Dual-Context Calculi for Modal Logic

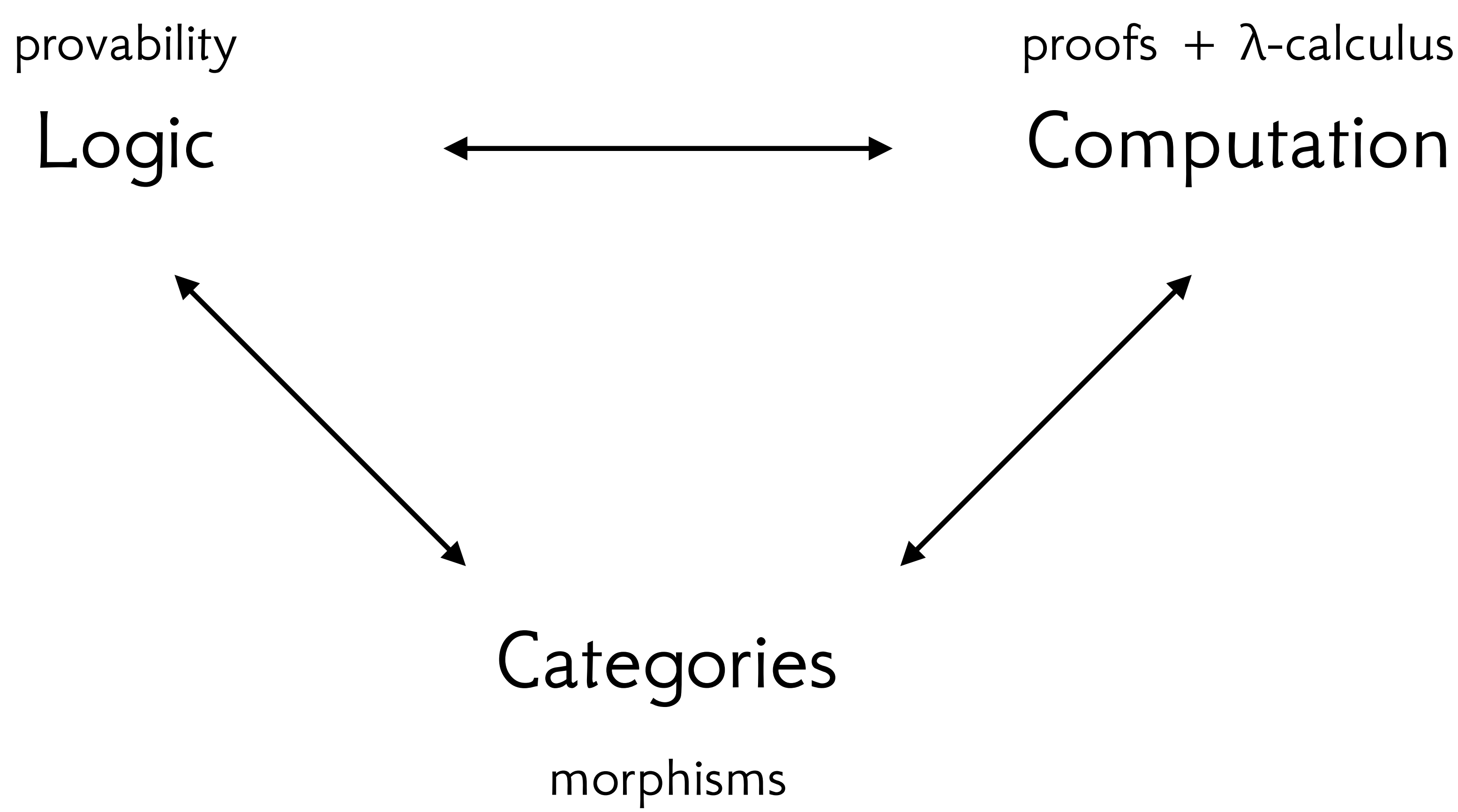
Alex Kavvos

Department of Computer Science, University of Oxford

LICS 2017, 21 June 2017

arXiv:1602.04860

The Curry-Howard-Lambek Correspondence



How does it work for **modal logic**?

What does that tell us about programming and computation?

Curry-Howard for modalities

- Far from trivial — far too many formulations.
- See the survey: arXiv:1605.08106. Main strands:
  - Box modalities: K, S4, GL, ... $\Box$
  - Diamond modalities: for all of the above $\Diamond$
  - PLL/CL (Moggi)
  - some variants of Constructive Linear Temporal Logic $\bigcirc$
- PLL/CL (effects), S4 and CLTL (metaprogramming) most used.
- This talk: demystifying box fragment, through **dual contexts**.

The Logics in Question

- A standard Hilbert system:

$$\frac{}{\Gamma, A \vdash A}\,(assn) \qquad \frac{A \text{ is an axiom}}{\Gamma \vdash A}\,(ax)$$

$$\frac{\Gamma \vdash A \to B \quad \Gamma \vdash A}{\Gamma \vdash B}\,(MP) \qquad \frac{\vdash A}{\Gamma \vdash \Box A}\,(NEC)$$

- plus axioms for intuitionistic propositional logic, and:

$$\Box(A \to B) \to \Box A \to \Box B \longrightarrow \mathsf{K}$$

$$\Box A \to \Box\Box A \longrightarrow \mathsf{K4},\ \mathsf{S4}$$

$$\Box A \to A \longrightarrow \mathsf{S4},\ \mathsf{T}$$

$$\Box(\Box A \to A) \to \Box A \longrightarrow \mathsf{GL}$$

K4

S4

T

GL

Dual contexts

- Dual context systems:
  - a kind of natural deduction with **two contexts**
  - introduced by Girard, developed by many over the 90s
- Judgments:

intuitionistic assumptions

$$\Delta\,;\Gamma \vdash A$$

modal assumptions

E.g. introduction rule for S4:

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

An idea: sequent calculus...

- Developed by Gentzen in the 1930s to study normalisation of proofs.

$$A_1, \ldots, A_n \vdash B$$

- Two kinds of rules:
  - right rules: introduce a connective on the right of $\vdash$
    => introduction rules in natural deduction
  - left rules: 'gerrymandering' with assumptions, left of $\vdash$
    => elimination rules in natural deduction (upside down)
- First attempts at modalities: 1950s.
  E.g. Intuitionistic S4, right modality rule:

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

From sequent calculi to dual contexts

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

They look very similar.

Interpret this way:

$$\Delta\,;\Gamma \vdash A \qquad \Longrightarrow \qquad \Box\Delta, \Gamma \vdash A$$

then we see that

INTRODUCTION RULE = RIGHT RULE + WEAKENING

From s.c. to d.c.

K, T

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

K4

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

GL

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

S4

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

Surely, that's not all!

True. The cases of T and S4 also have a left rule:

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

"If A is enough to infer B, then $\Box$A is more than enough."

For this, we need **another assumption/variable rule:**

$$\frac{}{\Delta, A\,; \Gamma \vdash A}$$

The Elimination Rule

- Common to all dual context systems,

ELIMINATION = CUT FOR MODAL CONTEXT

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

- Unfortunate that we have to include any form of cut rule...
- ...but this uniformly works, for all of the systems considered.
- **Slogan:**

  Let the introduction rule govern the behaviour of the modality.

Dual context λ-calculi

A simple annotation of the derivation with a **proof term**, which essentially represents the entire derivation. E.g. for conjunction:

$$\dfrac{\dfrac{\vdots}{\Delta\,;\Gamma \vdash A} \qquad \dfrac{\vdots}{\Delta\,;\Gamma \vdash B}}{\Delta\,;\Gamma \vdash A \wedge B} \quad \longrightarrow \quad \dfrac{\dfrac{\vdots}{\Delta\,;\Gamma \vdash M : A} \qquad \dfrac{\vdots}{\Delta\,;\Gamma \vdash N : B}}{\Delta\,;\Gamma \vdash \langle M, N\rangle : A \times B}$$

Likewise, for, say, K:

$$\dfrac{\dfrac{\vdots}{\cdot\,;\Delta \vdash A}}{\Delta\,;\Gamma \vdash \Box A} \quad \longrightarrow \quad \dfrac{\dfrac{\vdots}{\cdot\,;\Delta \vdash M : A}}{\Delta\,;\Gamma \vdash \text{box } M : \Box A}$$

Dual context λ-calculi

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

Careful! Watch out for commuting conversions.

- Introduction rule: box construct.
- Elimination rule: a form of **explicit substitution**
- Dynamics: $\mathsf{let\ box}\ u \Leftarrow \mathsf{box}\ M\ \mathsf{in}\ N \longrightarrow N[M/u]$

THEOREM. The five resulting systems (K, K4, T, S4, GL) satisfy **subject reduction**, are **confluent** and **strongly normalising**. Up to some commuting conversions, they also satisfy the **subformula property**.

The problem with K4 & GL

- Annotating $\dfrac{\Delta\,;\Delta \vdash A}{\Delta\,;\Gamma \vdash \Box A}$ naïvely yields $\dfrac{\Delta\,;\Delta \vdash M : A}{\Delta\,;\Gamma \vdash \text{box } M : \Box A}$
- Then all the variables in the two contexts clash!
- **Solution**: Introduce an **involution** $(-)^{\perp} : \mathcal{V} \xrightarrow{\cong} \mathcal{V}$ between variables: $x \text{ modal} \longleftrightarrow x^{\perp} \text{ intuitionstic}$
- Self-inverse: makes some proofs easier.
- Also acts on contexts & terms!
- Final form of the rule:

$$\frac{\Delta\,;\Delta^{\perp} \vdash M^{\perp} : A}{\Delta\,;\Gamma \vdash \text{box } M : \Box A}$$

Categorical Semantics

- Simple and effective; based on the notion of a **strong monoidal (= product-preserving) endofunctor** on a CCC (with $\otimes = \times$;"strongness" required even for the β rule).
- Semantics of K4, T = "half a comonad"
- Semantics of S4 = product-preserving comonad
- Semantics of GL: complicated (modal fixed points)
- All sound — see the technical report on lambdabetaeta.eu
- Completeness verified for K, K4, T.

Some open questions

- Does this also work for diamond modalities?
- Is there a general structural theorem we can prove here?
- What is the computational interpretation/application?
  Idea: modalities control the flow of data.
  E.g. K = the logic of "homomorphic encryption"
- Initiality theorems?

Thank you.