Curry-Howard for Modal Logic

Alex Kavvos

Department of Mathematics and Computer Science, Wesleyan University

CUNY Computational Logic Seminar, 30 Oct 2018

Outline

1. Curry-Howard
   - Hilbert systems
   - Natural deduction
   - The Curry-Howard correspondence
2. Normal Modal Logic
   - Modalities and Axioms
   - Hilbert systems for modal logic
   - Bierman and de Paiva's system for S4
   - The Pfenning-Davies system for S4
   - Programming applications
3. Cutting-edge work

Curry-Howard

The Curry-Howard-Lambek correspondence

$$\begin{tikzcd} \text{logic} \arrow[rr, leftrightarrow] \arrow[dr, leftrightarrow] & & \text{computation} \arrow[dl, leftrightarrow] \\ & \text{categories} & \end{tikzcd}$$

For the connection "logic $\leftrightarrow$ computation" perhaps the most seminal reference of all (at least in France and the UK) is

- Jean-Yves Girard, Yves Lafont, and Paul Taylor (1989). *Proofs and Types.* Cambridge University Press

For the relationship to categories, perhaps

- Samson Abramsky and Nikos Tzevelekos (2011). "Introduction to Categories and Categorical Logic". In: *New Structures for Physics.* Ed. by Bob Coecke. Springer-Verlag, pp. 3–94. DOI: 10.1007/978-3-642-12821-9_1. arXiv: 1102.1313

What is logic about?

Traditionally,

$\boxed{\text{truth}}$

- which sentences are **true**?
- can I split them into **axioms**, which are evidently true, and
- a few simple **inference rules**, that preserve truth?

A bit arbitrary. To make it less so,

- can I find a **yardstick**, maybe human language, or another mathematical theory that I feel I understand well, i.e. a **semantics**,
- into which I can **translate** my *axioms* and my *inference rules*, and find that they look good (**soundness**),
- and also hopefully prove that **everything that the translation says looks good ('is true') is provable in my system**? (**completeness**)

What is logic about?

Beginning in the 1930s, some of the focus shifts to

$\boxed{\text{proof}}$

- what follows from what? what is a proof?
- can I isolate the **structural rules** that generate my notion of proof?
- can I explain what it means for a proof to be **normal**, i.e. as simple as possible? can I simplify proofs?

Also a bit arbitary. To make it less so,

- can I find a **yardstick**, maybe another mathematical theory that I feel I understand well, i.e. a **semantics**,
- into which I can **translate** my *structural rules* to this theory, and find that they look good (**soundness**),
- and also hopefully prove that **everything that the translation says is a proof is expressible in my system**? (**full completeness**)

An example of each: (I) Hilbert systems for prop. logic

Judgements: $\Gamma \vdash A$

- *contexts*: $\Gamma = A_1, \ldots, A_n$ is a finite list, where the A_i are formulas of propositional logic
- *axioms*: pick some (without excluded middle); e.g. for conjunction:

$$A \to (B \to A \wedge B)$$
$$A \wedge B \to A$$
$$A \wedge B \to B$$

- *rules*: **axiom**, **assumption**, **modus ponens**:

$$\frac{}{\Gamma, A, \Delta \vdash A} \qquad \frac{A \text{ is an axiom}}{\Gamma \vdash A} \qquad \frac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}$$

An example of each: (I) Hilbert systems for prop. logic

$$\frac{}{\Gamma, A, \Delta \vdash A} \qquad \frac{A \text{ is an axiom}}{\Gamma \vdash A} \qquad \frac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}$$

For this system we can prove theorems. For example:

Theorem (Deduction)

The following rule is admissible:

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}$$

Note: a rule $\frac{\mathcal{I}}{\mathcal{J}}$ is *admissible* if from a proof $\frac{\vdots}{\mathcal{I}}$ we can construct a proof $\frac{\vdots}{\mathcal{J}}$ (**in the metatheory!**).

An example of each: (II) Gentzen natural deduction

Gentzen's thesis, ca. 1934-5: *natural deduction* and *sequent calculus*
Main ideas:

- **connectives** as structural elements;
- each connective has an **introduction rule**,
- and an **elimination rule**.

E.g. the axioms

$$\begin{aligned} A \to (B \to A \wedge B) \\ A \wedge B \to A \\ A \wedge B \to B \end{aligned}$$

are replaced by

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,(\wedge\mathcal{I}) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\,(\wedge\mathcal{E}_1) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\,(\wedge\mathcal{E}_2)$$

An example of each: (II) Gentzen natural deduction

Natural Deduction (NJ) for intuitionistic propositional logic

Judgements: $\Gamma \vdash A$ again

$$\frac{}{\Gamma, A, \Delta \vdash A}\ (\text{assn})$$

$$\frac{}{\Gamma \vdash \top}\ (\top\mathcal{I}) \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash A}\ (\bot\mathcal{E})$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ (\wedge\mathcal{I}) \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ (\wedge\mathcal{E}_1) \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ (\wedge\mathcal{E}_2)$$

$$\frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C \quad \Gamma \vdash A \vee B}{\Gamma \vdash C}\ (\vee\mathcal{E}) \quad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ (\vee\mathcal{I}_1) \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ (\vee\mathcal{I}_2)$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ (\to\mathcal{I}) \quad \frac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}\ (\to\mathcal{E})$$

An example of each: (II) Gentzen natural deduction

Theorem (Equivalence)

There is a proof $\dfrac{\vdots}{\Gamma \vdash A}$ *in the Hilbert system (without excluded middle) if and only if there is a proof* $\dfrac{\vdots}{\Gamma \vdash A}$ *in natural deduction.*

(Can be extended to cover excluded middle, but we do not want it.)

Theorem (Cut)

The following rule is admissible:

$$\frac{\Gamma \vdash A \quad \Gamma, A, \Delta \vdash C}{\Gamma, \Delta \vdash C}$$

Very easy to prove: just a simple induction!

Doing silly things

- You can do silly things in natural deduction.
- (You can do silly things in Hilbert systems too…
- but NJ has a lot of **symmetry**, so can tell when one is being silly.)

Suppose there is a proof $\dfrac{\dfrac{\dfrac{\mathcal{D}}{\Gamma \vdash A} \quad \dfrac{\mathcal{D}'}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\,(\wedge\mathcal{I})}{\Gamma \vdash A}\,(\wedge\mathcal{E}_1)$. Isn't this just $\dfrac{\mathcal{D}}{\Gamma \vdash A}$?

Proof dynamics

We can introduce a *dynamics* on proofs, i.e. a *reduction* relation:

$$\dfrac{\dfrac{\dfrac{\mathcal{D}}{\Gamma \vdash A} \qquad \dfrac{\mathcal{D}'}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B}\ (\wedge\mathcal{I})}{\Gamma \vdash A}\ (\wedge\mathcal{E}_1) \qquad \longrightarrow \qquad \dfrac{\mathcal{D}}{\Gamma \vdash A}$$

Similarly:

$$\dfrac{\dfrac{\dfrac{\mathcal{D}}{\Gamma, A \vdash B}}{\Gamma \vdash A \to B}\ (\to \mathcal{I}) \qquad \dfrac{\mathcal{D}'}{\Gamma \vdash A}}{\Gamma \vdash B}\ (\to \mathcal{E}) \qquad \longrightarrow \qquad \dfrac{\mathcal{D}[\mathcal{D}'/A]}{\Gamma \vdash B}$$

where $\mathcal{D}[\mathcal{D}'/A]$ is $\mathcal{D}$ with every use of assumption A is replaced by $\mathcal{D}'$.

The Curry-Howard correspondence

- We are now **studying proofs as mathematical objects**!
- But the notation is very cumbersome.
- Why don't we *linearise* it?

$$\dfrac{\dfrac{\vdots}{\Gamma \vdash A} \quad \dfrac{\vdots}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B} \quad \Longrightarrow \quad \dfrac{\dfrac{\vdots}{\Gamma \vdash M : A} \quad \dfrac{\vdots}{\Gamma \vdash N : B}}{\Gamma \vdash \langle M, N \rangle : A \times B}$$

$$\dfrac{\dfrac{\vdots}{\Gamma \vdash A \wedge B}}{\Gamma \vdash A} \quad \Longrightarrow \quad \dfrac{\dfrac{\vdots}{\Gamma \vdash P : A \times B}}{\Gamma \vdash \pi_1(P) : A}$$

formulæ = types

proofs (of natural deduction) = programs

reduction/simplification = computation

The Curry-Howard correspondence

formulæ = types

proofs (in natural deduction) = programs

reduction (simplification of proofs) = computation

$$\boxed{\text{the } \textit{proof term } M \text{ in } \Gamma \vdash M : A \text{ is a } \textit{summary} \text{ of a derivation with conclusion } \Gamma \vdash A}$$

Recall the reduction

$$\dfrac{\dfrac{\mathcal{D}}{\Gamma \vdash A} \quad \dfrac{\vdots}{\Gamma \vdash B}}{\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}} \quad \longrightarrow \quad \dfrac{\mathcal{D}}{\Gamma \vdash A}$$

We now write it as a reduction of *proof terms*:

$$\pi_1(\langle M, N \rangle) \longrightarrow M$$

The Curry-Howard correspondence

Natural Deduction (NJ) for intuitionistic propositional logic

Judgements: $\Gamma \vdash A$

$$\frac{}{\Gamma, A, \Delta \vdash A}\,(\text{assn})$$

$$\frac{}{\Gamma \vdash \top}\,(\top\mathcal{I}) \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash A}\,(\bot\mathcal{E})$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,(\wedge\mathcal{I}) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\,(\wedge\mathcal{E}_1) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\,(\wedge\mathcal{E}_2)$$

$$\frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C \quad \Gamma \vdash A \vee B}{\Gamma \vdash C}\,(\vee\mathcal{E}) \qquad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,(\vee\mathcal{I}_1) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\,(\vee\mathcal{I}_2)$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\,(\to\mathcal{I}) \qquad \frac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}\,(\to\mathcal{E})$$

The Curry-Howard correspondence

The simply-typed λ-calculus

Judgements: $\Gamma \vdash M : A$

$$\frac{}{\Gamma, x : A, \Delta \vdash x : A}\ (\text{assn})$$

$$\frac{}{\Gamma \vdash * : \top}\ (\top\mathcal{I}) \qquad \frac{\Gamma \vdash M : \bot}{\Gamma \vdash \mathsf{absurd}(M) : A}\ (\bot\mathcal{E})$$

$$\frac{\Gamma \vdash M : A \quad \Gamma \vdash N : B}{\Gamma \vdash \langle M, N \rangle : A \times B}\ (\times\mathcal{I}) \qquad \frac{\Gamma \vdash M : A \times B}{\Gamma \vdash \pi_1(M) : A}\ (\times\mathcal{E}_1) \qquad \frac{\Gamma \vdash M : A \times B}{\Gamma \vdash \pi_2(M) : B}\ (\times\mathcal{E}_2)$$

$$\frac{\Gamma, u : A \vdash M : C \quad \Gamma, v : B \vdash N : C \quad \Gamma \vdash P : A + B}{\Gamma \vdash \mathsf{match}_C\ (P, u.\ M, v.\ N) : C}\ (+\mathcal{E}) \qquad \frac{\Gamma \vdash M : A}{\Gamma \vdash \mathsf{inl}(M) : A + B}$$

$$\frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x{:}A.\ M : A \to B}\ (\to \mathcal{I}) \qquad \frac{\Gamma \vdash M : A \to B \quad \Gamma \vdash N : A}{\Gamma \vdash M(N) : B}\ (\to \mathcal{E})$$

Dynamics of the simply-typed λ-calculus

The main principle is:

$$\boxed{\text{Elimination is post-inverse to introduction}}$$

Take the rules for implication:

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma, x : A \vdash M : B}}{\Gamma \vdash \lambda x{:}A.\ M : A \to B}\ (\to \mathcal{I}) \qquad \dfrac{\vdots}{\Gamma \vdash N : A}}{\Gamma \vdash (\lambda x{:}A.\ M)(N) : B}\ (\to \mathcal{E})$$

The dynamics specifies that

$$(\lambda x{:}A.\ M)(N) \longrightarrow M[N/x]$$

Moreover, the dynamics is a **congruence**; e.g.

$$\langle(\lambda x{:}A.\ M)(N), \pi_1(P)\rangle \longrightarrow \langle M[N/x], \pi_1(P)\rangle$$

Reasoning about proofs

The **three pillars of the Curry-Howard correspondence**:

- **confluence**, a.k.a. the Church-Rosser property
  - proofs are mathematical expressions: their meaning is determined by their parts, and the order of reductions is irrelevant
- **strong normalisation**, due to Tait (1967)
  - if $\Gamma \vdash M_1 : A$ then there is no infinite reduction sequence

$$M_1 \longrightarrow M_2 \longrightarrow \dots$$

- the **subformula property**, due to Prawitz (1965)
  - if $\Gamma \vdash N : A$ is *normal*, i.e. there is no reduction step $N \longrightarrow N'$, then the derivation of $\Gamma \vdash N : A$ can *only* mention subformulas of A and subformulas of assumptions in Γ (no irrelevant stuff, no detours)

To sum up,

> one can eliminate detours from a proof in finite time

Extending Curry-Howard

- Classical logic?
  - Works, but is not nice and easy.
  - Seems to cause *non-local control flow*, related in particular to *continuations*.
  - See the following notes for pointers:
    - Stéphane Graham-Lengrand (2015). "The Curry-Howard view of classical logic". In:
- First-order logic? **Yes**, in Howard's paper.
- More interestingly, higher-order logic:
  - The most active community works on **Martin-Löf type theory**, also known as **dependent type theory**. See
    - Bengt Nordström, Kent Petersson, and Jan M. Smith (1990). *Programming in Martin-Löf's Type Theory: an Introduction*. Oxford University Press. DOI: 10.1016/0377-0427(91)90052-L

  and also **homotopy type theory**.

Some references

Noticed by Curry and Feys in terms of combinators. First openly stated in 1969 by W. A. Howard in:

- William A Howard (1980). "The formulae-as-types notion of construction". In: *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*. Ed. by Jonathan P. Seldin and J. Roger Hindley. Boston, MA: Academic Press, pp. 479–490

Books:

- Jean-Yves Girard, Yves Lafont, and Paul Taylor (1989). *Proofs and Types*. Cambridge University Press
- Morten Heine Sørensen and Pawel Urzyczyn (2006). *Lectures on the Curry-Howard Isomorphism*. Elsevier

And an interesting paper on natural deduction:

- Per Martin-Löf (1996). "On the meanings of the logical constants and the justification of the logical laws". In: *Nordic Journal of Philosophy* 1.1, pp. 11–60

Normal Modal Logic

Modal Logic

In the most general sense,

$$\boxed{\text{modality} = \text{a unary operation on formulæ}}$$

- Some common notations: $\Box A$, $\Diamond A$, $T(A)$, $F(A)$, $\|A\|$, ...
- A very rich theory developed following the discovery of *Kripke semantics* (Kripke, 1963).

By using Kripke semantics we have already accepted the K axiom:

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

which in category theory we like to write as

$$\Box(A \times B) \cong \Box A \times \Box B$$

We will focus on the necessity fragment with K for now.

Some common axioms

$$
\begin{aligned}
(\mathsf{K}) &\quad \Box(A \to B) \to (\Box A \to \Box B) \\
(\mathsf{4}) &\quad \Box A \to \Box\Box A \\
(\mathsf{T}) &\quad \Box A \to A \\
(\mathsf{GL}) &\quad \Box(\Box A \to A) \to \Box A
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{CK} &\stackrel{\text{def}}{=} (\mathsf{IPL}_\Box) \oplus (\mathsf{K}) \\
\mathsf{CK4} &\stackrel{\text{def}}{=} (\mathsf{IPL}_\Box) \oplus (\mathsf{K}) \oplus (\mathsf{4}) \\
\mathsf{CT} &\stackrel{\text{def}}{=} (\mathsf{IPL}_\Box) \oplus (\mathsf{K}) \oplus (\mathsf{T}) \\
\mathsf{CS4} &\stackrel{\text{def}}{=} (\mathsf{IPL}_\Box) \oplus (\mathsf{K}) \oplus (\mathsf{4}) \oplus (\mathsf{T}) \\
\mathsf{CGL} &\stackrel{\text{def}}{=} (\mathsf{IPL}_\Box) \oplus (\mathsf{K}) \oplus (\mathsf{GL})
\end{aligned}
$$

$(\mathsf{IPL}_\Box) \stackrel{\text{def}}{=}$ axioms of int. prop. logic, but over syntax with $\Box$

$\oplus \stackrel{\text{def}}{=}$ union followed by closure under deduction

Hilbert systems for normal modal logic

Judgements: $\Gamma \vdash A$

- *contexts*: $\Gamma = A_1, \ldots, A_n$ is a finite list, where the A_i are formulas of propositional logic
- *axioms*: as in the previous slide, for each logic
- *rules*: **axiom**, **assumption**, **modus ponens** and **necessitation**:

$$\frac{}{\Gamma, A, \Delta \vdash A} \qquad \frac{A \text{ is an axiom}}{\Gamma \vdash A} \qquad \frac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B} \qquad \boxed{\frac{\vdash A}{\Gamma \vdash \Box A}}$$

A wayward rule; see

- Raul Hakli and Sara Negri (2012). "Does the deduction theorem fail for modal logic?" In: *Synthese* 187.3, pp. 849–867. DOI: 10.1007/s11229-011-9905-9

Hilbert systems for modal logic

Theorem (Deduction)

The following rule is admissible: $$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}$$

Let $\Box(A_1, \ldots, A_n) \stackrel{\text{def}}{=} \Box A_1, \ldots, \Box A_n$.

Theorem (Scott's rule)

The following rule is admissible: $$\frac{\Gamma \vdash A}{\Box\Gamma \vdash \Box A}$$

Theorem (Four rule)

If axiom 4 is included, the following rule is admissible: $$\frac{\Box\Gamma, \Gamma \vdash A}{\Box\Gamma \vdash \Box A}$$

Hilbert systems for modal logic

Theorem (Löb's rule)

If axiom GL is included, the following rule is admissible: $\dfrac{\Box\Gamma, \Gamma, \Box A \vdash A}{\Box\Gamma \vdash \Box A}$

Theorem (T rule)

If axiom T is included, the following rule is admissible: $\dfrac{\Gamma \vdash A}{\Box\Gamma \vdash A}$

Natural deduction for modal logic?

- Not easy, especially if we want Curry-Howard + three pillars.
- Many attempts, appearing as early as the seminar work of Prawitz (1965, 1971) on natural deduction.
- I wrote a long (unpublished) survey on this:
  - G. A. Kavvos (2016). "The Many Worlds of Modal Lambda Calculi: I. Curry-Howard for Necessity, Possibility and Time". In: *CoRR*. arXiv: 1605.08106

  As of Oct 2018 I consider this draft inaccurate and incomplete.
- The first prim and proper extension of Curry-Howard to any modal logic is the crowning achievement of Bierman and Paiva (1996, 2000).

Bierman and de Paiva's system for S4

A trick that often works in passing from Hilbert systems to the natural deduction system:

$$\boxed{\text{take the admissible rules as introduction rules}}$$

E.g.

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B} \quad \rightsquigarrow \quad \frac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x{:}A.\ M : A \to B}$$

Does not work here; the obvious adaptation of $\dfrac{\Box\Gamma \vdash A}{\Box\Gamma \vdash \Box A}$ to

$$\frac{x_1 : \Box A_1, \ldots, x_n : \Box A_n \vdash N : B}{x_1 : \Box A_1, \ldots, x_n : \Box A_n \vdash \mathrm{box}\ N : \Box B}$$

does not even satisfy basic correctness properties (in particular, subject reduction—a.k.a closure under substitution—fails).

Bierman and de Paiva's system for S4

Bierman and de Paiva's solution:

$$\frac{\Gamma \vdash M_1 : \Box A_1 \quad \dots \quad \Gamma \vdash M_n : \Box A_n \qquad x_1 : \Box A_1, \dots, x_n : \Box A_n \vdash N : B}{\Gamma \vdash \text{box } N \text{ with } M_1, \dots, M_n \text{ for } x_1, \dots x_n : \Box B}$$

Like the rule, but including 'substitutes' for all x_i (*explicit substitutions*).
The elimination rule is:

$$\frac{\Gamma \vdash M : \Box A}{\Gamma \vdash \text{unbox } M : A}$$

along with dynamics:

$$\text{unbox } (\text{box } N \text{ with } M_1, \dots, M_n \text{ for } x_1, \dots x_n) \longrightarrow N[M_1/x_1, \dots, M_n/x_n]$$

Theorem (Bierman, de Paiva, Goubault-Larrecq)

The above coincides with the Hilbert system, and satisfies the three pillars.

Bierman and de Paiva's system for S4

$$\frac{\Gamma \vdash M_1 : \Box A_1 \quad \ldots \quad \Gamma \vdash M_n : \Box A_n \qquad x_1 : \Box A_1, \ldots, x_n : \Box A_n \vdash N : B}{\Gamma \vdash \text{box } N \text{ with } M_1, \ldots, M_n \text{ for } x_1, \ldots x_n : \Box B}$$

Proof-theoretically, not a great rule:

- the third pillar (subformula property) works only if we add many **commuting conversions**, i.e. extra 'non-logical' reductions
- some **harmony**, but still a bit dissonant: the connective that is being introduced ($\Box$) already appears in the premise!

Bierman and de Paiva's system for S4

$$\frac{\Gamma \vdash M_1 : \Box A_1 \quad \ldots \quad \Gamma \vdash M_n : \Box A_n \qquad x_1 : \Box A_1, \ldots, x_n : \Box A_n \vdash N : B}{\Gamma \vdash \text{box } N \text{ with } M_1, \ldots, M_n \text{ for } x_1, \ldots x_n : \Box B}$$

Proof-theoretically, not a great rule:

- the third pillar (subformula property) works only if we add many **commuting conversions**, i.e. extra 'non-logical' reductions
- some **harmony**, but still a bit dissonant: the connective that is being introduced ($\Box$) already appears in the premise!

Bierman and de Paiva's system for S4

$$\frac{\Gamma \vdash M_1 : \Box A_1 \quad \dots \quad \Gamma \vdash M_n : \Box A_n \qquad x_1 : \Box A_1, \dots, x_n : \Box A_n \vdash N : B}{\Gamma \vdash \text{box } N \text{ with } M_1, \dots, M_n \text{ for } x_1, \dots x_n : \Box B}$$

Proof-theoretically, not a great rule:

- the third pillar (subformula property) works only if we add many **commuting conversions**, i.e. extra 'non-logical' reductions
- some **harmony**, but still a bit dissonant: the connective that is being introduced ($\Box$) already appears in the premise!

Bierman and de Paiva's system for S4

$$\frac{\Gamma \vdash M_1 : \Box A_1 \quad \ldots \quad \Gamma \vdash M_n : \Box A_n \qquad x_1 : \Box A_1, \ldots, x_n : \Box A_n \vdash N : B}{\Gamma \vdash \text{box } N \text{ with } M_1, \ldots, M_n \text{ for } x_1, \ldots x_n : \Box B}$$

Proof-theoretically, not a great rule:

- the third pillar (subformula property) works only if we add many **commuting conversions**, i.e. extra 'non-logical' reductions
- some **harmony**, but still a bit dissonant: the connective that is being introduced ($\Box$) already appears in the premise!

Another idea, due to Pfenning and Davies (2001)

Consider the following version of the Four rule (missing an extra Γ):

$$\frac{\Box\Gamma \vdash A}{\Box\Gamma \vdash \Box A}$$

Dataflow interpretation: if all the assumptions are *modal*, then we can modalise the conclusion. There are two **modes**.
We make up a new type of judgement:

$$\overbrace{\Delta}^{\text{modal}} \; ; \; \underbrace{\Gamma}_{\text{intuitionistic}} \vdash A$$

Davies and Pfenning (2001) also call the assumptions Δ *valid*.

Another idea, due to Pfenning and Davies (2001)

We can now do the following:

$$\frac{\Box\Delta \vdash A}{\Box\Delta \vdash \Box A} \quad \rightsquigarrow \quad \frac{\Box\Delta \vdash A}{\Box\Delta, \Gamma \vdash \Box A} \quad \rightsquigarrow \quad \frac{\Delta\,;\cdot \vdash A}{\Delta\,;\Gamma \vdash \Box A}$$

If $\Delta = \cdot$ this is just necessitation: $\dfrac{\cdot\,;\cdot \vdash A}{\cdot\,;\Gamma \vdash \Box A}$

As for elimination, forget unbox. Take a horrible cut rule instead, along with a rule for using/unboxing a modal assumption:

$$\frac{\Delta\,;\Gamma \vdash \Box A \quad \Delta, A\,;\Gamma \vdash C}{\Delta\,;\Gamma \vdash C}\,(\Box\mathcal{E}) \qquad \frac{}{\Delta, A, \Delta'\,;\Gamma \vdash A}\,(\Box\mathsf{var})$$

Another idea, due to Pfenning and Davies (ibid.)

It is straightforward to turn this into a λ-calculus for S4:

$$\frac{\Delta\,;\,\cdot \vdash M : A}{\Delta\,;\,\Gamma \vdash \mathsf{box}\ M : \Box A}\ (\Box\mathcal{I}) \qquad \frac{\Delta\,;\,\Gamma \vdash M : \Box A \qquad \Delta, u{:}A\,;\,\Gamma \vdash N : C}{\Delta\,;\,\Gamma \vdash \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N : C}\ (\Box\mathcal{E})$$

along with dynamics

$$\mathsf{let\ box}\ u \Leftarrow \mathsf{box}\ M\ \mathsf{in}\ N \longrightarrow N[M/u]$$

Theorem (K., LICS 2017)

The above coincides with the Hilbert system, and satisfies the three pillars.

I may have done the formal work, but the ideas are all in

- Frank Pfenning and Rowan Davies (2001). "A judgmental reconstruction of modal logic". In: *Mathematical Structures in Computer Science* 11.4, pp. 511–540. DOI: 10.1017/S0960129501003322

Reusing this idea

This idea can be adapted. In the case of K:

$$\frac{\Delta \vdash A}{\Box\Delta \vdash \Box A} \quad \rightsquigarrow \quad \frac{\Delta \vdash A}{\Box\Delta, \Gamma \vdash \Box A} \quad \rightsquigarrow \quad \frac{\cdot\,;\,\Delta \vdash A}{\Delta\,;\,\Gamma \vdash \Box A}$$

If $\Gamma = \cdot$ this is just Scott's rule: $\dfrac{\cdot\,;\,\Delta \vdash A}{\Delta\,;\,\cdot \vdash \Box A}$ Cf. $\dfrac{\Delta \vdash A}{\Box\Delta \vdash \Box A}$

Reusing this idea

K, T
$$\frac{\Delta \vdash A}{\Box\Delta \vdash \Box A} \rightsquigarrow \frac{\Delta \vdash A}{\Box\Delta, \Gamma \vdash \Box A} \rightsquigarrow \frac{\cdot\, ; \Delta \vdash A}{\Delta\, ; \Gamma \vdash \Box A}$$

K4
$$\frac{\Box\Delta, \Delta \vdash A}{\Box\Delta \vdash \Box A} \rightsquigarrow \frac{\Box\Delta, \Delta \vdash A}{\Box\Delta, \Gamma \vdash \Box A} \rightsquigarrow \frac{\Delta\, ; \Delta \vdash A}{\Delta\, ; \Gamma \vdash \Box A}$$

GL
$$\frac{\Box\Delta, \Delta, \Box A \vdash A}{\Box\Delta \vdash \Box A} \rightsquigarrow \frac{\Box\Delta, \Delta, \Box A \vdash A}{\Box\Delta, \Gamma \vdash \Box A} \rightsquigarrow \frac{\Delta\, ; \Delta, \Box A \vdash A}{\Delta\, ; \Gamma \vdash \Box A}$$

S4
$$\frac{\Box\Delta \vdash A}{\Box\Delta \vdash \Box A} \rightsquigarrow \frac{\Box\Delta \vdash A}{\Box\Delta, \Gamma \vdash \Box A} \rightsquigarrow \frac{\Delta\, ; \cdot \vdash A}{\Delta\, ; \Gamma \vdash \Box A}$$

Reusing this idea

$$\frac{\cdot\,;\Delta \vdash M : A}{\Delta\,;\Gamma \vdash \mathsf{box}\ M : \Box A}\ (\Box_{\mathsf{K}}\mathcal{I}) \qquad \frac{\Delta\,;\Delta^{\perp} \vdash M^{\perp} : A}{\Delta\,;\Gamma \vdash \mathsf{box}\ M : \Box A}\ (\Box_{\mathsf{K4}}\mathcal{I})$$

$$\frac{\Delta\,;\Delta^{\perp}, z^{\perp} : \Box A \vdash M^{\perp} : A}{\Delta\,;\Gamma \vdash \mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ M : \Box A}\ (\Box_{\mathsf{GL}}\mathcal{I}) \qquad \frac{\Delta\,;\Gamma \vdash M : \Box A \quad \Delta, u{:}A\,;\Gamma \vdash N : C}{\Delta\,;\Gamma \vdash \mathsf{let}\ \mathsf{box}\ u \Leftarrow M\ \mathsf{in}\ N : C}$$

Each of these leads to a λ-calculus with the same elim. rule. Dynamics:

$$\mathsf{let}\ \mathsf{box}\ u \Leftarrow \mathsf{box}\ M\ \mathsf{in}\ N \longrightarrow N[M/u]$$

and, in the case of GL,

$$\mathsf{let}\ \mathsf{box}\ u \Leftarrow \mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ M\ \mathsf{in}\ N \longrightarrow N\left[M\left[\mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ M/z\right]/u\right]$$

Theorem (K., LICS 2017)

The above coincide with the corresponding Hilbert systems, and satisfy the three pillars.

Programming languages and modalities

Consider the closed term

$$\mathsf{ax_K} \stackrel{\text{def}}{=} \lambda f : \Box(A \to B).\ \lambda x : \Box A.\ \text{let box } g \Leftarrow f \text{ in let box } y \Leftarrow x \text{ in box } (g\, y)$$

which has type $\Box(A \to B) \to \Box A \to \Box B$. This satisfies

$$\mathsf{ax_K}\ (\text{box } F)\ (\text{box } M) \longrightarrow^* \text{box } (F\, M) : \Box B$$

If we read

$\text{box } F : \Box(A \to B)$	code F of type $A \to B$
$\text{box } M : \Box A$	code M of type A

then $\mathsf{ax_K}$ takes *code for a function*, and *code for an argument*, and produces *code for its result*. It's **metaprogramming**!
Cf. **subst** : $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ on Gödel numbering:

$$\textbf{subst}\ (\ulcorner \phi(x) \urcorner)\ (\ulcorner t \urcorner) = \ulcorner \phi(t) \urcorner$$

Programming languages and modalities

Consider the closed term

$$\mathsf{ax}_\mathsf{K} \stackrel{\text{def}}{=} \lambda f : \Box(A \to B).\ \lambda x : \Box A.\ \text{let box } g \Leftarrow f \text{ in let box } y \Leftarrow x \text{ in box } (g\,y)$$

which has type $\Box(A \to B) \to \Box A \to \Box B$. This satisfies

$$\mathsf{ax}_\mathsf{K}\ (\text{box } F)\ (\text{box } M) \longrightarrow^* \text{box } (F\,M) : \Box B$$

If we read

$\text{box } F : \Box(A \to B)$	code F of type $A \to B$
$\text{box } M : \Box A$	code M of type A

then ax_K takes *code for a function*, and *code for an argument*, and produces *code for its result*. It's **metaprogramming**!
Cf. **subst** : $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ on Gödel numbering:

$$\textbf{subst}\ (\ulcorner \phi(x) \urcorner)\ (\ulcorner t \urcorner) = \ulcorner \phi(t) \urcorner$$

Programming languages and modalities

Consider the closed term

$$\mathsf{ax_K} \stackrel{\text{def}}{=} \lambda f : \Box(A \to B).\ \lambda x : \Box A.\ \text{let box } g \Leftarrow f \text{ in let box } y \Leftarrow x \text{ in box } (g\, y)$$

which has type $\Box(A \to B) \to \Box A \to \Box B$. This satisfies

$$\mathsf{ax_K}\ (\text{box } F)\ (\text{box } M) \longrightarrow^* \text{box } (F\, M) : \Box B$$

If we read

$\text{box } F : \Box(A \to B)$	code F of type $A \to B$
$\text{box } M : \Box A$	code M of type A

then $\mathsf{ax_K}$ takes *code for a function*, and *code for an argument*, and produces *code for its result*. It's **metaprogramming**!
Cf. **subst** : $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ on Gödel numbering:

$$\textbf{subst}\ (\ulcorner \phi(x) \urcorner)\ (\ulcorner t \urcorner) = \ulcorner \phi(t) \urcorner$$

A metaprogramming example

From Davies and Pfenning (2001):

$$\begin{array}{l} \mathit{power} \equiv \mathbf{fix}\ p{:}\mathsf{nat} \to \Box(\mathsf{nat} \to \mathsf{nat}). \\ \qquad \lambda n{:}\mathsf{nat}.\ \mathbf{case}\ n \\ \qquad\quad \mathbf{of}\ \mathbf{z} \quad \Rightarrow \mathbf{box}\ (\lambda x{:}\mathsf{nat}.\ \mathsf{s}\ \mathbf{z}) \\ \qquad\quad \mid\ \mathsf{s}\ m \Rightarrow \mathbf{let\ box}\ q = p\ m\ \mathbf{in} \\ \qquad\qquad\qquad\qquad \mathbf{box}\ (\lambda x{:}\mathsf{nat}.\ \mathit{times}\ x\ (q\ x)) \end{array}$$

$$\begin{array}{rl} \mathit{power}\ \mathbf{z} & \hookrightarrow \mathbf{box}\ (\lambda x{:}\mathsf{nat}.\ \mathsf{s}\ \mathbf{z}) \\ \mathit{power}\ (\mathsf{s}\ \mathbf{z}) & \hookrightarrow \mathbf{box}\ (\lambda x{:}\mathsf{nat}.\ \mathit{times}\ x\ ((\lambda x{:}\mathsf{nat}.\ \mathsf{s}\ \mathbf{z})x)) \\ \mathit{power}\ (\mathsf{s}\ (\mathsf{s}\ \mathbf{z})) & \hookrightarrow \mathbf{box}\ (\lambda x{:}\mathsf{nat}.\ \mathit{times}\ x \\ & \qquad ((\lambda x{:}\mathsf{nat}.\ \mathit{times}\ x\ ((\lambda x{:}\mathsf{nat}.\ \mathsf{s}\ \mathbf{z})x))x)) \end{array}$$

Programming languages and modalities

Some recent work:

- Ranald Clouston (2018). "Fitch-Style Modal Lambda Calculi". In: *Proceedings of FoSSaCS 2018.* Vol. 10803. Lecture Notes in Computer Science. DOI: 10.1007/978-3-319-89366-2_14. arXiv: 1710.08326. Tense logic!
- Michael Shulman (2018). "Brouwer's fixed-point theorem in real-cohesive homotopy type theory". In: *Mathematical Structures in Computer Science* 28.6, pp. 856–941. DOI: 10.1017/S0960129517000147. arXiv: 1509.07584
- Ranald Clouston et al. (2016). "The guarded lambda calculus: Programming and reasoning with guarded recursion for coinductive types". In: *Logical Methods in Computer Science* 12.3, pp. 1–39. DOI: 10.2168/LMCS-12(3:7)2016
- Neelakantan R. Krishnaswami (2013). "Higher-order functional reactive programming without spacetime leaks". In: *Proceedings of the 18th ACM SIGPLAN international conference on Functional programming - ICFP '13.* ACM. New York, New York, USA: ACM Press, p. 221. DOI: 10.1145/2500365.2500588
- Pierre-Louis Curien, Marcelo Fiore, and Guillaume Munch-Maccagnoni (2016). "A theory of effects and resources: adjunction models and polarised calculi". In: *Proceedings of the 43rd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages - POPL 2016.* New York, New York, USA: ACM Press, pp. 44–56. DOI: 10.1145/2837614.2837652
- Tomas Petricek, Dominic Orchard, and Alan Mycroft (2014). "Coeffects: A calculus of context-dependent computation". In: *Proceedings of the 19th ACM SIGPLAN international conference on Functional programming - ICFP '14*, pp. 123–135. DOI: 10.1145/2628136.2628160
- Andreas Nuyts, Andrea Vezzosi, and Dominique Devriese (Aug. 2017). "Parametric quantifiers for dependent type theory". In: *Proceedings of the ACM on Programming Languages* 1.ICFP. DOI: 10.1145/3110276

Cutting-edge work

Cutting-edge work

- A new multi-modal framework:
  - Daniel R. Licata, Michael Shulman, and Mitchell Riley (2017). "A Fibrational Framework for Substructural and Modal Logics". In: *2nd International Conference on Formal Structures for Computation and Deduction (FSCD 2017)*. Ed. by Dale Miller. Vol. 84. Leibniz International Proceedings in Informatics (LIPIcs). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 25:1–25:22. DOI: 10.4230/LIPIcs.FSCD.2017.25

  Idea: define the *modes* and their *relationship*. *Modalities* (operations that change mode) are then induced.
- An application to language-based security:
  - G. A. Kavvos (2018b). "Modalities, Cohesion, and Information Flow". In: arXiv: 1809.07897 To appear in: POPL 2019.

References I

Abramsky, Samson and Nikos Tzevelekos (2011). “Introduction to Categories and Categorical Logic”. In: *New Structures for Physics*. Ed. by Bob Coecke. Springer-Verlag, pp. 3–94. DOI: 10.1007/978-3-642-12821-9_1. arXiv: 1102.1313.

Bierman, Gavin M. and Valeria de Paiva (1996). *Intuitionistic Necessity Revisited*. Tech. rep. University of Birmingham.

– (2000). “On an Intuitionistic Modal Logic”. In: *Studia Logica* 65.3, pp. 383–416. DOI: 10.1023/A:1005291931660.

Clouston, Ranald (2018). “Fitch-Style Modal Lambda Calculi”. In: *Proceedings of FoSSaCS 2018*. Vol. 10803. Lecture Notes in Computer Science. DOI: 10.1007/978-3-319-89366-2_14. arXiv: 1710.08326.

References II

Clouston, Ranald et al. (2016). "The guarded lambda calculus: Programming and reasoning with guarded recursion for coinductive types". In: *Logical Methods in Computer Science* 12.3, pp. 1–39. DOI: 10.2168/LMCS-12(3:7)2016.

Curien, Pierre-Louis, Marcelo Fiore, and Guillaume Munch-Maccagnoni (2016). "A theory of effects and resources: adjunction models and polarised calculi". In: *Proceedings of the 43rd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages - POPL 2016.* New York, New York, USA: ACM Press, pp. 44–56. DOI: 10.1145/2837614.2837652.

Davies, Rowan and Frank Pfenning (2001). "A modal analysis of staged computation". In: *Journal of the ACM* 48.3, pp. 555–604. DOI: 10.1145/382780.382785.

Girard, Jean-Yves, Yves Lafont, and Paul Taylor (1989). *Proofs and Types.* Cambridge University Press.

References III

- Graham-Lengrand, Stéphane (2015). "The Curry-Howard view of classical logic". In:
- Hakli, Raul and Sara Negri (2012). "Does the deduction theorem fail for modal logic?" In: *Synthese* 187.3, pp. 849–867. DOI: 10.1007/s11229-011-9905-9.
- Howard, William A (1980). "The formulae-as-types notion of construction". In: *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*. Ed. by Jonathan P. Seldin and J. Roger Hindley. Boston, MA: Academic Press, pp. 479–490.
- Kavvos, G. A. (2016). "The Many Worlds of Modal Lambda Calculi: I. Curry-Howard for Necessity, Possibility and Time". In: *CoRR*. arXiv: 1605.08106.
- – (Aug. 2018a). "Dual-Context Calculi for Modal Logic". In: *CoRR*. arXiv: 1602.04860.

References IV

Kavvos, G. A. (2018b). "Modalities, Cohesion, and Information Flow". In: arXiv: 1809.07897.

Kripke, Saul A. (1963). "Semantical Analysis of Modal Logic I. Normal Modal Propositional Calculi". In: *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik* 9.5-6, pp. 67–96. DOI: 10.1002/malq.19630090502.

Krishnaswami, Neelakantan R. (2013). "Higher-order functional reactive programming without spacetime leaks". In: *Proceedings of the 18th ACM SIGPLAN international conference on Functional programming - ICFP '13.* ACM. New York, New York, USA: ACM Press, p. 221. DOI: 10.1145/2500365.2500588.

References V

Licata, Daniel R., Michael Shulman, and Mitchell Riley (2017). "A Fibrational Framework for Substructural and Modal Logics". In: *2nd International Conference on Formal Structures for Computation and Deduction (FSCD 2017)*. Ed. by Dale Miller. Vol. 84. Leibniz International Proceedings in Informatics (LIPIcs). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 25:1–25:22. DOI: 10.4230/LIPIcs.FSCD.2017.25.

Martin-Löf, Per (1996). "On the meanings of the logical constants and the justification of the logical laws". In: *Nordic Journal of Philosophy* 1.1, pp. 11–60.

Nordström, Bengt, Kent Petersson, and Jan M. Smith (1990). *Programming in Martin-Löf's Type Theory: an Introduction*. Oxford University Press. DOI: 10.1016/0377-0427(91)90052-L.

Nuyts, Andreas, Andrea Vezzosi, and Dominique Devriese (Aug. 2017). "Parametric quantifiers for dependent type theory". In: *Proceedings of the ACM on Programming Languages* 1.ICFP. DOI: 10.1145/3110276.

References VI

- Petricek, Tomas, Dominic Orchard, and Alan Mycroft (2014). "Coeffects: A calculus of context-dependent computation". In: *Proceedings of the 19th ACM SIGPLAN international conference on Functional programming - ICFP '14*, pp. 123–135. DOI: 10.1145/2628136.2628160.
- Pfenning, Frank and Rowan Davies (2001). "A judgmental reconstruction of modal logic". In: *Mathematical Structures in Computer Science* 11.4, pp. 511–540. DOI: 10.1017/S0960129501003322.
- Prawitz, Dag (1965). *Natural Deduction: a proof-theoretical study.* Almquist and Wiksell.
- – (1971). "Ideas and Results in Proof Theory". In: *Proceedings of the Second Scandinavian Logic Symposium.* Ed. by J. E. Fenstad. Vol. 63. Studies in logic and the foundations of mathematics. Amsterdam: North-Holland.

References VII

Shulman, Michael (2018). "Brouwer's fixed-point theorem in real-cohesive homotopy type theory". In: *Mathematical Structures in Computer Science* 28.6, pp. 856–941. DOI: 10.1017/S0960129517000147. arXiv: 1509.07584.

Sørensen, Morten Heine and Pawel Urzyczyn (2006). *Lectures on the Curry-Howard Isomorphism.* Elsevier.

Tait, W. W. (1967). "Intensional Interpretations of Functionals of Finite Type I". In: *Journal of Symbolic Logic* 32.2, pp. 198–212.