Normalization for Fitch-Style Modal Calculi

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

[1] Chalmers University of Technology

ICFP '22, Ljubljana

What is a Modality?

$$\Box : \mathrm{Type} \to \mathrm{Type}$$

The Necessity Modality

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

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

Applications for Modal Types

Interpretations of $\Box A$:

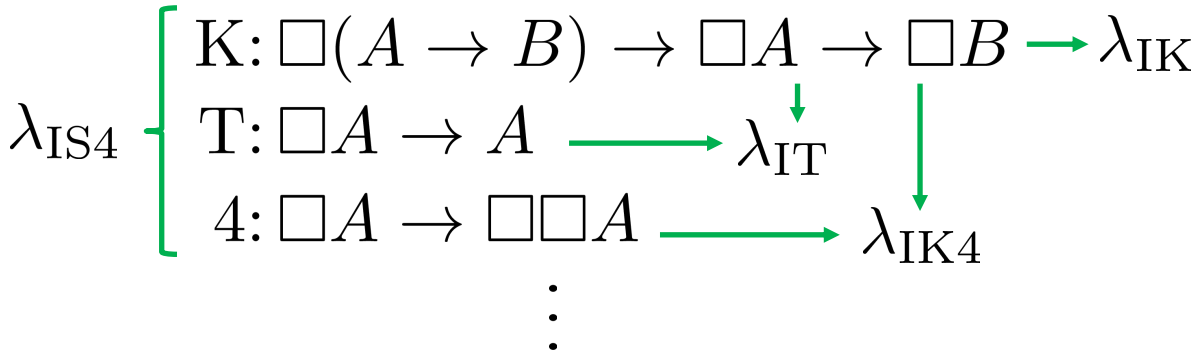
Impure languages: Pure value of type A

Information-flow control: Secret of type A

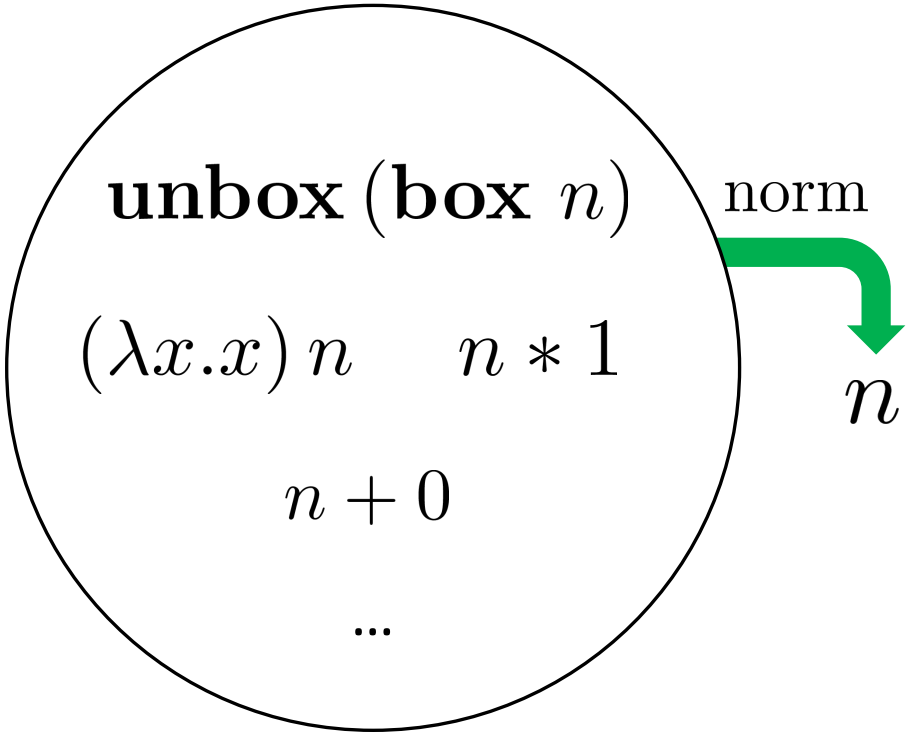
Staged computation: Code of type A

E.g., T: $\Box A \to A$ is not always desirable

Variety of Modal Operations



Why Normalization Matters



- Capability safety
- Noninterference
- Binding-time correctness
- Decidability
- Completeness
- ...

Fitch-Style Modal Calculi

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

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

Uniform introduction rule.

Fitch-Style Modal Calculi

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

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

Repetitive and tedious syntactic reasoning

Difficult to mechanize normalization

🔒 appears as an ad hoc device dry of intuition

Normalization by Evaluation (NbE)

$$\begin{aligned}
&\mathrm{eval} \quad : \Gamma \vdash A \to (\llbracket \Gamma \rrbracket \Rightarrow \llbracket A \rrbracket) \\
&\mathrm{quote} : (\llbracket \Gamma \rrbracket \Rightarrow \llbracket A \rrbracket) \to \Gamma \vdash_{\mathrm{NF}} A
\end{aligned}$$

$$\begin{aligned}
&\mathrm{norm} : \Gamma \vdash A \to \Gamma \vdash_{\mathrm{NF}} A \\
&\mathrm{norm} = \mathrm{quote} \circ \mathrm{eval}
\end{aligned}$$

Models of Fitch-Style Modal Calculi

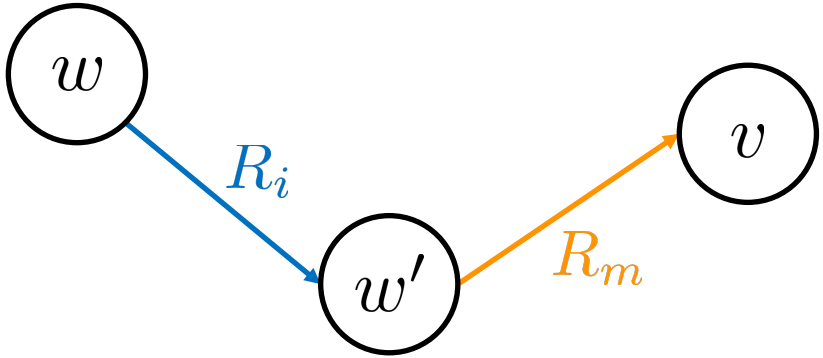
$$\text{What is } [\![\Gamma]\!] \Rightarrow [\![A]\!]?$$

The Story

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

Part 1: Possible-World Semantics

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



...

$$[\![\Box A]\!]_w = \forall w'.\, w\ R_i\ w' \rightarrow \forall v.\, w'\ R_m\ v \rightarrow [\![A]\!]_v$$

Possible-World Semantics

$$
\begin{aligned}
[\![\cdot]\!]_w &= () \\
[\![\Delta, A]\!]_w &= [\![\Delta]\!]_w \times [\![A]\!]_w \\
[\![\Delta, \blacksquare]\!]_w &= ??
\end{aligned}
$$

Box ~ Future

Lock ~ Past

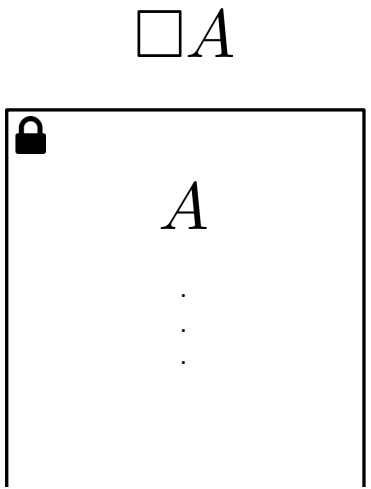
Possible-World Semantics

$$[\![\cdot]\!]_w = ()$$

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

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

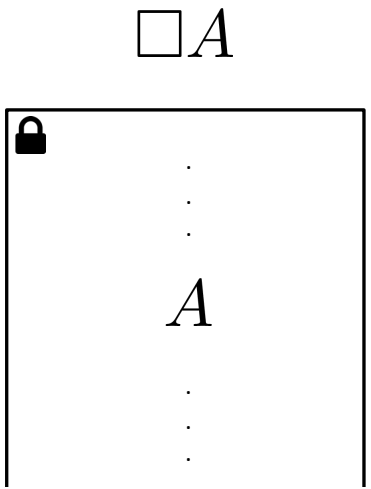
Portal Into the Future!



Import

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

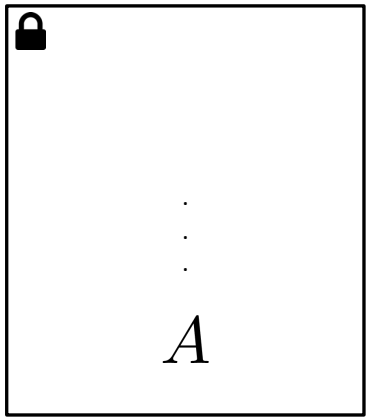
Portal Into the Future!



Import

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

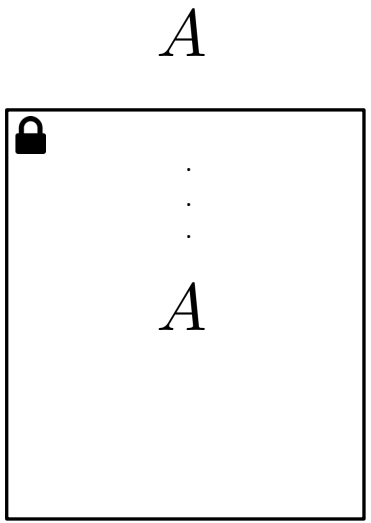
Portal Into the Future!



$\Box A$ Export

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

Portal Into the Future!



Copy

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

Part 2: NbE Using Possible-World Semantics

$$\begin{aligned}
&\mathrm{eval} \quad : \Gamma \vdash A \to (\forall w.\ [\![\Gamma]\!]_w \to [\![A]\!]_w) \\
&\mathrm{quote} : (\forall w.\ [\![\Gamma]\!]_w \to [\![A]\!]_w) \to \Gamma \vdash_{\mathrm{NF}} A
\end{aligned}$$

$$\begin{aligned}
&\mathrm{norm} : \Gamma \vdash A \to \Gamma \vdash_{\mathrm{NF}} A \\
&\mathrm{norm} = \mathrm{quote} \circ \mathrm{eval}
\end{aligned}$$

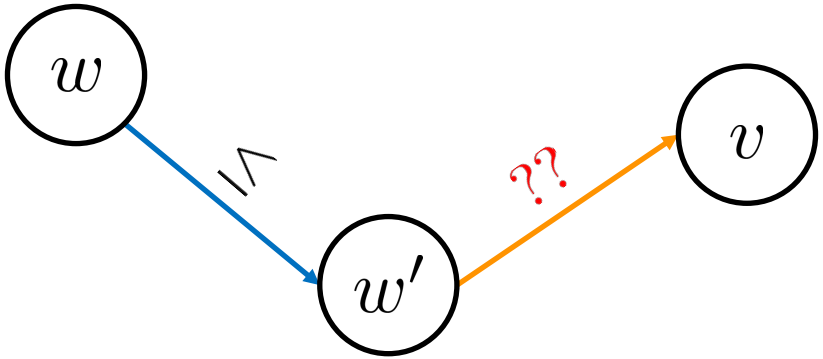
Constructing an NbE Model

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

$\mathcal{W}$ = Contexts

R_i = $\leq$ (OPEs)

R_m = ??



Key Observation: From the Syntax

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

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

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

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

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

Key Observation: From the Syntax

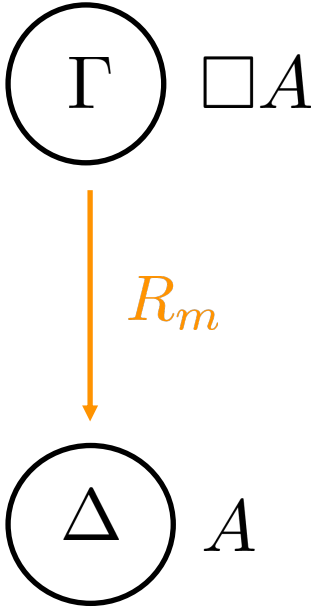
$$\frac{\Gamma, \text{🔒} \vdash t : A}{\Gamma \vdash \mathbf{box}\ t : \Box A}$$

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

Key Observation: From the Syntax

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

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



Constructing NbE Models

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

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

Constructing NbE Models

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

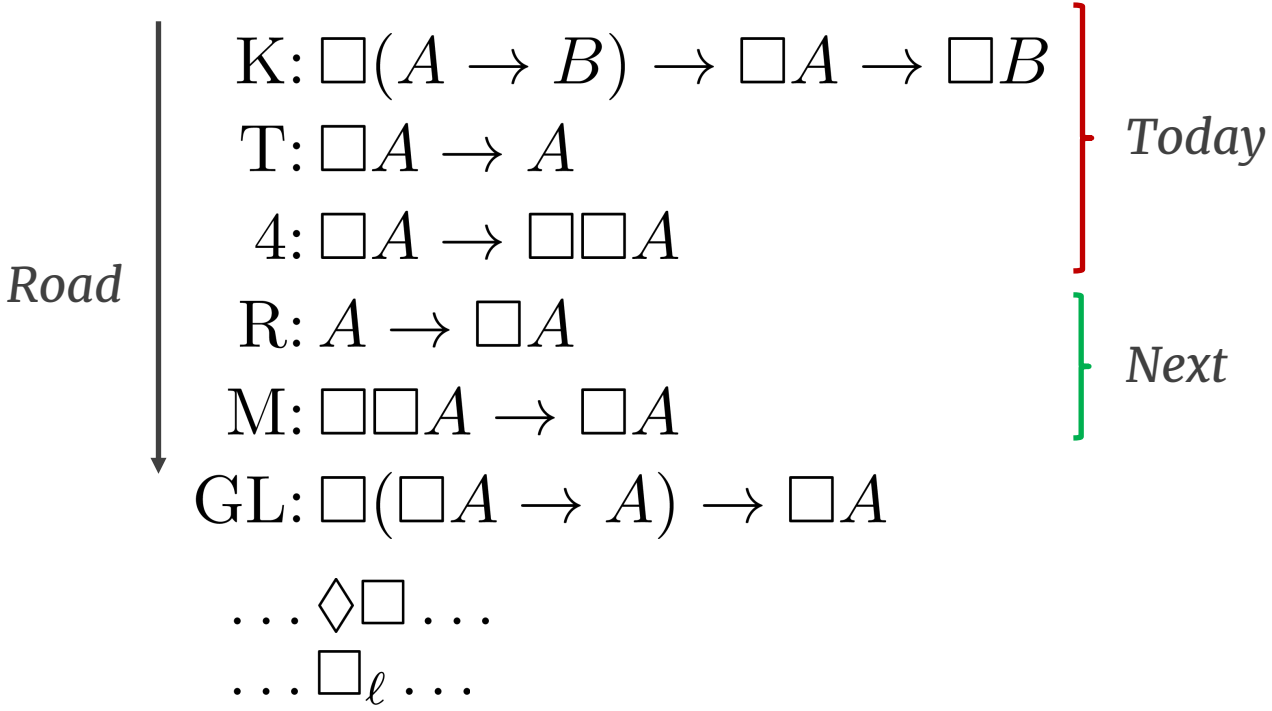
$$\lambda_{\mathrm{IS4}}\ \frac{\Gamma \vdash t : \Box A}{\Gamma, \Gamma' \vdash \mathbf{unbox}\ t : A}$$

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

R_m is reflexive and transitive

. . . and similarly for λ_{IK4} and λ_{IT}.

The Road Ahead



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