Semantic Analysis of Normalization by Evaluation for Fitch-Style Modal Lambda Calculi

Nachiappan Valliappan[1], *Fabian Ruch*, *Carlos Tomé Cortiñas*[1]

[1] *Chalmers University of Technology*

Modal logic IK

$$\frac{\cdot \vdash A}{\Gamma \vdash \Box A}\ \textsc{Necessitation}$$

$$\frac{}{\Gamma \vdash \Box(A \to B) \to \Box A \to \Box B}\ \textsc{Axiom K}$$

Fitch-style lambda calculus for IK (λ_{IK}) [Borghuis 1994]

$$\Gamma ::= \cdot \mid \Gamma, x : A \mid \Gamma, \text{🔒}$$

$$\frac{}{\Gamma, x : A, \Gamma' \vdash x : A}\ \text{🔒} \notin \Gamma' \qquad \frac{\Gamma, \text{🔒} \vdash t : A}{\Gamma \vdash \mathbf{box}\ t : \Box A} \qquad \frac{\Gamma \vdash t : \Box A}{\Gamma, \text{🔒}, \Gamma' \vdash \mathbf{unbox}\ t : A}\ \text{🔒} \notin \Gamma'$$

$$A \nvdash \Box A \qquad \Box(A \times B) \vdash \Box A$$

$$\Box A \nvdash A \qquad \Box A, \Box B \vdash \Box(A \times B)$$

Applications of NbE for modal lambda calculi

Interpretations of $\Box A$:

Staging: Code of type A

Security: Sensitive values of type A

Purity: Pure values of type A

NbE can be used to prove:

- Domain-specific theorems, e.g., noninterference
- Completeness theorems, e.g., completeness of possible-worlds semantics

Normalization by Evaluation

$$
\begin{aligned}
(\!|\ \_\ |\!) &: \Gamma \vdash A \to [\![\Gamma]\!] \dot{\to} [\![A]\!] \\
\downarrow^{A} &: [\![A]\!] \dot{\to} \mathrm{Nf}\ A \\
\uparrow^{A} &: \mathrm{Ne}\ A \dot{\to} [\![A]\!]
\end{aligned}
$$

$$
\begin{aligned}
&norm\ :\ \Gamma \vdash A \to\ \mathrm{Nf}_{\Gamma}\ A \\
&norm\ t = \downarrow^{A} ((\!|\ t\ |\!)\ \gamma_{\mathrm{id}})
\end{aligned}
$$

NbE model for λ_{IK}

$\llparenthesis\ \_\ \rrparenthesis\colon\ \mathrm{STLC} \rightsquigarrow \mathrm{CCC}\ \mathcal{C}$

$W\colon$ Category of contexts and OPEs

$\widehat{W}$ as NbE model for STLC

$\llparenthesis\ \_\ \rrparenthesis\colon\ \lambda_{\mathrm{IK}} \rightsquigarrow \mathrm{CCC}_{\text{🔒} \dashv \Box}\ \mathcal{C}$ [Clouston 2018]

$W_{\text{🔒}}\colon$ Akin to W, morphisms preserve locks

$\widehat{W_{\text{🔒}}}$ as NbE model for λ_{IK}

Adjoint functors Lock ⊣ Box

$$[\![\Box A]\!]_\Gamma = \mathrm{Box}_\Gamma\ [\![A]\!] \qquad [\![\Delta, \text{🔒}]\!]_\Gamma = \mathrm{Lock}_\Gamma\ [\![\Delta]\!]$$

$$\mathcal{A} : \widehat{W_{\text{🔒}}}$$

$$\frac{x : \mathcal{A}_{\Gamma,\text{🔒}}}{\mathsf{box}\ x : \mathrm{Box}_\Gamma\ \mathcal{A}} \qquad \frac{x : \mathcal{A}_\Gamma}{\mathsf{lock}\ x : \mathrm{Lock}_{\Gamma,\text{🔒},\Gamma'}\ \mathcal{A}}\ \text{🔒} \notin \Gamma'$$

Gives $(\!|\mathbf{box}|\!)$ and $(\!|\mathbf{unbox}|\!)$, and $\downarrow^{\Box A}$ and $\uparrow^{\Box A}$

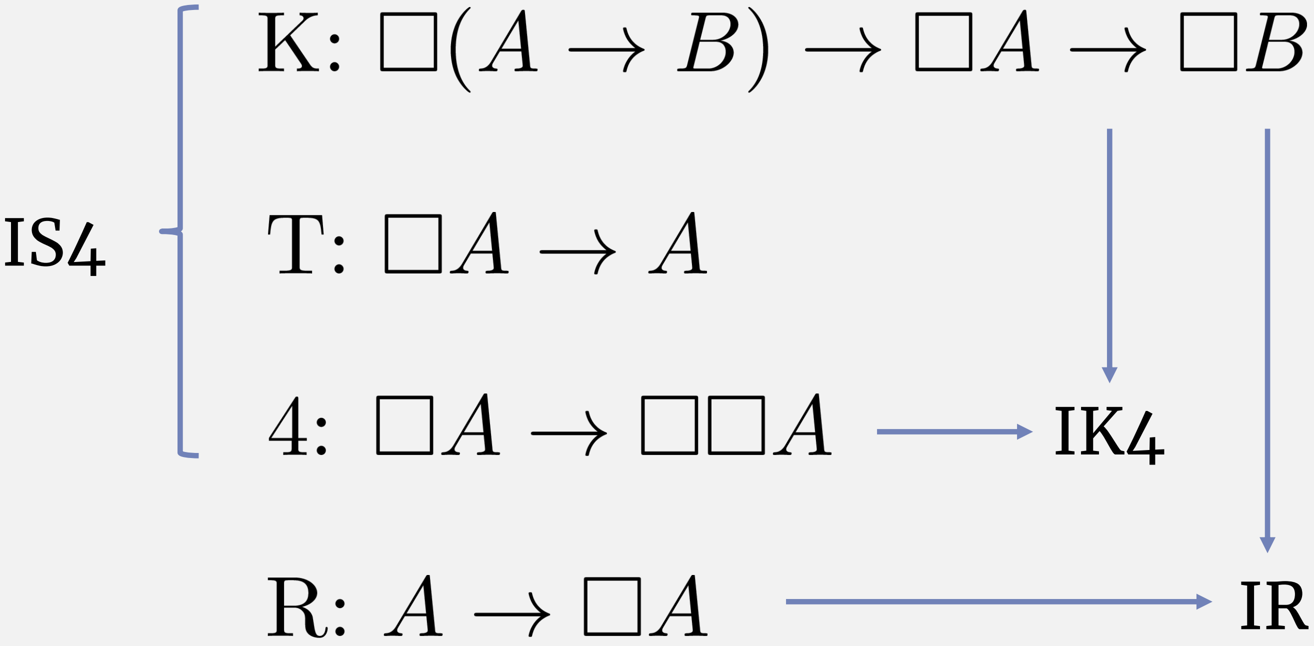
NbE as an instance of possible-worlds semantics

Semantics for λ_{IK} parameterized by a *frame* $(\mathcal{W}, \leq, R)$

(subject to conditions on $\leq$ and R)

$$\left.\begin{array}{l}\text{Pick objects of } W_{\text{🔒}} \text{ for } \mathcal{W}\\ \text{Pick morphisms of } W_{\text{🔒}} \text{ for } \leq\\ \Gamma \; R \; \Delta \text{ iff } \exists \Gamma'.\ \Delta = \Gamma, \text{🔒}, \Gamma' \text{ s.t. } \text{🔒} \notin \Gamma'\end{array}\right\} \quad \begin{array}{l}\text{yields the NbE}\\ \text{model for } \lambda_{\text{IK}}\end{array}$$

Next steps: Axioms beyond K



IS4

K: $\Box(A \to B) \to \Box A \to \Box B$

T: $\Box A \to A$

4: $\Box A \to \Box\Box A$

IK4

R: $A \to \Box A$

IR

Agda mechanization: github.com/nachivpn/k

EOM