Normalization for Fitch-Style Modal Lambda Calculi

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

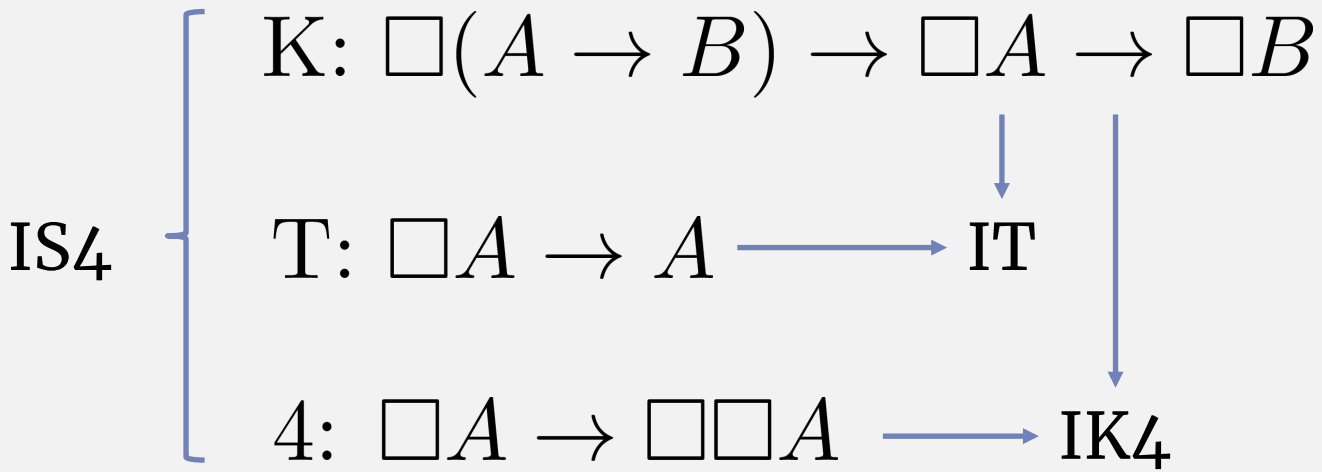
[1] Chalmers University of Technology

Modal Logic Intuitionistic K (IK)

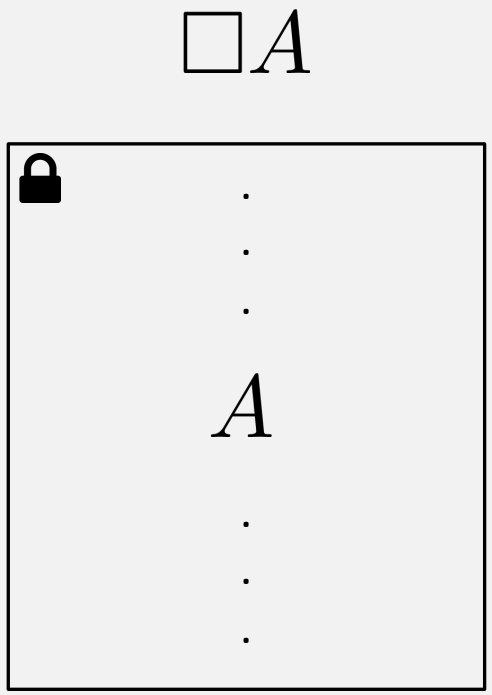
$$\frac{\cdot \vdash A}{\Gamma \vdash \Box A}\ \textsc{Necessitation}$$

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

Intuitionistic Logics With Axioms Beyond K



From Fitch-style Natural Deduction to a λ-calculus

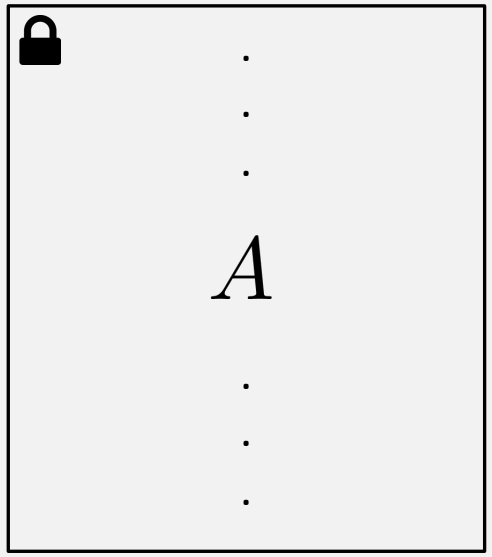


K-import

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

From Fitch-style Natural Deduction to a λ-calculus

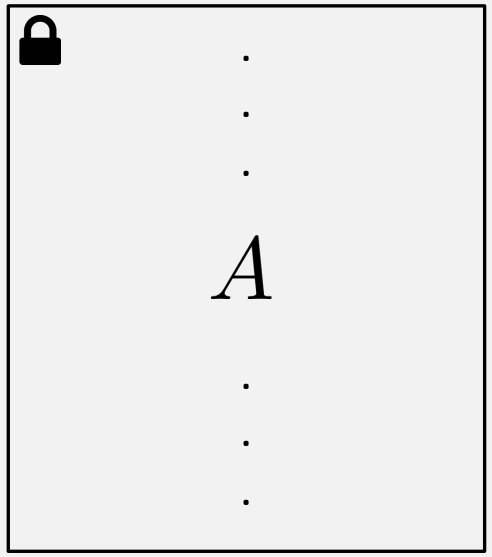
$\Box A$



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

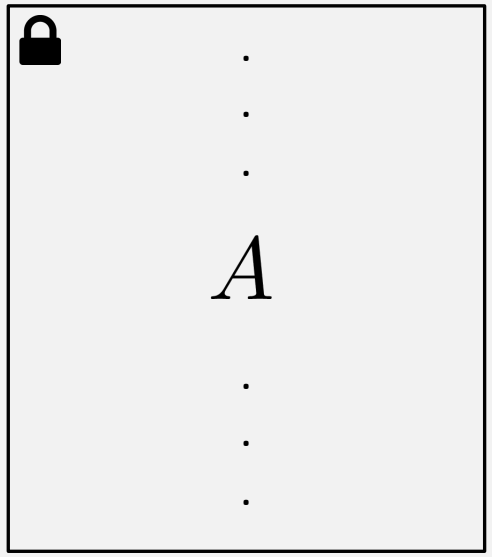


$\Box A$ K-export

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

From Fitch-style Natural Deduction to a λ-calculus

$k.$ A



Copy k

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

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?

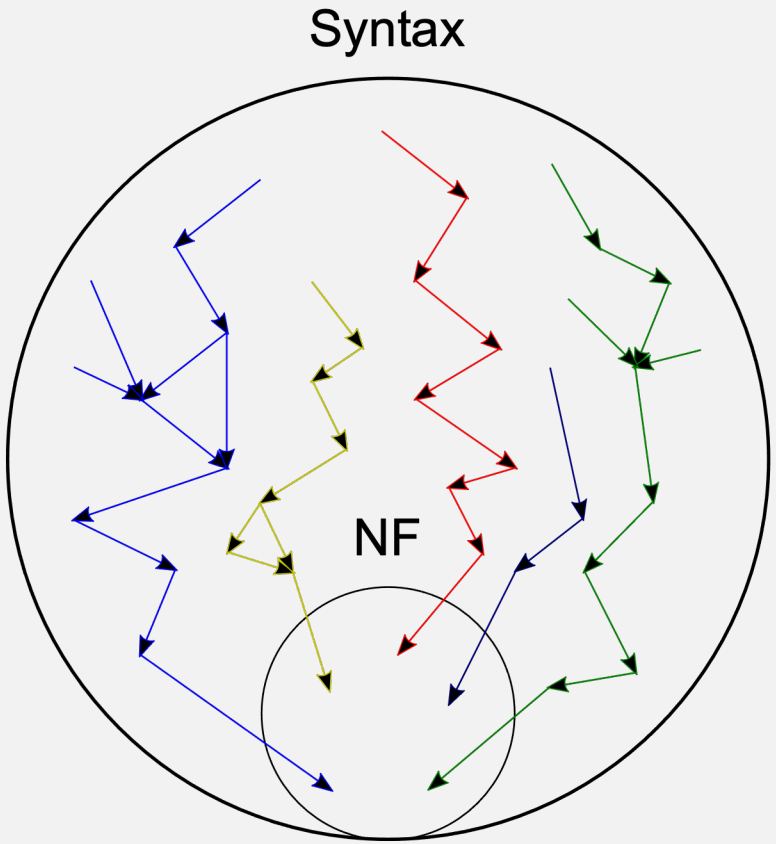


Image credit: Sam Lindley, University of Edinburgh

Normalization by Rewriting?

η rules complicate rewriting

Each system demands different syntactic lemmas

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

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

Normalization by Evaluation

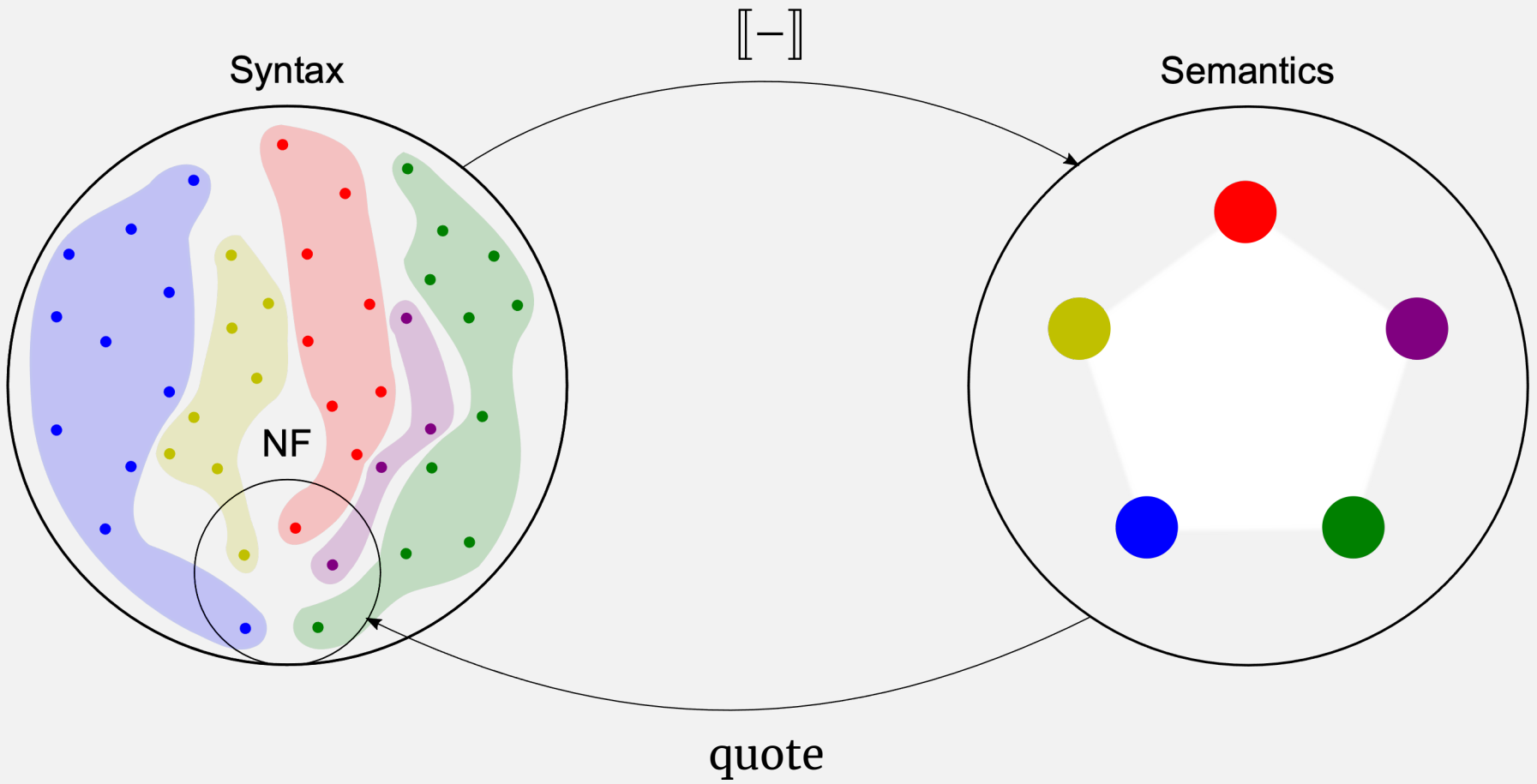


Image credit: Sam Lindley, University of Edinburgh

The Story

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

Possible Worlds Semantics for IK [Božić & Došen 1984]

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

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

R_i is a preorder

$R_i; R_m \subseteq R_m; R_i$

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

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

$$[\![\Box A]\!]_w = \forall w'.\ wR_mw' \Rightarrow [\![A]\!]_{w'}$$

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

Possible Worlds Semantics for λ_{IK}

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

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

R_i is a preorder

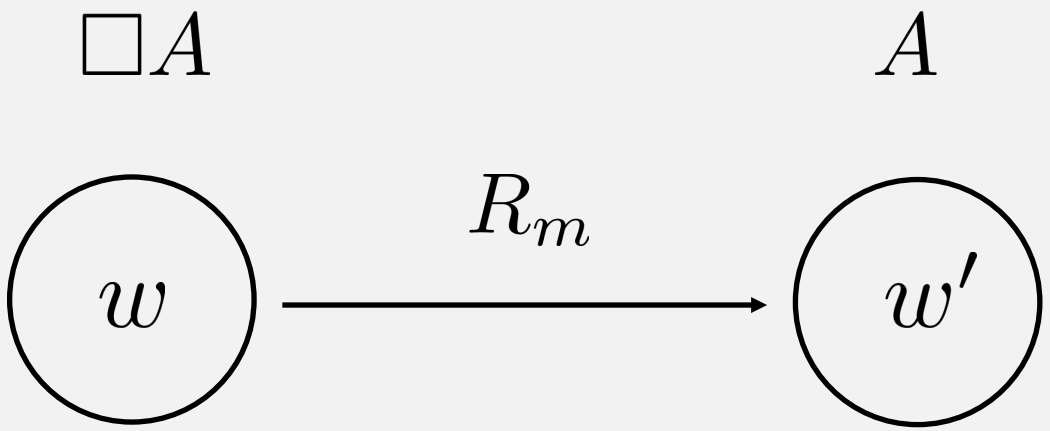
$R_i ; R_m \subseteq R_m ; R_i$

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

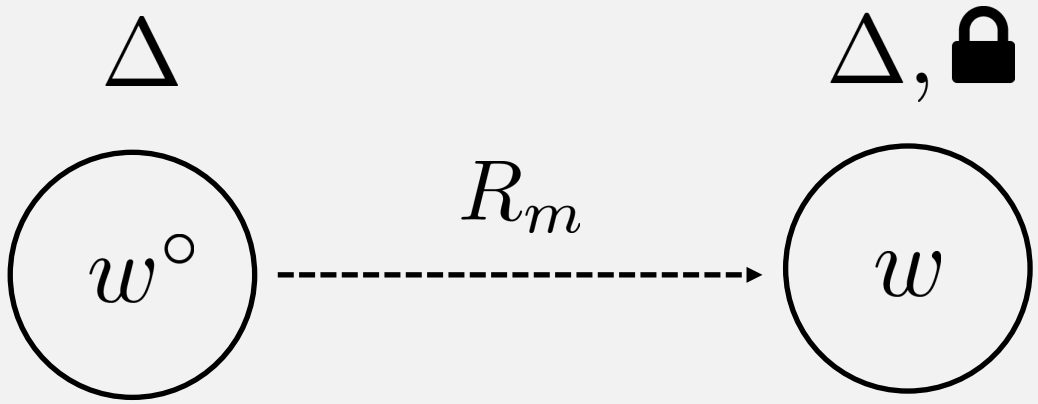
$$[\![\Delta, A]\!]_w = [\![\Delta]\!]_w \wedge [\![A]\!]_w$$

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

Box ~ Future



Lock ~ Past



Possible Worlds Semantics for λ_{IK}

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

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

R_i is a preorder

$R_i; R_m \subseteq R_m; R_i$

$R_m; R_i \subseteq R_i; R_m$

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

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

$$[\![\Delta, \blacksquare]\!]_w = \exists w^\circ.\ w^\circ R_m w \wedge [\![\Delta]\!]_{w^\circ}$$

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

Possible Worlds Semantics for λ_{IK}

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

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

R_i is a preorder

$R_i; R_m = R_m; R_i$

Normalization by Evaluation

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

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

$$\text{norm} \ : \ \Gamma \vdash A \to \ \Gamma \vdash_{\text{Nf}} A$$

$$\text{norm}\ t = \ \text{quote}\ [\![t]\!]$$

Normal Forms

$$\frac{\Gamma, 🔒 \vdash_{\mathrm{nf}} t : A}{\Gamma \vdash_{\mathrm{nf}} \mathbf{box}\ t : \Box A} \qquad \frac{\Gamma \vdash_{\mathrm{ne}} t : \Box A}{\Gamma, 🔒, \Gamma' \vdash_{\mathrm{ne}} \mathbf{unbox}\ t : A}\ 🔒 \notin \Gamma'$$

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

$R_i ; R_m = R_m ; R_i$

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

standard!

[Coquand 1993]

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

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

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

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

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

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

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

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

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

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 $\lambda_{\text{IK/IT/IK4/IS4}}$

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

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

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

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

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

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


Why?

Potential 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:

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

Necessitation is Admissible in λ_{IK}

$$\vdash A \implies \vdash \Box A$$

$$\dfrac{\dfrac{\vdash t : A}{\rule{2em}{0.4pt}\!\!\rule{2em}{0.4pt}}\ \text{by renaming}}{\dfrac{\boldsymbol{\color{black}\blacksquare} \vdash t : A}{\vdash \mathbf{box}\ t : \Box A}}$$

What About "Denecessitation"?

$$\vdash \Box A \implies \vdash A$$

How would you prove this?

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

Denecessitation Can be *Proved Using Normal Forms*

$$\vdash \Box A \implies \vdash A$$

$$\dfrac{\dfrac{\times}{\vdash_{\mathrm{ne}} t : \Box B}}{\lock \vdash_{\mathrm{ne}} \mathbf{unbox}\ t : B}$$

No neutrals in empty context, dismissed!

Only culprit that introduces 🔒

.
.

$$\dfrac{\lock \vdash_{\mathrm{nf}} t : A}{\vdash_{\mathrm{nf}} \mathbf{box}\ t : \Box A}$$

Remove 🔒 to get $\vdash_{\mathrm{nf}} t : \Box A$

In a Nutshell

Normalization can be achieved for Fitch-style modal lambda calculi by constructing NbE models as instances of their possible-world semantics, thus avoiding ad hoc syntactic approaches based on rewriting.

Agda mechanization: github.com/nachivpn/k

EOM