Normalization for Fitch-Style Modal Calculi

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

[1] Chalmers University of Technology

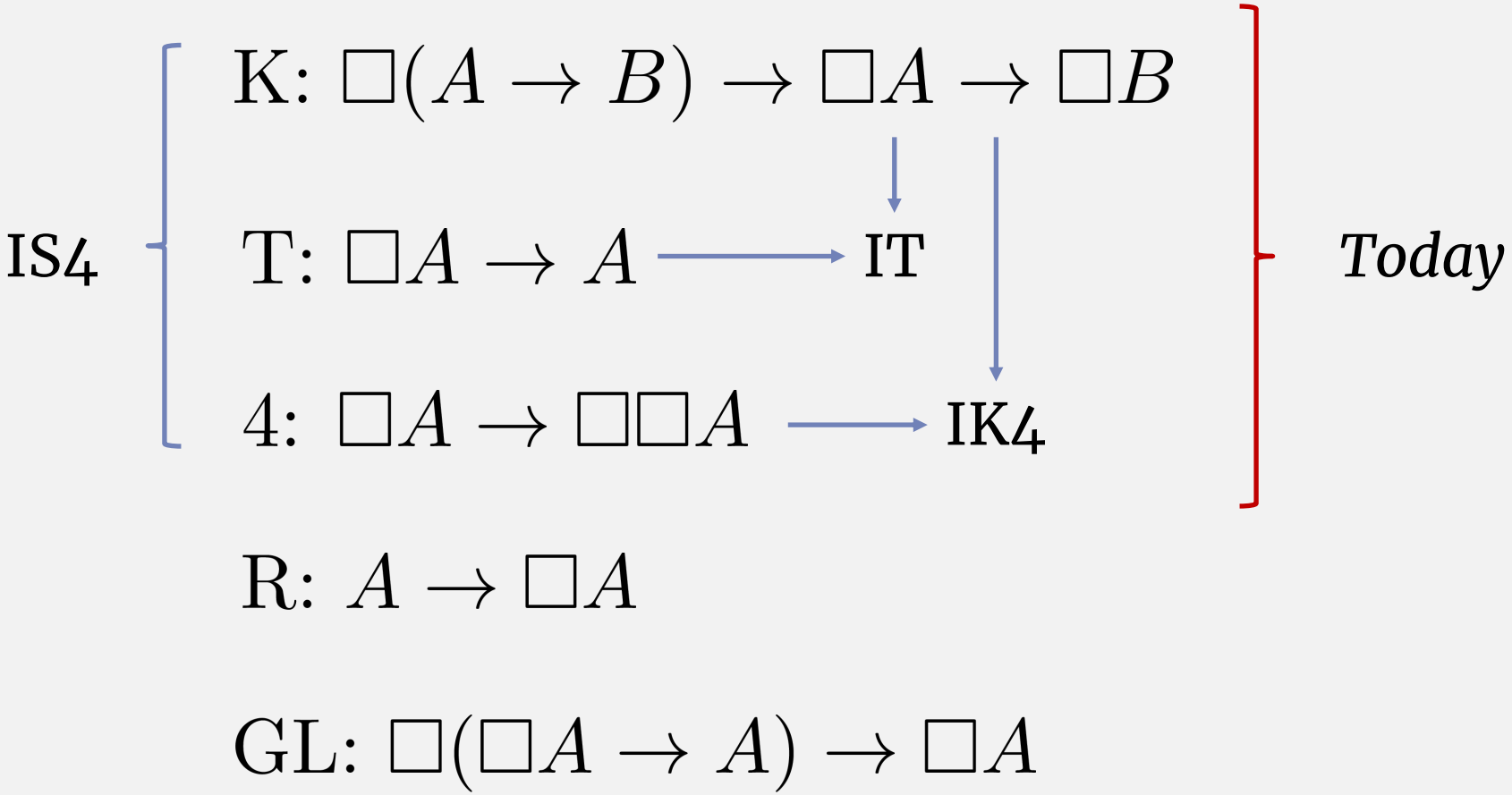
SPLS Glasgow, July 1, 2022

Modal Logic Intuitionistic K (IK)

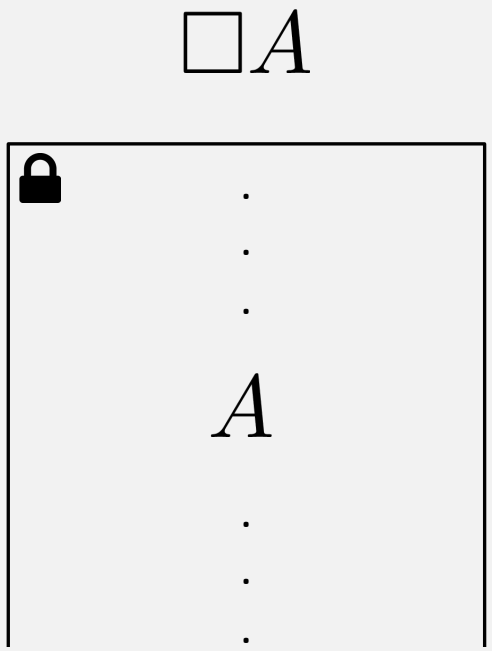
$$\frac{\cdot \vdash A}{\Gamma \vdash \Box A}\ \textsc{Necessitation}$$

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

Axioms Beyond K



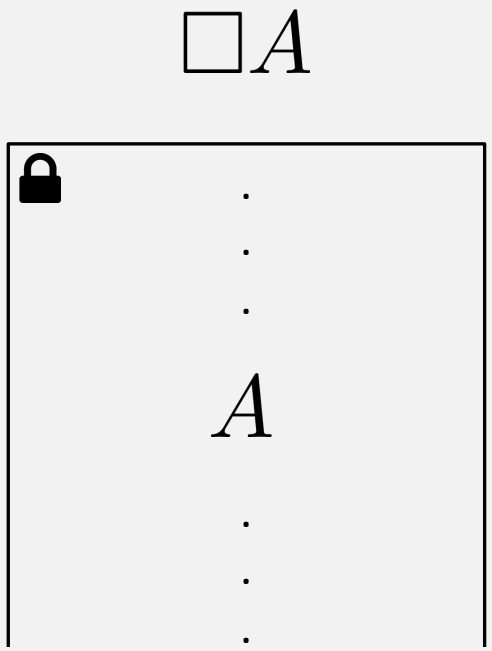
From Fitch-Style Natural Deduction to a λ-calculus



K-import

$$\frac{\Gamma \vdash t : \Box A}{\Gamma, 🔒 \vdash \mathbf{unbox}\ t : A}$$

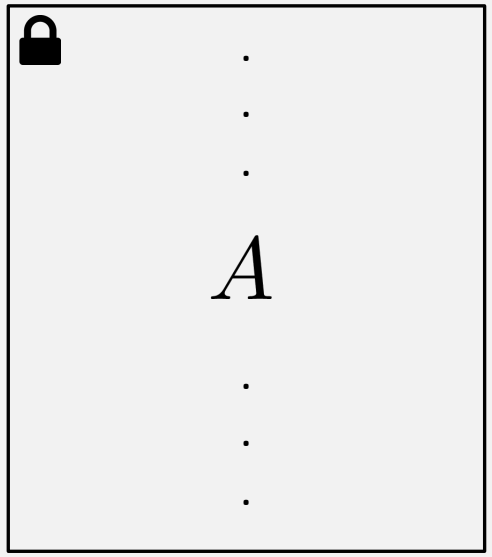
From Fitch-Style Natural Deduction to a λ-calculus



K-import

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

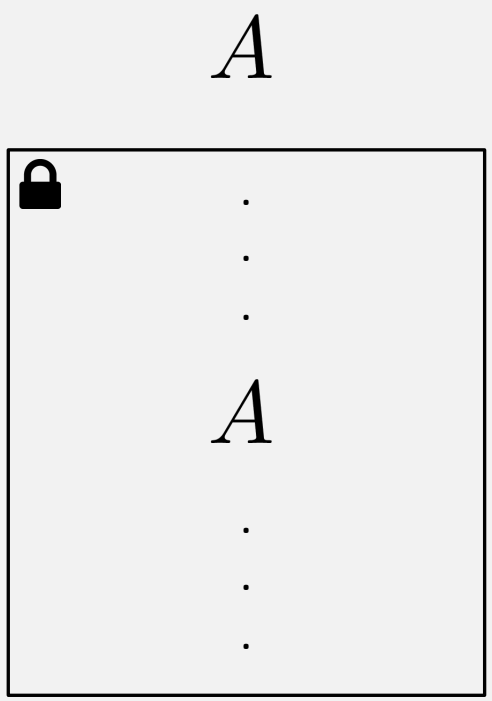
From Fitch-Style Natural Deduction to a λ-calculus



$\Box A$ K-export

$$\frac{\Gamma, \text{🔒} \vdash t : A}{\Gamma \vdash \mathbf{box}\ t : \Box A}$$

From Fitch-Style Natural Deduction to a λ-calculus



Copy

$$\frac{}{\Gamma, x : A, \Gamma' \vdash x : A} \; \lock \notin \Gamma'$$

Fitch-Style Lambda Calculus for IK (λ_{IK}) [Borghuis 1994]

$$\Gamma ::= \cdot \mid \Gamma, x : A \mid \Gamma, 🔒$$

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

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

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

Normalization Rules

$$(\beta) \quad \mathbf{unbox}\ (\mathbf{box}\ t) \longrightarrow t$$

$$(\eta) \quad \Gamma \vdash t \longrightarrow \mathbf{box}\ (\mathbf{unbox}\ t) : \Box A$$

Normalization by Rewriting?

η rules complicate the reduction relation

Each system demands different syntactic lemmas

$$\lambda_{\mathrm{IK}}\ \frac{\Gamma \vdash t : \Box A}{\Gamma, \blacksquare, \Gamma' \vdash \mathbf{unbox}\ t : A}\ \blacksquare \notin \Gamma' \qquad \lambda_{\mathrm{IK4}}\ \frac{\Gamma \vdash t : \Box A}{\Gamma, \blacksquare, \Gamma' \vdash \mathbf{unbox}\ t : A}$$

$$\lambda_{\mathrm{IT}}\ \frac{\Gamma \vdash t : \Box A}{\Gamma, \Gamma' \vdash \mathbf{unbox}\ t : A}\ \#_{\blacksquare}(\Gamma') \leq 1 \qquad \lambda_{\mathrm{IS4}}\ \frac{\Gamma \vdash t : \Box A}{\Gamma, \Gamma' \vdash \mathbf{unbox}\ t : A}$$

Normalization by Evaluation

$$(\!| \_ |\!) \ : \Gamma \vdash A \Rightarrow [\![\Gamma]\!] \dot{\to} [\![A]\!]$$

$$\text{quote} : [\![\Gamma]\!] \dot{\to} [\![A]\!] \Rightarrow \Gamma \vdash_{\mathbf{NF}} A$$

$$\text{norm} \ : \ \Gamma \vdash A \Rightarrow \ \Gamma \vdash_{\mathbf{NF}} A$$

$$\text{norm}\ t = \ \text{quote}\ (\!|t|\!)$$

Models of Fitch-Style Modal Calculi

$$\text{What is } [\![\Gamma]\!] \dot{\to} [\![A]\!]?$$

The Story

- *Part 1*: Identify the possible-world semantics
- *Part 2*: Construct NbE models as instances

Possible-World Semantics for IPL

Model $\mathcal{M}$: $(\mathcal{F}, V)$

Frame $\mathcal{F}$: $(\mathcal{W}, R_i)$

R_i is a preorder that V respects

$$[\![\tau]\!]_w = V(w, \tau)$$

$$[\![A \to B]\!]_w = \forall w'.\ wR_iw' \Rightarrow [\![A]\!]_{w'} \Rightarrow [\![B]\!]_{w'}$$

Monotonicity: $wR_iw' \Rightarrow [\![A]\!]_w \Rightarrow [\![A]\!]_{w'}$

Possible-World Semantics for IK [Plotkin and Stirling 1986]

Model $\mathcal{M}$: $(\mathcal{F}, V)$

Frame $\mathcal{F}$: $(\mathcal{W}, R_i, R_m)$

R_i is $[\ldots]$

$$[\![\tau]\!]_w = V(w, \tau)$$
$$[\![A \to B]\!]_w = \forall w'.\ wR_iw' \Rightarrow [\![A]\!]_{w'} \Rightarrow [\![B]\!]_{w'}$$
$$[\![\Box A]\!]_w = \forall w'.\ wR_iw' \Rightarrow \forall v.\ w'R_mv \Rightarrow [\![A]\!]_v$$

Monotonicity: $wR_iw' \Rightarrow [\![A]\!]_w \Rightarrow [\![A]\!]_{w'}$

Possible-World Semantics for λ_{IK}

Model $\mathcal{M}$: $(\mathcal{F}, V)$

Frame $\mathcal{F}$: $(\mathcal{W}, R_i, R_m)$

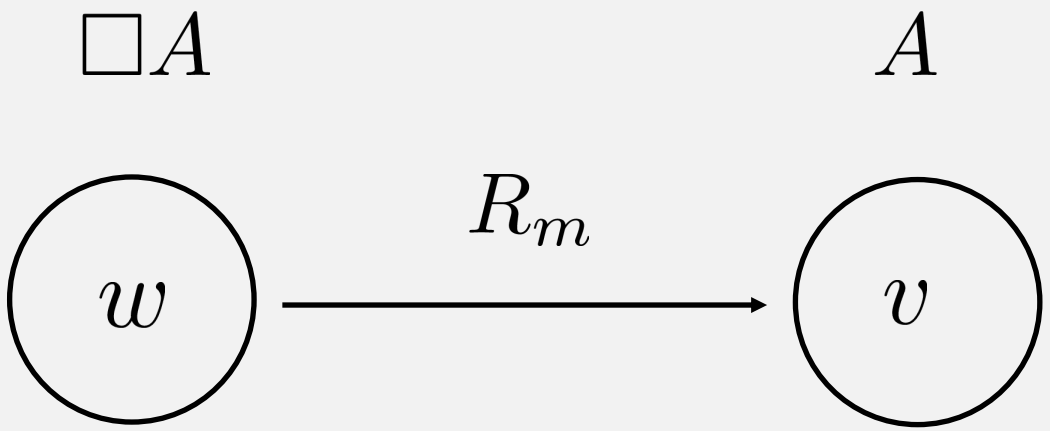
R_i is $[\ldots]$

$$[\![\cdot]\!]_w = \top$$

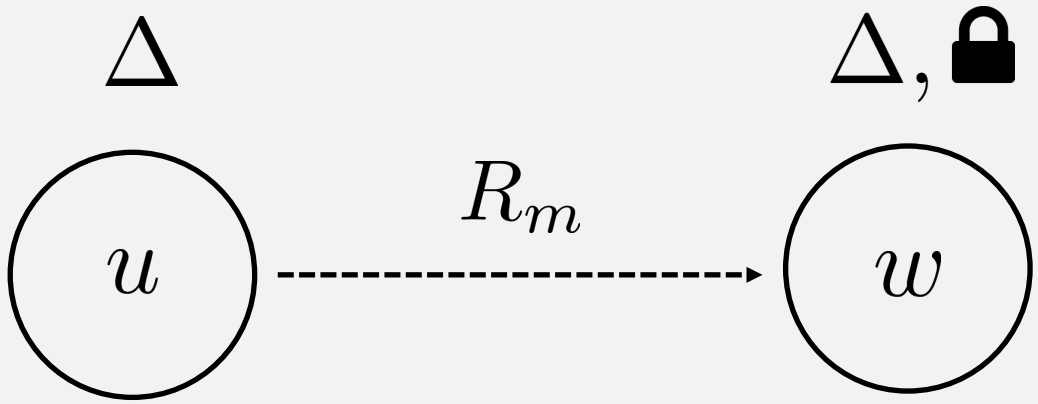
$$[\![\Delta, A]\!]_w = [\![\Delta]\!]_w \times [\![A]\!]_w$$

$$[\![\Delta, \blacksquare]\!]_w = ??$$

Box ~ Future



Lock ~ Past



Possible-World Semantics for λ_{IK}

Model $\mathcal{M}$: $(\mathcal{F}, V)$

Frame $\mathcal{F}$: $(\mathcal{W}, R_i, R_m)$

R_i is $[\ldots]$

$R_m; R_i \subseteq R_i; R_m$

$$[\![\cdot]\!]_w = \top$$

$$[\![\Delta, A]\!]_w = [\![\Delta]\!]_w \times [\![A]\!]_w$$

$$[\![\Delta, \blacksquare]\!]_w = \exists u.\ [\![\Delta]\!]_u \times u R_m w$$

Monotonicity: $w R_i w' \Rightarrow [\![\Delta]\!]_w \Rightarrow [\![\Delta]\!]_{w'}$

Possible-World Semantics for λ_{IK}

Model $\mathcal{M}$: $(\mathcal{F}, V)$

Frame $\mathcal{F}$: $(\mathcal{W}, R_i, R_m)$

R_i is a preorder that V respects

$R_m; R_i \subseteq R_i; R_m$

NbE Using Possible-World Semantics

$$(\!| \_ |\!) \ : \Gamma \vdash A \Rightarrow (\forall w.\ [\![\Gamma]\!]_w \Rightarrow [\![A]\!]_w)$$

$$\text{quote} : (\forall w.\ [\![\Gamma]\!]_w \Rightarrow [\![A]\!]_w) \Rightarrow \Gamma \vdash_{\mathrm{NF}} A$$

$$\text{norm} \ : \ \Gamma \vdash A \Rightarrow \ \Gamma \vdash_{\mathrm{NF}} A$$

$$\text{norm}\ t = \ \text{quote}\ (\!|t|\!)$$

Normal Forms

$$\frac{\Gamma, 🔒 \vdash_{\mathrm{NF}} t : A}{\Gamma \vdash_{\mathrm{NF}} \mathbf{box}\ t : \Box A}$$

$$\frac{\Gamma \vdash_{\mathrm{NE}} t : \Box A}{\Gamma, 🔒, \Gamma' \vdash_{\mathrm{NE}} \mathbf{unbox}\ t : A}\ 🔒 \notin \Gamma'$$

Constructing an NbE Model for STLC

Model $\mathcal{M}$: $(\mathcal{F}, V)$

Frame $\mathcal{F}$: $(\mathcal{W}, R_i)$

R_i is a preorder that V respects

$$\text{quote} : (\forall w.\ [\![\Gamma]\!]_w \Rightarrow [\![A]\!]_w) \Rightarrow \Gamma \vdash_{\text{NF}} A$$

[Coquand 1993]

$$\begin{cases} \mathcal{W} = \text{Contexts} \\ V(\Gamma, \tau) = \Gamma \vdash_{\text{NE}} \tau \\ R_i = \leq \text{ (Weaker)} \end{cases}$$

Constructing an NbE Model for λ_{IK}

Model $\mathcal{M}$: $(\mathcal{F}, V)$

Frame $\mathcal{F}$: $(\mathcal{W}, R_i, R_m)$

R_i is a preorder that V respects

$R_m ; R_i \subseteq R_i ; R_m$

quote : $(\forall w.\ [\![\Gamma]\!]_w \Rightarrow [\![A]\!]_w) \Rightarrow \Gamma \vdash_{\text{NF}} A$

$\mathcal{W} =$ Contexts

$V(\Gamma, \tau) = \Gamma \vdash_{\text{NE}} \tau$

$R_i = \leq$ (Weaker)

$R_m =$??

Key Observation From the Syntax of $\lambda_{\text{IK/IT/IK4/IS4}}$

$$\frac{\Gamma, \blacksquare \vdash t : A}{\Gamma \vdash \mathbf{box}\ t : \Box A}$$

$$\lambda_{\text{IK}}\ \frac{\Gamma \vdash t : \Box A}{\Gamma, \blacksquare, \Gamma' \vdash \mathbf{unbox}\ t : A}\ \blacksquare \notin \Gamma'$$

$$\lambda_{\text{IK4}}\ \frac{\Gamma \vdash t : \Box A}{\Gamma, \blacksquare, \Gamma' \vdash \mathbf{unbox}\ t : A}$$

$$\lambda_{\text{IT}}\ \frac{\Gamma \vdash t : \Box A}{\Gamma, \Gamma' \vdash \mathbf{unbox}\ t : A}\ \#_{\blacksquare}(\Gamma') \leq 1$$

$$\lambda_{\text{IS4}}\ \frac{\Gamma \vdash t : \Box A}{\Gamma, \Gamma' \vdash \mathbf{unbox}\ t : A}$$

Key Observation From the Syntax of $\lambda_{\text{IK/IT/IK4/IS4}}$

$$\frac{\forall \Gamma'.\ \Gamma R_m \Gamma' \Rightarrow \Gamma' \vdash t : A}{\Gamma \vdash \mathbf{box}\ t : \Box A} \qquad \frac{\exists \Gamma.\ \Gamma \vdash t : \Box A \times \Gamma R_m \Delta}{\Delta \vdash \mathbf{unbox}\ t : A}$$

$$\frac{\Gamma, 🔒 \vdash t : A}{\Gamma \vdash \mathbf{box}\ t : \Box A} \qquad \frac{\Gamma \vdash t : \Box A \qquad \Gamma R_m \Delta}{\Delta \vdash \mathbf{unbox}\ t : A}$$

Constructing an NbE Model for λ_{IK}

$$\lambda_{\text{IK}}\ \frac{\Gamma \vdash t : \Box A}{\Gamma, \color{red}{\underline{🔒}}, \Gamma' \vdash \mathbf{unbox}\ t : A}\ \color{red}{\underline{🔒 \notin \Gamma'}}$$

$$\Gamma R_m \Delta \triangleq \exists \Gamma'.\ \Delta = \Gamma, 🔒, \Gamma' \text{ s.t. } 🔒 \notin \Gamma'$$

Constructing an NbE Model for λ_{IT}

T: $\Box A \to A$

$$\lambda_{\mathrm{IT}}\ \frac{\Gamma \vdash t : \Box A}{\Gamma, \Gamma' \vdash \mathbf{unbox}\ t : A}\ \#_{\text{🔒}}(\Gamma') \leq 1$$

$$\Gamma R_m \Delta \triangleq \exists \Gamma'.\ \Delta = \Gamma, \Gamma' \text{ s.t. } \#_{\text{🔒}}(\Gamma') \leq 1$$

R_m is reflexive

Constructing an NbE Model for λ_{IK4}

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

$$\lambda_{\text{IK4}}\ \frac{\Gamma \vdash t : \Box A}{\Gamma, \color{red}{\blacksquare}, \Gamma' \vdash \mathbf{unbox}\ t : A}$$

$$\Gamma R_m \Delta \triangleq \exists \Gamma'.\ \Delta = \Gamma, \blacksquare, \Gamma'$$

R_m is transitive

Constructing an NbE Model for λ_{IS4}

T: $\Box A \to A$

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

$$\lambda_{\text{IS4}}\ \frac{\Gamma \vdash t : \Box A}{\Gamma, \Gamma' \vdash \mathbf{unbox}\ t : A}$$

$$\Gamma R_m \Delta \triangleq \exists \Gamma'.\ \Delta = \Gamma, \Gamma'$$

R_m is reflexive and transitive

Constructing an NbE Model for $\lambda_{\text{IK/IT/IK4/IS4}}$

$$\text{quote} : (\forall \Delta.\ [\![\Gamma]\!]_\Delta \Rightarrow [\![A]\!]_\Delta) \Rightarrow \Gamma \vdash_{\text{NF}} A$$

$$\text{using reify} : \forall \Gamma.\ [\![\Box A]\!]_\Gamma \Rightarrow \Gamma \vdash_{\text{NF}} \Box A$$

$$\text{Know } [\![\Box A]\!]_\Gamma = \forall \Gamma'.\ \Gamma R_i \Gamma' \Rightarrow \forall \Sigma.\ \Gamma' R_m\ \Sigma \Rightarrow [\![A]\!]_\Sigma$$

$$\text{Pick } \Gamma' \text{ as } \Gamma \text{ and } \Sigma \text{ as } \Gamma, 🔒 \text{ to get } [\![A]\!]_{\Gamma, 🔒}$$

$$\text{reify } [\![A]\!]_{\Gamma, 🔒} \text{ to get } n : \Gamma, 🔒 \vdash_{\text{NF}} A$$

$$\textbf{box}\ n : \Gamma \vdash_{\text{NF}} \Box A$$


Why?

Programming Language Applications

Interpretations of $\Box A$:

Language with capabilities for effects: Pure values of type A

Information-flow: Secret value of type A

Partial Evaluation: Dynamic value of type A

Normal forms can be used to prove:

- Capability safety
- Noninterference
- Binding-time correctness

Proving Capability Safety

Show: Any term $c : \mathrm{Cap} \vdash t : \Box(\mathrm{T}())$ does not print

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \mathrm{return}\ t : \mathrm{T}A} \qquad \frac{\Gamma \vdash c : \mathrm{Cap} \quad \Gamma \vdash s : \mathrm{String}}{\Gamma \vdash \mathrm{print}\ c\ s : \mathrm{T}()}$$

$$\frac{\Gamma \vdash t : \mathrm{T}A \quad \Gamma \vdash f : A \to \mathrm{T}B}{\Gamma \vdash t \gg\!= u : \mathrm{T}B}$$

Extend λ_{IS4} with a monad for printing

Proving Capability Safety

Show: Any term $c : \mathrm{Cap} \vdash t : \Box(\mathrm{T}())$ does not print

$$c : \mathrm{Cap} \vdash_{\mathrm{NF}} \mathbf{box}\ (m_1 \gg\!= m_2 \gg\!= \ldots \gg\!= (\mathrm{return}\ ()))$$

$$c : \mathrm{Cap}, \text{🔒} \vdash_{\mathrm{NF}} m_1 \gg\!= m_2 \gg\!= \ldots \gg\!= (\mathrm{return}\ ())$$

$$m_i = \mathrm{print}\ c\ s \text{ is impossible}$$

$$c : \mathrm{Cap}, \text{🔒} \vdash_{\mathrm{NF}} \mathrm{return}\ ()$$

$$c : \mathrm{Cap} \vdash_{\mathrm{NF}} \mathbf{box}\ (\mathrm{return}\ ())$$

Completeness, Decidability and Logical Applications

NbE can be used to prove:

- Deductive completness with possible-world semantics
- Completeness of equational theory with categorical models
- Decidability of equational theory
- Constructive proof of Denecessitation

In a Nutshell

Normalization for Fitch-style modal calculi can be achieved by constructing NbE models as instances of their possible-world semantics, thus avoiding tedious syntactic arguments based on reduction.

Paper and Mechanization: nachivpn.me/k

EOM