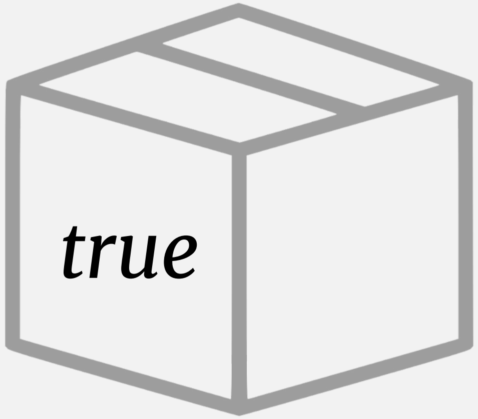
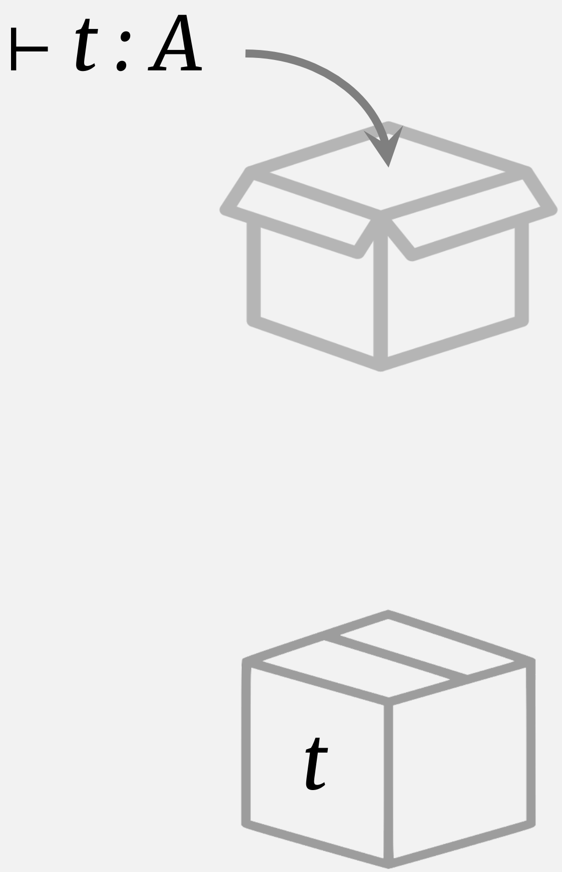
Boxes and Locks

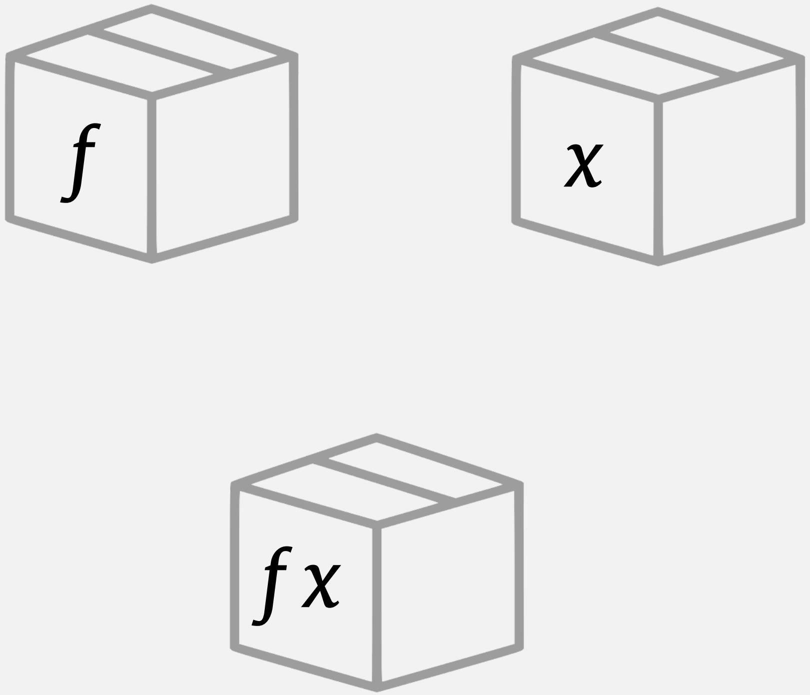
Nachiappan V.



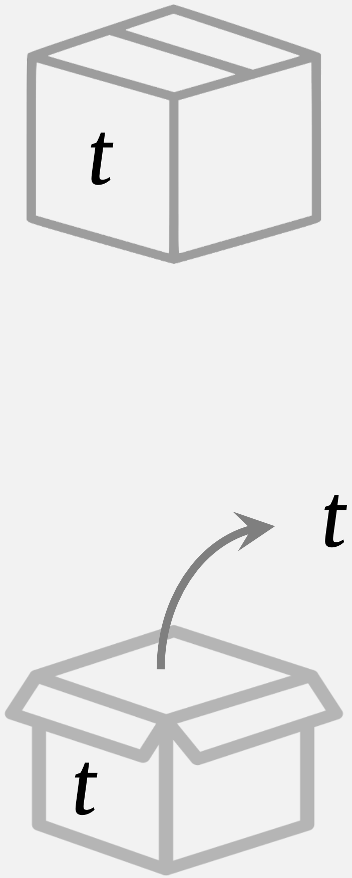
$: \quad \Box \mathit{Bool}$



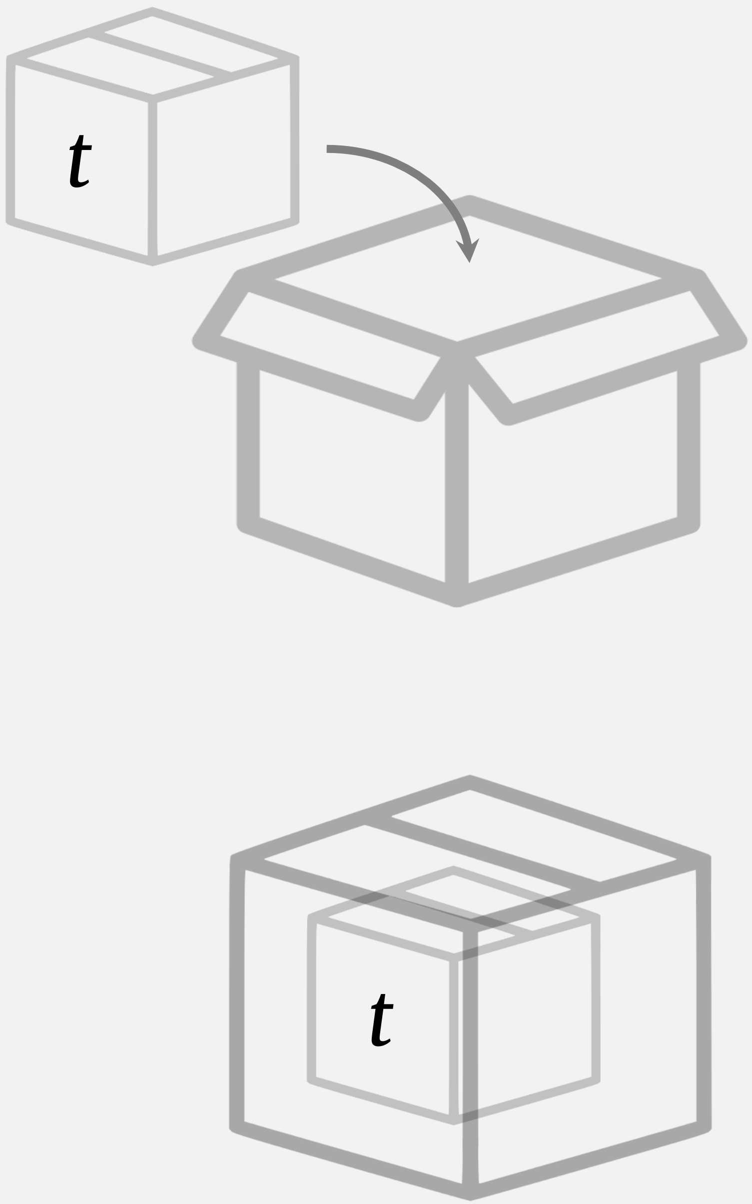
$$\frac{\vdash A}{\Gamma \vdash \Box A}\ \textsc{Nec}.$$



$$\mathrm{K}\colon \Gamma \vdash \Box(A \to B) \to \Box A \to \Box B$$



$$\mathrm{T}\colon \Gamma \vdash \Box A \to A$$



$$4\colon\ \Gamma \vdash \Box A \to \Box\Box A$$

IS4

$$\text{K: } \Gamma \vdash \Box(A \to B) \to \Box A \to \Box B$$

Today's focus

$$\text{T: } \Gamma \vdash \Box A \to A$$

$$\text{4: } \Gamma \vdash \Box A \to \Box\Box A$$

IK4

$$\text{R: } \Gamma \vdash A \to \Box A$$

IR

Fitch-style IK

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

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

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

Axiom K is derivable

$$\dfrac{\dfrac{\ldots, \blacksquare \vdash \textbf{unbox}\ f : A \to B \qquad \ldots, \blacksquare \vdash \textbf{unbox}\ x : A}{\Gamma, f : \Box(A \to B), x : \Box A, \blacksquare \vdash \textbf{app}\ (\textbf{unbox}\ f)\ (\textbf{unbox}\ x) : B}}{\Gamma, f : \Box(A \to B), x : \Box A \vdash \textbf{box}\ (\textbf{app}\ (\textbf{unbox}\ f)\ (\textbf{unbox}\ x)) : \Box B}$$

$$\dfrac{\Gamma \vdash t : \Box A}{\Gamma, \blacksquare, \Gamma' \vdash \textbf{unbox}\ t : A}\ \blacksquare \notin \Gamma' \qquad \dfrac{\Gamma, \blacksquare \vdash t : A}{\Gamma \vdash \textbf{box}\ t : \Box A}$$

Necessitation is admissible

$$\vdash A \quad \Longrightarrow \quad \vdash \Box A$$

$$\dfrac{\dfrac{\vdash t : A}{\blacksquare \vdash t : A}\ \text{WK}}{\vdash \mathbf{box}\ t : \Box A}$$

What about "Denecessitation"?

$$\vdash \Box A \quad \Longrightarrow \quad \vdash A$$

How would you prove this?

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

Normalization Rules

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

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

Normal Forms

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

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

Normalization by Evaluation

$$\llparenthesis\ \_\ \rrparenthesis \ : (\Gamma \vdash A) \to [\![\Gamma]\!]_\Delta \to [\![A]\!]_\Delta$$

$$\downarrow_A \ : [\![A]\!]_\Gamma \to (\Gamma \vdash_{\mathrm{nf}} A)$$

$$norm\ t = \downarrow (\llparenthesis\ t\ \rrparenthesis\ \gamma_{id})$$

Interpretation

$$[\![\tau]\!]_\Gamma = \Gamma \vdash_{\mathrm{nf}} \tau$$

$$[\![A \to B]\!]_\Gamma = \Gamma' \leq \Gamma \to [\![A]\!]_{\Gamma'} \to [\![B]\!]_{\Gamma'}$$

$$\boxed{[\![\Box A]\!]_\Gamma = \mathrm{Box}_\Gamma\ [\![A]\!]}$$

$$[\![\cdot]\!]_\Gamma = \top$$

$$[\![\Delta, A]\!]_\Gamma = [\![\Delta]\!]_\Gamma \times [\![A]\!]_\Gamma$$

$$\boxed{[\![\Delta, 🔒]\!]_\Gamma = \mathrm{Lock}_\Gamma\ [\![\Delta]\!]}$$

Boxes and Locks

$$\mathcal{A} : \mathrm{Ctx} \to \mathrm{Set}$$

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

$$(\text{🔒} \notin \Gamma')$$

$$unbox : \mathrm{Box}_{\Gamma}\ [\![\ A\ ]\!] \to [\![\ A\ ]\!]_{\Gamma, \text{🔒}, \Gamma'}$$

$$unbox\ (\mathsf{box}\ x) = wk\ x$$

Evaluation

$$\begin{aligned}
(\!|\ _\ |\!) &: (\Gamma \vdash A) \to [\![\Gamma]\!]_\Delta \to [\![A]\!]_\Delta \\
(\!|\ \mathbf{box}\ t\ |\!)\ \gamma &= \mathsf{box}\ ((\!|\ t\ |\!)\ \gamma) \\
(\!|\ \mathbf{unbox}\ t\ |\!)\ \langle \gamma, _ \rangle &= (\!|\ \mathbf{unbox}\ t\ |\!)\ \gamma \\
(\!|\ \mathbf{unbox}\ t\ |\!)\ (\mathsf{lock}\ \gamma) &= \mathit{unbox}\ ((\!|\ t\ |\!)\ \gamma)
\end{aligned}$$

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

Reification and Reflection

$$\downarrow_A \; : [\![A]\!]_\Gamma \to (\Gamma \vdash_{\mathrm{nf}} A)$$

$$\downarrow_{\Box A} \; (\mathsf{box}\ x) \quad = \mathbf{box}\ (\downarrow_A \;\; x)$$

$$\uparrow_A \; : (\Gamma \vdash_{\mathrm{ne}} A) \to [\![A]\!]_\Gamma$$

$$\uparrow_{\Box A} \; m \qquad\qquad = \mathsf{box}\ (\uparrow_A (\mathbf{unbox}\ m))$$

Denecessitation can be proved using normal forms

$$\vdash \Box A \quad \Longrightarrow \quad \vdash A$$

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

No neutrals in empty context, dismissed!

Only culprit that introduces 🔒

$$\vdots$$

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

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

Why?

1. Useful

- Towards confluence, decidability, consistency, etc.

- Simplify / prove new application-specific theorems?

  (e.g., partial evaluation/staging theorems, noninterference, etc.)

- Type-directed partial evaluation for modal type systems

2. Extensible: Boxes, Locks and (fake) Diamonds!

IK$\blacklozenge$

$$\frac{\Gamma \vdash t : A}{\Gamma, \text{🔒}, \Gamma' \vdash \mathbf{dia}\ t : \blacklozenge A}\ \text{🔒} \notin \Gamma' \qquad \frac{\Gamma \vdash t : \blacklozenge A \qquad A, \text{🔒} \vdash u : B}{\Gamma \vdash \mathbf{bind}\ t\ u : B}$$

Interpreting $\blacklozenge$

$$\frac{x : \mathrm{Lock}_{\Gamma} \mathcal{A}}{\mathsf{val}\ x : \mathrm{Dia}_{\Gamma}\ \mathcal{A}} \qquad \frac{m : \Gamma \vdash_{\mathrm{ne}} \blacklozenge A \qquad y : \mathrm{Dia}_{A, \text{🔒}}\ \mathcal{A}}{\mathsf{bindst}\ m\ y : \mathrm{Dia}_{\Gamma}\ \mathcal{A}}\ \text{🔒} \notin \Gamma'$$

2. Extensible: IS4, IK4, IR

$$\text{IS4}\left\{\begin{array}{l} \text{K: } \Gamma \vdash \Box(A \to B) \to \Box A \to \Box B \\[1em] \text{T: } \Gamma \vdash \Box A \to A \\[1em] \text{4: } \Gamma \vdash \Box A \to \Box\Box A \longrightarrow \text{IK4} \end{array}\right.$$

$$\text{R: } \Gamma \vdash A \to \Box A \longrightarrow \text{IR}$$

3. Comprehensible: Reduction traces

DEMO

4. Elegant: Boxes and Locks, in an Adjoint relationship

$$unit : \mathcal{A} \overset{\cdot}{\longrightarrow} \text{Box}\ (\text{Lock}\ \mathcal{A}) \qquad\qquad counit : \text{Lock}\ (\text{Box}\ \mathcal{A}) \overset{\cdot}{\longrightarrow} \mathcal{A}$$

$$unit\ x = \mathsf{box}\ (\mathsf{lock}\ x) \qquad\qquad counit\ (\mathsf{lock}\ (\mathsf{box}\ x)) = wk\ x$$

$$\begin{tikzcd}
\text{Lock}\ \mathcal{A} \arrow[r, "id"] & \text{Lock}\ \mathcal{A} \arrow[dl, "\text{Lock}_1(unit)"] \arrow[dl, phantom, shift right=6ex, "\circlearrowleft"] \\
\text{Lock}\ (\text{Box}\ (\text{Lock}\ \mathcal{A})) \arrow[u, "counit"] &
\end{tikzcd}$$

What would you like to see more of?

Modalities (S4, K4, R, etc.)

Semantics

Applications

Extensions (0, +, Nat, etc.)

EOM