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

provability
Logic

proofs + λ-calculus
Computation

Categories
morphisms

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, ...
  - Diamond modalities: for all of the above
  - PLL/CL (Moggi)
  - some variants of Constructive Linear Temporal Logic
  - 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:
  \[
  \frac{\Gamma, A \vdash A}{\Gamma, A \vdash A} \quad \text{(assn)}
  \]
  \[
  \frac{\Gamma \vdash A \rightarrow B, \Gamma \vdash A}{\Gamma \vdash B} \quad \text{(MP)}
  \]
  \[
  \frac{\vdash A}{\Gamma \vdash \Box A} \quad \text{(NEC)}
  \]

- plus axioms for intuitionistic propositional logic, and:
  \[
  \Box(A \rightarrow B) \rightarrow \Box A \rightarrow \Box B \quad \text{K}
  \]
  \[
  \Box A \rightarrow \Box \Box A \quad \text{K4}
  \]
  \[
  \Box A \rightarrow A \quad \text{S4}
  \]
  \[
  \Box(\Box A \rightarrow A) \rightarrow \Box A \quad \text{T}
  \]
  \[
  \Box(\Box A \rightarrow A) \rightarrow \Box A \quad \text{GL}
  \]
Dual contexts

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

- Judgments:
  - $\Delta ; \Gamma \vdash A$
    - intuitionistic assumptions
    - modal assumptions

E.g. introduction rule for S4: 

\[
\Delta ; \cdot \vdash A \\
\Delta ; \Gamma \vdash \Box A
\]
An idea: sequent calculus...

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

- 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:
  \[
  \square \Gamma \vdash A, \quad \square \Gamma \vdash \square A
  \]
From sequent calculi to dual contexts

\[
\frac{\Box \Gamma \vdash A}{\Box \Gamma \vdash \Box A} \quad \frac{\Delta ; \cdot \vdash A}{\Delta ; \Gamma \vdash \Box A}
\]

They look very similar.

Interpret this way:

\[
\Delta ; \Gamma \vdash A \implies \Box \Delta, \Gamma \vdash A
\]

then we see that

\[
\text{INTRODUCTION RULE} = \text{RIGHT RULE} + \text{WEAKENING}
\]
From s.c. to d.c.

K, T

\[ \begin{align*}
\Gamma \vdash A & \quad \therefore \Delta ; \Gamma \vdash A \\
\square \Gamma \vdash \square A & \quad \Delta ; \Gamma \vdash \square A \\
\square \Gamma, \Gamma \vdash A & \quad \Delta ; \Delta \vdash A \\
\square \Gamma \vdash \square A & \quad \Delta ; \Gamma \vdash \square A
\end{align*} \]

K4

\[ \begin{align*}
\square \Gamma, \Gamma \vdash A & \quad \Delta ; \Delta, \square A \vdash A \\
\square \Gamma \vdash \square A & \quad \Delta ; \Gamma \vdash \square A
\end{align*} \]

GL

\[ \begin{align*}
\square \Gamma, \Gamma, \square A \vdash A & \quad \Delta ; \Delta, \square A \vdash A \\
\square \Gamma \vdash \square A & \quad \Delta ; \Gamma \vdash \square A
\end{align*} \]

S4

\[ \begin{align*}
\square \Gamma \vdash A & \quad \Delta ; \cdot \vdash A \\
\square \Gamma \vdash \square A & \quad \Delta ; \Gamma \vdash \square A
\end{align*} \]
Surely, that’s not all!

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

\[
\Gamma, A \vdash B \\
\Gamma, \Box A \vdash B
\]

“If A is enough to infer B, then \(\Box A\) is more than enough.”

For this, we need another assumption/variable rule:

\[
\Delta, A; \Gamma \vdash A
\]
The Elimination Rule

• Common to all dual context systems,

ELIMINATION = CUT FOR MODAL CONTEXT

\[ \Delta ; \Gamma \vdash \Box A \quad \Delta, A; \Gamma \vdash C \]

\[ \Delta ; \Gamma \vdash C \]

• 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 $\lambda$-calculi

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

\[
\begin{array}{c}
\Delta; \Gamma \vdash A \\
\Delta; \Gamma \vdash B \\
\hline
\Delta; \Gamma \vdash A \land B
\end{array}
\]

\[
\begin{array}{c}
\Delta; \Gamma \vdash M : A \\
\Delta; \Gamma \vdash N : B \\
\hline
\Delta; \Gamma \vdash \langle M, N \rangle : A \times B
\end{array}
\]

Likewise, for, say, $K$:

\[
\begin{array}{c}
\therefore; \Delta \vdash A \\
\hline
\Delta; \Gamma \vdash \Box A
\end{array}
\]

\[
\begin{array}{c}
\therefore; \Delta \vdash M : A \\
\hline
\Delta; \Gamma \vdash \text{box } M : \Box A
\end{array}
\]
Dual context $\lambda$-calculi

\[
\begin{align*}
\text{• Introduction rule: box construct.} \\
\text{• Elimination rule: a form of explicit substitution} \\
\text{• Dynamics: let box } u \leftarrow \text{box } M \text{ in } N \rightarrow N[M/u]
\end{align*}
\]

**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 \( \Gamma, \Delta \vdash A \) na"ively yields \( \Gamma, \Delta \vdash \Box A \)

- Then all the variables in the two contexts clash!

- **Solution**: Introduce an **involution** \((-\)\): \(\forall \mapsto \forall\)
  between variables: \(x\) modal \(\longleftrightarrow\) \(x^{\perp}\) intuitionistic

- Self-inverse: makes some proofs easier.

- Also acts on contexts & terms!

- Final form of the rule:
  \[
  \Gamma, \Delta \vdash M^{\perp} : A \\
  \Delta, \Gamma \vdash \Box M : \Box A
  \]
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 $\beta$ 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.