bar{y}]\ \bar{\pi}\,\rangle_{A\times B}
$$

CBV version

$$\begin{array}{lcll}
\texttt{rea} \;\; x^A & \bar\rho & \triangleq & \bar\rho(x)^{\perp\perp} \\
\texttt{rea} \;\; (\lambda x^A.\, t^B) & \bar\rho & \triangleq & \lambda(\bar v^{|A|_V}, \bar e^{\|B\|}).\, \langle\, \texttt{rea}\ t\ \bar\rho[x \mapsto \bar v] \mid \bar e\,\rangle_B \\
\texttt{rea} \;\; (t^{A\to B}\ u^A) & \bar\rho & \triangleq & \lambda\bar\pi^{\|B\|_V}.\left\langle\, \texttt{rea}\ u\ \bar\rho \,\middle|\, \lambda \bar v_u^{|A|_V}.\, \texttt{rea}\ t\ \bar\rho\ \left(\bar v_u, \bar\pi^{\perp\perp}\right)\,\right\rangle_A
\end{array}$$

$$\texttt{rea}\ \left(t^A, u^B\right)\ \bar\rho\ \triangleq$$

$$\lambda\bar\pi^{\|A\times B\|}.\left\langle\, \texttt{rea}\ t\ \bar\rho \,\middle|\, \lambda\bar v_t^{|A|_V}.\left\langle\, \texttt{rea}\ u\ \bar\rho \,\middle|\, \lambda\bar v_u^{|B|_V}.\, \bar\pi\ (\bar v_t, \bar v_u)\,\right\rangle_B\right\rangle_A$$

$$\texttt{rea}\,(\texttt{let}\ (x,y) = t^{A\times B}\ \texttt{in}\ u^C)\ \bar\rho\ \triangleq$$

$$\lambda\bar\pi^{\|C\|_V}.\,\langle\, \texttt{rea}\ t\ \bar\rho \mid \lambda(\bar x, \bar y).\ \texttt{rea}\ u\ \bar\rho[x \mapsto \bar x, y \mapsto \bar y]\ \bar\pi\,\rangle_{A\times B}$$

Extraction

(Years) after writing all this on paper, we implemented it in Coq – mechanized type-checking.

We hoped that extraction would return the "simplified" code back.

$$m \in \perp\!\!\!\perp \triangleq \{m_n \in \mathbb{M}_N \mid m \leadsto m_1 \leadsto \ldots \leadsto m_n\}$$

Extraction

(Years) after writing all this on paper, we implemented it in Coq – mechanized type-checking.
We hoped that extraction would return the "simplified" code back.

$$m \in \perp\!\!\!\perp \triangleq \{m_n \in \mathbb{M}_N \mid m \rightsquigarrow m_1 \rightsquigarrow \ldots \rightsquigarrow m_n\}$$

```
Record FamR (A : Type) : Type :=
  In { J: Type ;
       R: A → J → Prop }.
Definition belong {A} : FamR A → A → Type :=
  fun T t ⇒ { t0 : J(T) | R(T) t t0 }.
Definition pole : FamR machine :=
  In machine
    (fun m m' ⇒ Util.many red m m' ∧ ¬(exists m'', red m' m'')).
Definition orthT (P : FamR term): FamR stack :=
  In (forall t: term, belong t P → J(pole))
     (fun e k ⇒ forall t t_P, R(pole) (t , e) (k t t_P)).
```

Related work: NbE

Hugo Herbelin (informally) explains that realizability and normalization-by-evaluation (NbE) are two sides of the same coin.

$$(\mathit{rea}) \quad \vdash t : A \rightarrow t \in |A|$$

$$(\mathit{NbE}) \quad (\vdash t : A \rightarrow \ \Vdash A) \ \wedge \ (\ \Vdash A \rightarrow \{v \ \mathrm{NF} \mid \ \vdash v : A\})$$

The computational aspect of NbE was already obvious – duh!

The end.

Thanks!

Any questions?

Auxiliary definitions

$$\begin{array}{lcl} \_^{\perp\perp} & : & \mathcal{J}(|P|_V) \to \mathcal{J}(|P|) \\ (\bar{v}^{|P|_V})^{\perp\perp} & \triangleq & \lambda \bar{e}^{\|P\|}.\, \bar{e}\ \bar{v} \end{array}$$

$$\begin{array}{lcl} \_^{\perp\perp} & : & \mathcal{J}(\|N\|_V) \to \mathcal{J}(\|N\|_V) \\ (\bar{\pi}^{\|N\|_V})^{\perp\perp} & \triangleq & \lambda \bar{t}^{|N|}.\, \bar{t}\ \bar{\pi} \end{array}$$

$$\begin{array}{lcl} \_^{\perp\perp} & : & \mathcal{J}(|A|_V) \to \mathcal{J}(|A|) \\ (\bar{v}^{|P|_V})^{\perp\perp} & \triangleq & \bar{v}^{\perp\perp} \\ (\bar{t}^{|N|})^{\perp\perp} & \triangleq & \bar{t} \end{array}$$

$$\begin{array}{lcl} \_^{\perp\perp} & : & \mathcal{J}(\|A\|_V) \to \mathcal{J}(\|A\|) \\ (\bar{e}^{\|P\|_V})^{\perp\perp} & \triangleq & \bar{e} \\ (\bar{\pi}^{\|N\|_V})^{\perp\perp} & \triangleq & \bar{\pi}^{\perp\perp} \end{array}$$