Dual-Context Calculi for Modal Logic

G. A. Kavvos
Department of Computer Science
University of Oxford
Email: alex.kavvos@cs.ox.ac.uk

***Abstract*—We show how to derive natural deduction systems for the necessity fragment of various constructive modal logics by exploiting a pattern found in sequent calculi. The resulting systems are dual-context systems, in the style pioneered by Girard, Barber, Plotkin, Pfenning, Davies, and others. This amounts to a full extension of the Curry-Howard-Lambek correspondence to the necessity fragments of a constructive variant of the modal logics K, $\mathsf{K4}$, GL, T, and $\mathsf{S4}$. We investigate the metatheory of these calculi, as well as their categorical semantics. Finally, we speculate on their computational interpretation.**

I. Introduction

The study of modal λ-calculi, and the modal logics associated with them through the Curry-Howard correspondence [1]–[3] began at the dawn of the 1990s, heralded by the developments in Linear Logic. Early milestones include Moggi's *monadic metalanguage* [4], and the discovery of a constructive $\mathsf{S4}$ modality by [5]. This was followed by an explosion of developments, as well as some first applications. This era is surveyed by [6]. Since the early 2000s this field has been commandeered by the programming language community, see e.g. [7]–[10].

The major issue with modal proof theory is that its methods are, at their best, kaleidoscopic: some types of calculi seem to work better for certain logics, but fail to suit others. It is easy to develop an intuition about these patterns, but it is much harder to explain why a particular pattern suits a particular modal logic.

In the sequel we propose an explanation that clarifies why the necessity fragments of the most popular normal modal logics—namely K, T, $\mathsf{K4}$, GL and $\mathsf{S4}$—are best suited to *dual-context calculi*, as pioneered by [11]–[18]. The crux of the argument is that separating assumptions into a modal zone and an intuitionistic zone allows one to 'mimic' rules from known cut-free sequent calculi for these logics.

Our investigation is structured as follows. We first define and discuss the the aforementioned constructive modal logics, and present a Hilbert system for each. We then show how to systematically derive dual-context calculi from sequent calculi, and we study the metatheory of the five resulting systems, as well as a notion of reduction. The addition of a few commuting conversions also yields the subformula property. Finally, we develop the category theory necessary to model these calculi, and discover sound categorical semantics for them.

Our contribution is twofold. On the theoretical side, it amounts to a full extension of the *Curry-Howard-Lambek isomorphism*—based on the usual triptych of *logic*, *computation* and *categories*—to a handful of modal logics. Indeed, only fragments of our dual-context formulations have appeared before. The original formulation of dual-context $\mathsf{S4}$ belongs to Davies and Pfenning [18], who introduced dual contexts to modal logic. However, their work mostly concerned the type system and its applications to binding-time analysis, and they did not discuss reduction in depth. An approach that is similar in shape to ours for K and $\mathsf{K4}$ was presented by Frank Pfenning at the LFMTP '15 workshop [19] in the context of a *linear sequent calculus for K*, which seems to be closely related to the work of [20] in *elementary linear logic*. However, the natural deduction formulation of the (cartesian) modal version, as well as the technical innovations regarding the term calculus that are needed for $\mathsf{K4}$ and GL, are new. The only previous work on $\mathsf{K4}$ and GL was the rather complicated (non-dual) natural deduction calculus of Bellin [21], and the appreciably simpler dual-context formulations are presented here for the first time. Finally, the approach to T is entirely new. The reader is invited to consult the survey [22] for a more detailed history of the literature on modal λ-calculi.

On the other hand, the results in this paper are also meant to provide a solid foundation for applications in programming languages. Necessity modalities are a way to *control data flow* within a programming language. As such, a clear view of the landscape can help one pick the appropriate modal axioms to ensure some desired correctness property.

Before we proceed any further, let us mention that the full proofs for the present paper can be found in the accompanying technical report, available on the author's website.[1] In addition, the author has formalized most of the metatheoretic results in AGDA. The proofs are available either from his website, or his GitHub repository.[2]

II. The Logics in Question

In the sequel we will study the necessity fragment of five modal logics: constructive K (abbrv. CK), constructive $\mathsf{K4}$ (abbrv. $\mathsf{CK4}$), constructive T (abbrv. CT), constructive GL

The final version of this article is published by IEEE. Citation: DOI 10.1109/LICS.2017.8005089, 2017 32nd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)

978-1-5090-3018-7/17/$31.00

[1] www.lambdabetaeta.eu
[2] lambdabetaeta/modal-logics

(abbrv. CGL), and constructive S4 (abbrv. CS4). In this section we shall discuss the common characteristics amongst these logics, define their syntax, and present a Hilbert system for each.

A. Constructive Modal Logics

All of the above logics belong to a group of logics that are broadly referred to as *constructive modal logics*. These are intuitionistic variants of known modal logics which have been cherry-picked to satisfy a specific desideratum, namely to have a well-behaved Gentzen-style proof theory, and thereby an associated computational interpretation through the Curry-Howard isomorphism.

There are a few characteristics common to all these logics, which are rather more appreciable when the possibility modality ($\Diamond$) is taken into consideration: the de Morgan duality between $\Box$ and $\Diamond$ breaks down, rendering those two modalities logically independent. For that reason we shall mostly refer to the $\Box$ as the *box* modality, and $\Diamond$ as the *diamond* modality. Second, the principles $\Diamond(A \vee B) \to \Diamond A \vee \Diamond B$ and $\neg\Diamond\bot$ are not provable. (Recall that these two principles are tautologies if we employ traditional Kripke semantics [23].) But even if the diamond modality is essential in pinpointing the salient differences between constructive modal logics and other forms of intuitionistic modal logic (e.g. [24]), it seems that its computational interpretation is not very crisp: the only application we know of is that of Pfenning [25]. Hence, we restrict our study to the more well-behaved box modality.

B. Hilbert Systems

The formulae of our logics are generated by the following Backus-Naur form:

$$A, B \quad ::= \quad p_i \mid \bot \mid A \wedge B \mid A \vee B \mid A \to B \mid \Box A$$

where p_i is drawn from a countable set of propositions. First, we introduce a judgment of the form $\Gamma \vdash A$, where Γ is a *context*, i.e. a list of formulae defined by the BNF

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

and A is a single formula. We shall use the comma to also denote concatenation—e.g. Γ, A, Δ shall mean the concatenation of three things: the context Γ, the context consisting of the single formula A, and the context Δ.

The judgment $\Gamma \vdash A$ is meant to be read as "from assumptions Γ, we infer A." The complete rules for generating $\Gamma \vdash A$, including the carefully-stated *rule of necessitation* for the box modality (for which see [26]), may be found in Figure 1.

C. Axioms

To obtain the aforementioned logics, all we need to do is vary the set of axioms. We write

$$(A_1) \oplus \cdots \oplus (A_n)$$

to mean the set of theorems A such that $\vdash A$ is derivable from all instances of the axiom schemata $(A_1), \ldots, (A_n)$ under the rules in Figure 1. We write $(\mathsf{IPL}_\Box)$ to mean all instances of the axioms of intuitionistic propositional logic, but also including formulas of the form $\Box A$ in the syntax. We will use the following axiom schemata:

Fig. 1. Hilbert systems

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

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

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

We then define the following logics:

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

To indicate that we are using the Hilbert system for e.g. CK, we annotate the turnstile, and write $\Gamma \vdash_{\mathsf{CK}} A$. We simply write $\Gamma \vdash A$ when the statement under discussion pertains to all of our Hilbert systems.

There are many interesting metatheoretic results about the above systems, including the admissibility of various structural and modal inference rules, but they are beyond the scope of the paper.

III. From Sequent Calculi to Dual Contexts

A. The Perennial Issues

In this section we discuss the issues that one has to tackle time and time again whilst devising modal λ-calculi for necessity modalities.

A brief perusal of the survey [22] indicates that most work in the subject is concentrated on the analysis of essentially two kinds of calculi: (a) those with *explicit substitutions*, following a style that was popularised by [5]; and (b) those employing *dual contexts*, a pattern that was imported into modal type theory by [17], [18].

Calculi with explicit substitutions suffer from multiple problems, mostly because they feature introduction rules for the modality which also partially function as cut rules. This is rather harmful when it comes to proof-theoretic *harmony*, and in all cases weaker than S4 this pattern breaks down the duality between introduction and elimination. Decoupling the introduction and cut aspect of these rules is essential for overcoming these problems.

The right intuition for achieving this 'decoupling' was introduced by Girard [11] in his attempt to combine classical, intuitionistic, and linear logic in one system. The gist of the idea is simple and can be turned into a slogan: *segregate assumptions*. This means that we should divide our usual context of assumptions in two, or—even better—think of it as consisting of *two zones*. We should think of one zone as the *primary zone*, and the assumptions occuring in it as the 'ordinary' sort of assumptions. The other zone is the *secondary zone*, and the assumptions in it normally have a different flavour. In this context, the introduction rule explains the interaction between the two contexts, whereas the elimination rule effects substitution for the secondary context.

This idea has been most profitable in the case of the *Dual Intuitionistic Linear Logic (DILL)* of [15], [16], where the primary context consists of *linear* assumptions, whereas the secondary consists of ordinary *intuitionistic* assumptions. The 'of course' modality (!) of Linear Logic is very much like a S4 modality, and—simply by lifting the linearity restrictions—[17], [18] adapted the work of Barber and Plotkin to the modal logic CS4 with considerable success. In this system, hereafter referred to as *Dual Constructive S4* (DS4), the primary context consists of intuitionistic assumptions, whereas the secondary context consists of *modal* assumptions.

However, the systems of Barber, Plotkin, Davies and Pfenning do not immediately seem adaptable to other logics. Indeed, the pattern may at first seem limited to modalities like 'of course' and the necessity of S4, which—categorically—are *comonads*. Recall that a comonad can be decomposed into an adjunction, which satisfies a *universal property*, and it may seem that the syntax heavily depends on that.

In the rest of this section we argue that, not only does the dual-context pattern not depend on this universal property at all, but that it can easily be adapted to capture the necessity fragments of all the other aforementioned logics.

B. Deriving dual-context calculi

We shall start with the usual suspect, namely the *sequent calculus*. Gentzen introduced the sequent calculus in the 1930s [27], [28] in order to study normalisation of proofs, known as *cut elimination* in this context; see [2] for an introduction.

Proofs in the sequent calculus consist of trees of *sequents*, which take the form $\Gamma \vdash A$, where Γ is a context. Thus in our notation a sequent is a different name for a judgment, like the ones of natural deduction.[3] The rules, however, are different, and they come in two flavours: *left rules* and *right rules*. Broadly speaking, right rules are exactly the introduction rules of natural deduction, as they only concern the conclusion A of the sequent. The left rules play a role similar to that of elimination rules, but they do so by 'gerrymandering' with the assumptions in Γ.

[3]Fundamental differences arise in the case of *classical logics*, where sequents are of the form $\Gamma \vdash \Delta$ where both Γ and Δ are lists of formulae. For the purposes of intuitionistic logic Δ consists of at most one formula—see [2, §5.1.3].

1) The Introduction Rules: Let us consider the right rule for the logic S4. In the intuitionistic case, the rule is

$$\frac{\Box\Gamma \vdash A}{\Box\Gamma \vdash \Box A}\,(\Box\mathcal{R})$$

One cannot help but notice this rule has an intuitive computational interpretation, in terms of 'flow of data.' We can read it as follows: if only modal data are used in inferring A, then we may safely obtain $\Box A$. Only 'boxed' things can flow into something that is 'boxed.'

Let us now take a closer look at dual-context systems for box modalities. A dual-context judgment is of the form

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

where both Δ and Γ are contexts. The assumptions in Δ are to be thought of as *modal*, whereas the assumptions in Γ are run-of-the-mill intuitionistic assumptions. A loose translation of a judgment of this form to the 'ordinary sort' would be

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

Under this translation, if we 'mimic' the right rule for S4 we would obtain the following:

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

where $\cdot$ denotes the empty context. However, natural deduction systems do not have any structural rules, so we have to include some kind of 'opportunity to weaken the context' in the above rule. If we do so, the result is

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

Under the translation described above, this is exactly the right rule for S4, weakening included. Incidentally, it is also exactly the introduction rule of [17] for their dual-context system DS4.

This pattern can actually be harvested to turn the right rules for box in sequent calculi to introduction rules in dual-context systems. We proceed to tackle each case separately, except T, which we discuss in §III-B6

2) K: The case for K is slightly harder to fathom at first sight. This is because its sequent calculus only has a single rule for the modality, which is known as *Scott's rule*:

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

As [29] discuss, this rule fundamentally unsavoury: it is both a left and a right rule at the same time. It cannot be split into two rules, which is the pattern that bestows sequent calculus its fundamental symmetries. Despite this, Scott's rule is reasonably well-behaved: see [30]–[32].

With the previous interpretation in mind, our introduction rule should take the following form:

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

Indeed, we emulate Scott's rule by ensuring that *all the intuitionistic assumptions become modal, at once*. The final form is reached again by adding opportunities for weakening:

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

3) K4: The right sequent calculus rule for the logic K4, as well as the proof of cut elimination, is due to Sambin and Valentini [33]. Using elements from his joint work with Sambin, as well some counterexamples found in the work of [30] on GL, Valentini's key observation is that, due to axiom 4, anything derivable from $\Box\Box A$ is derivable by $\Box A$. The (single) rule for the modality encapsulates this insight:

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

Thus, to derive $\Box A$ from a bunch of boxed assumptions, it suffices to derive A from two copies of the same assumptions, one boxed and one unboxed. A direct translation, after adding opportunities for weakening, amounts to the introduction rule:

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

4) GL: The correct formulation of sequent calculus for GL is a difficult problem that receives attention time and time again; see [34] for a recent approach. The *Leivant-Valentini* sequent calculus rule for GL [33] is this:

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

The only difference between this rule and the one for K4 is the appearance of the 'diagonal assumption' $\Box A$. We can straightforwardly use our translation to state it as an introduction rule:

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

5) The Elimination Rule: As discussed before, in a dual-context calculus we can consider one of these zones to be *primary*, and the other *secondary*, depending of course on our intentions. Assumptions in the primary zone are discharged by λ-abstraction. Thus, the function space of DILL is linear, whereas the function space of DS4 is intuitionistic. This mechanism provides for internal substitution for an assumption, by first λ-abstracting it and then applying the resulting function to an argument.

In contrast, substituting for assumptions in the secondary zone is the capacity of the *elimination rule*. This is a customary pattern for dual-context calculi: unlike primary assumptions, substitution for secondary assumptions is essentially a *cut rule*. In the term assignment system we will consider later, this takes the form of an *explicit substitution*, a type of 'let construct.' The rationale is this: the rest of the system controls how secondary assumptions arise and are used, and the elimination rule uniformly allows one to substitute for them.[4] To wit:

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

A lot of cheek is involved in trying to pass a cut rule as an elimination rule. Notwithstanding the hypocrisy, this is not only common, but also the best presently known solution to regaining the patterns of introduction/elimination in the presence of modality. It is the core of our second slogan: *in dual-context systems, substitution is a cut rule for secondary assumptions*.

6) A second variable rule: We have conveniently avoided discussing two things up to this point: (a) the left rule for $\Box$ in S4, which is the only one of our logics that has both left and right rules, and (b) the case of T. These two are intimately related.

The left rule for the box in S4 is

$$\frac{\Gamma, A \vdash B}{\Gamma, \Box A \vdash B}\ (\Box\mathcal{L})$$

We can intuitively read it as follows: if A suffices to infer B, then $\Box A$ is more than enough to infer B. It is not hard to see that this encapsulates the T axiom, namely $\Box A \to A$. This rule, put together with Scott's rule, form a sequent calculus where cut is admissible; this is mentioned by [35] and attributed to [36].

One way of emulating this rule in our framework would be to have a construct that makes an assumption 'jump' from one context to another, but that is inelegant and probably unworkable. We are in natural deduction, and we have two kinds of assumptions: modal and intuitionistic. The way to imitate the above is to include a rule that allows one to use a *modal* assumption as if it were merely intuitionistic. To wit:

$$\frac{}{\Delta, A, \Delta'\,;\Gamma \vdash A}\ (\Box\mathsf{var})$$

This translates back to the sequent $\Box\Delta, \Box A, \Box\Delta', \Gamma \vdash A$.

A rule like this was introduced by [15], [16] for *dereliction* in DILL, and was also essential in Davies and Pfenning's DS4. In our case, we use it in combination with the introduction rule for K in order to make a system for T.

IV. Terms, Types & Metatheory

In this section we collect all the observations we have made in order to turn our natural deduction systems into term assignment systems, i.e. typed λ-calculi. First, we annotate each assumption A with a variable, e.g. $x : A$. Then, we annotate each judgment $\Delta\,;\Gamma \vdash A$ with a term M reprsenting the entire deduction that with that judgment as its conclusion—see [2, §3] or [3], [37] for an introduction. We omit a treatment of $\vee$, for it is largely orthogonal.

[4]Alternative approaches have also been considered. For example, one could introduce another abstraction operator, i.e. a 'modal λ.' This has been adopted by [25], in a dependently-typed setting.

Fig. 2. Definition and Typing Judgments

$$\textbf{Types} \quad A, B \quad ::= \quad p_i \mid A \times B \mid A \to B \mid \Box A$$

$$\textbf{Typing Contexts} \quad \Gamma, \Delta \quad ::= \quad \cdot \mid \Gamma, x{:}A$$

$$\begin{array}{rlll} \textbf{Terms} & M, N & ::= & x \mid \lambda x{:}A.\ M \mid MN \mid \langle M, N \rangle \\ & & & \mid \pi_1(M) \mid \pi_2(M) \\ & & & \mid \mathsf{box}\ M \mid \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N \\ & & & \mid \mathsf{fix}\ z\ \mathsf{in\ box}\ M \end{array}$$

Rules for all calculi:

$$\frac{}{\Delta\,;\Gamma, x{:}A, \Gamma' \vdash x : A}\ (\mathsf{var})$$

$$\frac{\Delta\,;\Gamma \vdash M : A \quad \Delta\,;\Gamma \vdash N : B}{\Delta\,;\Gamma \vdash \langle M, N \rangle : A \times B}\ (\times\mathcal{I})$$

$$\frac{\Delta\,;\Gamma \vdash M : A_1 \times A_2}{\Delta\,;\Gamma \vdash \pi_i\,(M) : A_i}\ (\times\mathcal{E}_i)$$

$$\frac{\Delta\,;\Gamma, x{:}A \vdash M : B}{\Delta\,;\Gamma \vdash \lambda x{:}A.\ M : A \to B}\ (\to\mathcal{I})$$

$$\frac{\Delta\,;\Gamma \vdash M : A \to B \quad \Delta\,;\Gamma \vdash N : A}{\Delta\,;\Gamma \vdash MN : B}\ (\to\mathcal{E})$$

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

Rules for K, $\mathsf{K4}$, GL:

$$\frac{\cdot\,;\Delta \vdash M : A}{\Delta\,;\Gamma \vdash \mathsf{box}\ M : \Box A}\ (\Box\mathcal{I}_{\mathsf{K}})$$

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

$$\frac{\Delta\,;\Delta^{\perp}, z^{\perp} : \Box A \vdash M^{\perp} : A}{\Delta\,;\Gamma \vdash \mathsf{fix}\ z\ \mathsf{in\ box}\ M : \Box A}\ (\Box\mathcal{I}_{\mathsf{GL}})$$

Rules for $\mathsf{S4}$:

$$\frac{}{\Delta, u{:}A, \Delta'\,;\Gamma \vdash u : A}\ (\Box\mathsf{var})$$

$$\frac{\Delta\,;\cdot \vdash M : A}{\Delta\,;\Gamma \vdash \mathsf{box}\ M : \Box A}\ (\Box\mathcal{I}_{\mathsf{S4}})$$

Rules for T: $(\Box\mathcal{I}_{\mathsf{K}})$ and $(\Box\mathsf{var})$

The grammars defining types, terms and contexts, as well as the typing rules for all our systems can be found in Figure 2. When we are at risk of confusion, we annotate the turnstile with a subscript to indicate which system we are referring to; e.g. $\Delta\,;\Gamma \vdash_{\mathsf{DGL}} M : A$ refers to the system consisting of the rules pertaining to all our calculi coupled with the introduction rule $(\Box\mathcal{I}_{\mathsf{GL}})$.

From this point onwards, we assume Barendregt's conventions: terms are identified by α-conversion, and bound variables are silently renamed whenever necessary. In $\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N$, u is a bound variable in N. Finally, we write $N[M/x]$ to indicate capture-avoiding substitution of M for x in N.

Furthermore, we shall assume that whenever we write a judgment like $\Delta\,;\Gamma \vdash M : A$, then Δ and Γ are *disjoint*, in the sense that $\textsc{Vars}\,(\Delta) \cap \textsc{Vars}\,(\Gamma) = \emptyset$, where

$$\textsc{Vars}\,(x_1 : A_1, \ldots, x_n : A_n) \stackrel{\text{def}}{=} \{x_1, \ldots, x_n\}$$

This causes a mild technical complication in the cases $\mathsf{K4}$ and GL. Fortunately, the solution is relatively simple, and we explain it now.

A. Complementary variables

Naively annotating the rule for $\mathsf{K4}$ would yield

$$\frac{\Delta\,;\Delta \vdash M : A}{\Delta\,;\Gamma \vdash \mathsf{box}\ M : \Box A}$$

This, however, violates our convention that the two contexts must be disjoint: the same variables will appear at both modal and intuitionistic positions. To overcome this we introduce the notion of *complementary variables*. Let $\mathcal{V}$ be our set of variables. A *complementation function* is an *involution* on variables. That is, it is a bijection $(-)^{\perp} : \mathcal{V} \xrightarrow{\cong} \mathcal{V}$ which happens to be its own inverse:

$$\left(x^{\perp}\right)^{\perp} = x$$

The idea is that, if u is the modal variable representing some assumption in Δ, we will write $u^{\perp}$ to refer to a variable x, that is uniquely associated to u, and represents the same assumption, but unboxed. For technical reasons, we would like that $x^{\perp}$ is the same variable as u.

We extend the involution to contexts:

$$(x_1 : A_1, \ldots, x_n : A_n)^{\perp} \stackrel{\text{def}}{=} x_1^{\perp} : A_1, \ldots, x_n^{\perp} : A_n$$

We also inductively extend $(-)^{\perp}$ to terms, with the exception that it shall not change anything inside a $\mathsf{box}\,(-)$ construct. It also need not change any bound modal variables, as for $\mathsf{K4}$ and GL these shall only occur under $\mathsf{box}\,(-)$ constructs:

$$\begin{aligned} (\lambda x : A.M)^{\perp} &\stackrel{\text{def}}{=} \lambda x^{\perp}{:}A.\ M^{\perp} \\ (MN)^{\perp} &\stackrel{\text{def}}{=} M^{\perp} N^{\perp} \\ \langle M, N \rangle &\stackrel{\text{def}}{=} \langle M^{\perp}, N^{\perp} \rangle \\ (\pi_i(M))^{\perp} &\stackrel{\text{def}}{=} \pi_i(M^{\perp}) \\ (\mathsf{box}\ M)^{\perp} &\stackrel{\text{def}}{=} \mathsf{box}\ M \\ (\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N)^{\perp} &\stackrel{\text{def}}{=} \mathsf{let\ box}\ u \Leftarrow M^{\perp}\ \mathsf{in}\ N^{\perp} \end{aligned}$$

We use this machinery to maintain disjoint contexts. When we encounter the introduction rule for the box and the modal context Δ gets 'copied' to the intuitionistic position, we will complement all variables in the copy, as well as all variables occuring in M, but not under any $\mathsf{box}\,(-)$ constructs:

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

We extend complementation to finite sets of variables, by setting

$$\{x_1, \ldots, x_n\} \stackrel{\text{def}}{=} x_1^{\perp}, \ldots, x_n^{\perp}$$

It is not hard to see that (a) the involutive behaviour of $(-)^{\perp}$ extends to all these extensions and (b) most common operations, such as $\text{VARS}\,(\cdot)$, commute with $(-)^{\perp}$. Furthermore, there is a simple relationship between complementation and substitution:

Theorem 1. *If $u^{\perp} \notin \text{FV}\,(M)$ then*

$$(M[N/u])^{\perp} \equiv M^{\perp}[N, N^{\perp}/u, u^{\perp}]$$

To conclude this section, we carefully define what it means for a pair of contexts to be well-defined.

Definition 1 (Well-defined contexts)**.** *A pair of contexts $\Delta\,;\Gamma$ is* well-defined *just if*

1) *They are* disjoint, *i.e.* $\text{VARS}\,(\Delta) \cap \text{VARS}\,(\Gamma) = \emptyset$.
2) *In the cases of K4 and GL, no two complementary variables occur in the same context; that is*

$$\text{VARS}\,(\Gamma) \cap \text{VARS}\left(\Gamma^{\perp}\right) = \emptyset$$
$$\text{VARS}\,(\Delta) \cap \text{VARS}\left(\Delta^{\perp}\right) = \emptyset$$

The second condition is easy to enforce, and will prove useful in some technical results found in the sequel.

B. Free variables: boxed and unboxed

Definition 2 (Free variables)**.**

1) *The* free variables $\text{FV}\,(M)$ *of a term M are defined by induction on the structure of the term in the usual manner, along with the following two modal cases:*

$$\text{FV}\,(\mathsf{box}\, M) \stackrel{\text{def}}{=} \text{FV}\,(M)$$
$$\text{FV}\,(\mathsf{let\ box}\, u \Leftarrow M \ \mathsf{in}\ N) \stackrel{\text{def}}{=} \text{FV}\,(M) \cup (\text{FV}\,(N) - \{u\})$$

and for GL we replace the clause for $\mathsf{box}\,(-)$ *with*

$$\text{FV}\,(\mathsf{fix}\ z\ \mathsf{in\ box}\ M) \stackrel{\text{def}}{=} \text{FV}\,(M) - \{z\}$$

2) *The* unboxed free variables $\text{FV}_0\,(M)$ *of a term are those that do* not *occur under the scope of a* $\mathsf{box}\,(-)$ *construct. They are formally defined by replacing the clause for* $\mathsf{box}\,(-)$ *in the definition of free variables by*

$$\text{FV}_0\,(\mathsf{box}\, M) \stackrel{\text{def}}{=} \emptyset$$

and, for GL,

$$\text{FV}_0\,(\mathsf{fix}\ z\ \mathsf{in\ box}\ M) \stackrel{\text{def}}{=} \emptyset$$

3) *The* boxed free variables $\text{FV}_{\geq 1}\,(M)$ *of a term M are those that* do *occur under the scope of a* $\mathsf{box}\,(-)$ *construct. They are formally defined by replacing the clauses for variables and for* $\mathsf{box}\,(-)$ *in the definition of free variables by*

$$\text{FV}_{\geq 1}\,(x) \stackrel{\text{def}}{=} \emptyset$$
$$\text{FV}_{\geq 1}\,(\mathsf{box}\, M) \stackrel{\text{def}}{=} \text{FV}\,(M)$$

and, for GL,

$$\text{FV}_{\geq 1}\,(\mathsf{fix}\ z\ \mathsf{in\ box}\ M) \stackrel{\text{def}}{=} \text{FV}\,(M) - \{z\}$$

Theorem 2 (Free variables)**.**

1) *For every term M, $\text{FV}\,(M) = \text{FV}_0\,(M) \cup \text{FV}_{\geq 1}\,(M)$.*
2) *For every term M, $\text{FV}_0\left(M^{\perp}\right) = \text{FV}_0\,(M)^{\perp}$.*
3) *For every term M, $\text{FV}_{\geq 1}\left(M^{\perp}\right) = \text{FV}_{\geq 1}\,(M)$.*
4) *If $\mathcal{S} \in \{$DK, DK4, DGL$\}$ and $\Delta\,;\Gamma \vdash_{\mathcal{S}} M : A$, then*

$$\text{FV}_0\,(M) \subseteq \text{VARS}\,(\Gamma)$$
$$\text{FV}_{\geq 1}\,(M) \subseteq \text{VARS}\,(\Delta)$$

5) *If $\mathcal{S} \in \{$DS4, DT$\}$ and $\Delta\,;\Gamma \vdash_{\mathcal{S}} M : A$, then*

$$\text{FV}_0\,(M) \subseteq \text{VARS}\,(\Gamma) \cup \text{VARS}\,(\Delta)$$
$$\text{FV}_{\geq 1}\,(M) \subseteq \text{VARS}\,(\Delta)$$

6) *If $\Delta;\Gamma, x{:}A, \Gamma' \vdash M : A$ and $x \notin \text{FV}\,(M)$, then $\Delta;\Gamma, \Gamma' \vdash M : A$.*
7) *If $\Delta, u{:}A, \Delta'\,;\Gamma \vdash M : A$ and $u \notin \text{FV}\,(M)$, then $\Delta, \Delta'\,;\Gamma \vdash M : A$.*

As expected, our systems satisfy the standard menu of structural results: weakening, contraction, exchange, and cut rules are admissible.

Theorem 3 (Structural & Cut)**.** *Weakening, exchange, and contraction rules for the intuitionistic context are admissible in all systems, as is the following cut rule:*

$$\frac{\Delta\,;\Gamma \vdash N : A \qquad \Delta\,;\Gamma, x{:}A, \Gamma' \vdash M : A}{\Delta\,;\Gamma, \Gamma' \vdash M[N/x] : A}$$

Theorem 4 (Modal Structural)**.** *Weakening, exchange and contraction rules are admissible for the modal context in all systems.*

Theorem 5 (Modal Cut)**.** *The following rules are admissible:*

1) *(Modal Cut for DK)*

$$\frac{\cdot\,;\Delta \vdash_{\textit{DK}} N : A \quad \Delta, u{:}A, \Delta'\,;\Gamma \vdash_{\textit{DK}} M : C}{\Delta, \Delta'\,;\Gamma \vdash_{\textit{DK}} M[N/u] : C}$$

2) *(Modal Cut for DK4)*

$$\frac{\Delta\,;\Delta^{\perp} \vdash_{\textit{DK4}} N^{\perp} : A \quad \Delta, u{:}A, \Delta'\,;\Gamma \vdash_{\textit{DK4}} M : C}{\Delta, \Delta'\,;\Gamma \vdash_{\textit{DK4}} M[N/u] : C}$$

3) *(Modal Cut for DGL)*

$$\frac{\begin{array}{c}\Delta\,;\Delta^{\perp}, z^{\perp} : \Box A \vdash_{\textit{DGL}} N^{\perp} : A \\ \Delta, u{:}A, \Delta'\,;\Gamma \vdash_{\textit{DGL}} M : C\end{array}}{\Delta, \Delta'\,;\Gamma \vdash_{\textit{DGL}} M\left[N\left[\mathsf{fix}\ z\ \mathsf{in\ box}\ N/z\right]/u\right] : C}$$

4) (Modal Cut for $\mathsf{DS4}$*)*

$$\frac{\Delta\,;\cdot\vdash_{\mathsf{DS4}} N : A \quad \Delta, u{:}A, \Delta'\,;\Gamma\vdash_{\mathsf{DS4}} M : C}{\Delta, \Delta'\,;\Gamma\vdash_{\mathsf{DS4}} M[N/u] : C}$$

5) (Modal Cut for DT*)*

$$\frac{\cdot\,;\Delta\vdash_{\mathsf{DT}} N : A \quad \Delta, u{:}A, \Delta'\,;\Gamma\vdash_{\mathsf{DT}} M : C}{\Delta, \Delta'\,;\Gamma\vdash_{\mathsf{DT}} M[N/u] : C}$$

Finally, in the cases where the T axiom is present, we may move variables from the intuitionstic to the modal context.

Theorem 6 (Modal Dereliction)**.** *If* $\mathcal{S} \in \{\mathsf{DS4}, \mathsf{DT}\}$*, then the following rule is admissible:*

$$\frac{\Delta\,;\Gamma, \Gamma'\vdash M : A}{\Delta, \Gamma\,;\Gamma'\vdash M : A}$$

C. Equivalence to Hilbert systems

We can prove metatheoretic properties for the Hilbert systems presented in §II-A that essentially correspond to the admissibility of the introduction rules of the dual-context systems. These lead to the following theorems. Given a context $\Gamma \equiv x_1 : A_1, \ldots, x_n : A_n$, write $\hat{\Gamma}$ for the context consisting only of the types, i.e. $A_1, \ldots, A_n$. Also, write $\mathsf{D}\mathcal{L}$ for the dual-context system corresponding to the logic $\mathcal{L}$ (e.g. if $\mathcal{L} \equiv \mathsf{CGL}$, then $\mathsf{D}\mathcal{L} \equiv \mathsf{DGL}$).

Theorem 7 (Hilbert to Dual)**.** *If* Γ *is a well-defined context and* $\hat{\Gamma} \vdash_{\mathcal{L}} A$*, then there exists a term* M *such that* $\cdot;\Gamma \vdash_{\mathsf{D}\mathcal{L}} M : A$*.*

Theorem 8 (Dual to Hilbert)**.** *If* $\Delta\,;\Gamma \vdash_{\mathsf{D}\mathcal{L}} M : A$ *then* $\Box\hat{\Delta}, \hat{\Gamma} \vdash_{\mathcal{L}} A$*.*

The proof of these theorems is beyond the scope of the paper.

V. Reduction

In this section we study a notion of reduction for our dual-context calculi. Our reduction relation,

$$\longrightarrow \;\subseteq\; \Lambda \times \Lambda$$

is defined in Figure 3, and it is essentially the standard notion of reduction previously considered by [18]. A similar notion of reduction was studied in the context of Dual Intuitionistic Linear Logic (DILL) by [38]. Unlike [38] we do not study the full reduction including η-contractions and commuting conversions.

Theorem 9 (Subject reduction)**.** *If* $\Delta\,;\Gamma \vdash M : A$ *and* $M \longrightarrow N$*, then* $\Delta\,;\Gamma \vdash N : A$*.*

Our notion of reduction is rather well-behaved:

Theorem 10. *The reduction relation* $\longrightarrow$ *is confluent and strongly normalizing.*

Whereas confluence is easy to show (using e.g. parallel reduction), strong normalization is slightly harder to obtain. We have done so by using the method of *candidates of reducibility (candidats de reducibilité)*, which is a kind of induction on types, rather closely related to the technique of *logical*

Fig. 3. Reduction

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

$$\frac{}{\pi_i(\langle M_1, M_2\rangle) \longrightarrow M_i}\ (\times\beta)$$

$$\frac{M \longrightarrow N}{\pi_i(M) \longrightarrow \pi_i(N)}\ (\mathsf{cong}_{\pi_i})$$

$$\frac{M_i \longrightarrow N_i \quad \text{and} \quad M_{1-i} \equiv N_{1-i}}{\langle M_0, M_1\rangle \longrightarrow \langle N_0, N_1\rangle}\ (\mathsf{cong}_{\times})$$

$$\frac{M \longrightarrow N}{\lambda x{:}A.\ M \longrightarrow \lambda x{:}A.\ N}\ (\mathsf{cong}_{\lambda})$$

$$\frac{M \longrightarrow N}{\mathsf{box}\ M \longrightarrow \mathsf{box}\ N}\ (\mathsf{cong}_{\mathsf{box}})$$

$$\frac{M \longrightarrow N}{MP \longrightarrow NP}\ (\mathsf{app}_1)$$

$$\frac{P \longrightarrow Q}{MP \longrightarrow MQ}\ (\mathsf{app}_2)$$

$$\frac{M \longrightarrow N}{\mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ M \longrightarrow \mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ N}\ (\mathsf{cong}_{\mathsf{fix}})$$

$$\frac{M \longrightarrow N}{\mathsf{let}\ \mathsf{box}\ u \Leftarrow M\ \mathsf{in}\ P \longrightarrow \mathsf{let}\ \mathsf{box}\ u \Leftarrow N\ \mathsf{in}\ P}\ (\mathsf{letbox}_1)$$

$$\frac{P \longrightarrow Q}{\mathsf{let}\ \mathsf{box}\ u \Leftarrow M\ \mathsf{in}\ P \longrightarrow \mathsf{let}\ \mathsf{box}\ u \Leftarrow M\ \mathsf{in}\ Q}\ (\mathsf{letbox}_2)$$

Beta rule for non-GL:

$$\frac{}{\mathsf{let}\ \mathsf{box}\ u \Leftarrow \mathsf{box}\ M\ \mathsf{in}\ N \longrightarrow N[M/u]}\ (\Box\beta)$$

Beta rule for GL:

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

relations—or, in this particular case, logical predicates–see [2, §14] for an introduction. The particular variant we use is a mixture of the versions of Girard [39] and Koletsos [40], see also [41], [42]. We hope that some of the details will appear in the full version of the present paper.

A. Subformula Property

The notion of reduction we have studied in this section is computationally interesting, but is *logically weak*, in the sense that it does not satisfy the *Subformula Property*.

The gist of the subformula property is that, in a 'normal' proof of formula A from assumptions Γ (i.e. a proof that has no *detours*), the only formulas involved should be either (a) subexpressions of the conclusion A, or (b) subexpressions of some premise in Γ. This is almost sufficient to say that the proof has a very specific structure: it proceeds by eliminating logical symbols of assumptions in Γ, and then uses the results to 'build up' a proof of A using only introduction rules. See [43] and [2] for a fuller discussion of these points.

Let us return to our systems. We define $\longrightarrow_c \subseteq \Lambda \times \Lambda$ to be the compatible closure of $\longrightarrow$ that includes the following clauses:

$$\begin{aligned}
&\pi_i\,(\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N) \\
\longrightarrow_c\ &\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ \pi_i(N) \\
&(\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ P)\,Q \\
\longrightarrow_c\ &\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ PQ \\
&\mathsf{let\ box}\ v \Leftarrow (\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N)\ \mathsf{in}\ P \\
\longrightarrow_c\ &\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ \mathsf{let\ box}\ v \Leftarrow N\ \mathsf{in}\ P
\end{aligned}$$

We can now prove the requisite property for this reduction relation.

Theorem 11 (Subformula Property)**.** *Let $\Delta\,;\Gamma \vdash M : A$, and suppose M is a $(\longrightarrow_c)$-normal form. Then, every type occuring in the derivation of $\Delta\,;\Gamma \vdash M : A$ is either a subexpression of the type A, or a subexpression of a type in Δ or Γ.*

We have thus established the notion of reduction $\longrightarrow_c$, which eliminates any structurally irrelevant occurences from a proof of the formula. Of course, one should extend the preceding analysis of $\longrightarrow$ to this notion, but we think that this may be harder than it sounds.

VI. Modal Category Theory

In order to formulate categorical semantics for our calculi, we shall need—first and foremost—a cartesian-closed category (CCC), for the underlying λ-calculus. For background on categorical semantics please refer to [44]–[46].

We shall model the modality by a *strong monoidal endofunctor*. In our case, the monoidal product will be the cartesian product of the cartesian closed category. Its being strongly monoidal corresponds to the isomorphism $\Box(A \times B) \cong \Box A \times \Box B$ which is another way of stating the modal axiom K. For want of space, we shall not treat the case of GL here.

In this section we develop a modest amount of monoidal category theory. The basic definitions of *monoidal categories*, *lax monoidal functors* and *monoidal natural transformations* may be found MacLane [47, §XI.2] and the survey of Melliès [48, §5].

Definition 3. *A* strong monoidal functor *between two cartesian categories is a lax monoidal functor where the components $m_{A,B} : F(A) \times F(B) \to F(A \times B)$ and the arrow $m_0 : \mathbf{1} \to F(\mathbf{1})$ are isomorphisms.*

One may also show that if the underlying category is cartesian, then a strong monoidal functor is *product-preserving*.[5] The natural transformations can be extended to more objects. We write $\prod_{i=1}^n A_n$ for the product $A_1 \times \cdots \times A_n$, where the $\times$ *associates to the left*. We define, by induction:

$$\begin{aligned}
m^{(0)} &\stackrel{\text{def}}{=} m_0 : \mathbf{1} \to F\mathbf{1} \\
m^{(n+1)} &\stackrel{\text{def}}{=} m \circ (m^{(n)} \times id) : \prod_{i=1}^{n+1} FA_i \to F\left(\prod_{i=1}^{n+1} A_i\right)
\end{aligned}$$

The combination of a CCC with a strong monoidal endofunctor is the quintessential structure in our development, so we give it a name.

Definition 4. *A* Kripke category $(\mathcal{C}, \times, \mathbf{1}, F)$ *is a cartesian closed category $\mathcal{C}$, considered as a monoidal category $(\mathcal{C}, \times, \mathbf{1})$, along with a* strong monoidal endofunctor $F : \mathcal{C} \longrightarrow \mathcal{C}$.

Kripke categories are the minimal setting in which one can the introduction rule for K by defining an operation

$$(-)^\bullet : \mathcal{C}\left(\prod_{i=1}^n A_i, B\right) \to \mathcal{C}\left(\prod_{i=1}^n FA_i, FB\right)$$

by

$$f^\bullet \stackrel{\text{def}}{=} Ff \circ m^{(n)}$$

When axiom $\mathsf{4}$ is involved, we will use the following structure, which is "half a comonad."

Definition 5. *A* Kripke-4 *category $(\mathcal{C}, \times, \mathbf{1}, Q, \delta)$ is a Kripke category $(\mathcal{C}, \times, \mathbf{1}, Q)$ along with a monoidal natural transformation $\delta : Q \Rightarrow Q^2$ such that the following diagram commutes:*

$$\begin{tikzcd}
QA \arrow[r, "\delta_A"] \arrow[d, "\delta_A"'] & Q^2A \arrow[d, "\delta_{Q(A)}"] \\
Q^2A \arrow[r, "Q(\delta_A)"'] & Q^3A
\end{tikzcd}$$

Like Kripke categories, Kripke-4 categories are the minimal setting in which one can model the introduction rule for $\mathsf{K4}$. To see this, let $(\mathcal{C}, \times, \mathbf{1}, Q, \delta)$ be a Kripke-4 category, and write

$$\prod_{i=1}^n A_i \times_l \prod_{j=1}^m B_j$$

[5] Please refer to the full version for the proof.

to mean the left-associating product $A_1 \times \cdots \times A_n \times B_1 \times \cdots \times B_m$. Also, write $\langle \overrightarrow{f_i}, \overrightarrow{g_i}, \overrightarrow{h_j} \rangle$ to mean the left-associating mediating morphism $\langle f_1, \ldots, f_n, g_1, \ldots, g_m, h_1, \ldots, g_p \rangle$. With this notation we can now define a map of hom-sets

$$(-)^{\#} : \mathcal{C}\left(\prod_{i=1}^{n} FA_i \times_l \prod_{i=1}^{n} A_i, B\right) \to \mathcal{C}\left(\prod_{i=1}^{n} FA_i, FB\right)$$

by

$$f^{\#} \stackrel{\text{def}}{=} Ff \circ m^{(2n)} \circ \langle \overrightarrow{\delta_{A_i}\pi_i}, \overrightarrow{\pi_i} \rangle$$

Similarly, the following structure will be the categorical analogue to the logic T.

Definition 6. *A* Kripke-T *category* $(\mathcal{C}, \times, \mathbf{1}, Q, \epsilon)$ *is a Kripke category* $(\mathcal{C}, \times, \mathbf{1}, Q)$ *along with a monoidal natural transformation* $\epsilon : Q \Rightarrow \mathsf{Id}$.

Modelling the modal dereliction rule amounts to precomposition with a product of a bunch of components of $\epsilon : Q \Rightarrow \mathsf{Id}$.

Our final modality is that of $\mathsf{S4}$. We will need the following notion from monoidal category theory.

Definition 7. *A* monoidal comonad *on a cartesian category* $\mathcal{C}$ *is a comonad* (Q, ϵ, δ) *such that* $Q : \mathcal{C} \longrightarrow \mathcal{C}$ *is a monoidal functor, and* $\epsilon : Q \Rightarrow \mathsf{Id}$ *and* $\delta : Q \Rightarrow Q^2$ *are monoidal natural transformations.*

Definition 8. *A* Bierman-de Paiva category (BdP category) $(\mathcal{C}, \times, \mathbf{1}, Q, \delta, \epsilon)$ *is a Kripke category* $(\mathcal{C}, \times, \mathbf{1}, Q)$ *whose functor* $Q : \mathcal{C} \longrightarrow \mathcal{C}$ *is part of a monoidal comonad* (Q, δ, ϵ).

Bierman-de Paiva categories are—as before—the minimal setting in which both the Four and T rules can be modelled. This time, the Four rule is modelled by *co-Kleisli extension*: we define the map

$$(-)^{*} : \mathcal{C}\left(\prod_{i=1}^{n} FA_i, B\right) \to \mathcal{C}\left(\prod_{i=1}^{n} FA_i, FB\right)$$

as follows:

$$f^{*} \stackrel{\text{def}}{=} Ff \circ m^{(n)} \circ \prod_{i=1}^{n} \delta_{A_i}$$

VII. Categorical Semantics

In this section we use the modal category theory developed in §VI to formulate a categorical semantics for our dual-context calculi. This completes the circle in terms of the Curry-Howard-Lambek correspondence, showing the following associations:

CK	$\longleftrightarrow$	DK	$\longleftrightarrow$	Kripke categories
CK4	$\longleftrightarrow$	DK4	$\longleftrightarrow$	Kripke-4 categories
CT	$\longleftrightarrow$	DT	$\longleftrightarrow$	Kripke-T categories
CS4	$\longleftrightarrow$	DS4	$\longleftrightarrow$	Bierman-de Paiva categories

where the first bi-implication refers to provability, whereas the second refers to soundness and completeness of the dual-context calculus with respect to the type of category on the right.

We begin by endowing our calculi with a equational theory, and then proceed to show soundness for the semantics in §VI. The equational theory we use is basic, and amounts to removing orientation from the reduction relation, and annotating with types. If we also add some commuting conversions to that theory, it is not hard to obtain completeness for this semantics, but we leave that to the full version. The rules for the theory may be found in Figures 4 and 5.

We are now fully equipped to define the categorical semantics of our dual-context systems, and we start by interpreting types and contexts. Given any Kripke category $(\mathcal{C}, \times, \mathbf{1}, F)$, and a map $\mathcal{I}(-)$ associating each base type p_i with an object $\mathcal{I}(p_i) \in \mathcal{C}$, we define an object $[\![A]\!] \in \mathcal{C}$ for every type A by induction:

$$\begin{aligned} [\![p_i]\!] &\stackrel{\text{def}}{=} \mathcal{I}(p_i) \\ [\![A \times B]\!] &\stackrel{\text{def}}{=} [\![A]\!] \times [\![B]\!] \quad [\![A \to B]\!] \stackrel{\text{def}}{=} [\![B]\!]^{[\![A]\!]} \\ [\![\Box A]\!] &\stackrel{\text{def}}{=} F([\![A]\!]) \end{aligned}$$

Then, given a well-defined context $\Delta\,;\Gamma$ where $\Delta = u_1{:}B_1, \ldots u_n{:}B_n$ and $\Gamma = x_1{:}A_1, \ldots, x_m{:}A_m$, we let

$$[\![\Delta\,;\Gamma]\!] \stackrel{\text{def}}{=} F(B_1) \times \cdots \times F(B_n) \times A_1 \times \cdots \times A_m$$

where the product is, as ever, left-associating.

We then extend the semantic map $[\![-]\!]$ to associate an arrow

$$[\![\Delta\,;\Gamma \vdash M : A]\!] : [\![\Delta\,;\Gamma]\!] \to [\![A]\!]$$

of the category $\mathcal{C}$ to each derivation $\Delta\,;\Gamma \vdash M : A$. The definition for rules common to all calculi are the same. For each logic we use x of the maps defined in §VI to interpret the introduction rules for the modality. Thus we need more than just a Kripke category: for $\mathsf{K4}$ we need a Kripke-4 category, for T we need a Kripke-T category, and for $\mathsf{S4}$ we need a Bierman-de Paiva category.

Most of the definitions are standard and may be found in [45], [46]. The new cases are given in Figure 6. The map

$$\pi_{\Delta}^{\Delta;\Gamma} : [\![\Delta\,;\Gamma]\!] \to [\![\Delta\,;\cdot]\!]$$

is the obvious projection. Moreover, the notation $\langle \overrightarrow{\pi_\Delta}, f, \overrightarrow{\pi_\Gamma} \rangle$ stands for

$$\langle \overrightarrow{\pi_\Delta}, f, \overrightarrow{\pi_\Gamma} \rangle \stackrel{\text{def}}{=} \langle \pi_1, \ldots, \pi_n, f, \pi_{n+1}, \ldots, \pi_{n+m} \rangle$$

We can then show that

Theorem 12 (Soundness)**.** *If* $\Delta\,;\Gamma \vdash_{\mathsf{D}\mathcal{L}} M = N : A$*, then we have that*

$$[\![\Delta\,;\Gamma \vdash M : A]\!]_{\mathcal{L}} = [\![\Delta\,;\Gamma \vdash N : A]\!]_{\mathcal{L}}$$

It is also relatively easy to argue that the above semantics is complete, by using the method of Lindenbaum and Tarski. However, that is not within the scope of the present paper.

VIII. Coda

We have achieved a full Curry-Howard-Lambek isomorphism for a handful of modal logics, spanning the logical aspect (Hilbert systems and provability), the computational aspect (a study of reduction), and the categorical aspect (proof-relevant semantics).

Fig. 4. Equations for all systems

Function Spaces

$$\frac{\Delta\,;\Gamma, x{:}A \vdash M : B \qquad \Delta\,;\Gamma \vdash N : A}{\Delta\,;\Gamma \vdash (\lambda x{:}A.M)\,N = M[N/x] : B}\,(\to\beta) \qquad \frac{\Delta\,;\Gamma \vdash M : A \to B \qquad x \notin \mathsf{fv}(M)}{\Delta\,;\Gamma \vdash M = \lambda x{:}A.Mx : A \to B}\,(\to\eta)$$

Modality

$$\frac{\Delta\,;\Gamma \vdash M : \Box A}{\Delta\,;\Gamma \vdash \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in\ box}\ u = M : \Box A}\,(\Box\eta) \qquad \frac{\Delta\,;\Gamma \vdash M = N : \Box A \qquad \Delta\,;\Gamma \vdash P = Q : C}{\Delta\,;\Gamma \vdash \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ P = \mathsf{let\ box}\ u \Leftarrow N\ \mathsf{in}\ Q : B}\,(\Box\mathsf{let\text{-}cong})$$

Remark. In addition to the above, one should also include (a) rules that ensure that equality is an equivalence relation, and (b) congruence rules for λ-abstraction and application.

Fig. 5. Equations for the modalities

For DK and DT:

$$\frac{\cdot\,;\Delta \vdash M : A \qquad \Delta, u : A\,;\Gamma \vdash N : C}{\Delta\,;\Gamma \vdash \mathsf{let\ box}\ u \Leftarrow \mathsf{box}\ M\ \mathsf{in}\ N = N[M/x] : C}\,(\Box\beta_{\mathsf{K}}) \qquad \frac{\cdot\,;\Delta \vdash M = N : A}{\Delta\,;\Gamma \vdash \mathsf{box}\ M = \mathsf{box}\ N : \Box A}\,(\Box\mathsf{cong}_{\mathsf{K}})$$

For $\mathsf{DK4}$:

$$\frac{\Delta\,;\Delta^{\perp} \vdash M^{\perp} : A \qquad \Delta, u{:}A\,;\Gamma \vdash N : C}{\Delta\,;\Gamma \vdash \mathsf{let\ box}\ u \Leftarrow \mathsf{box}\ M\ \mathsf{in}\ N = N[M/x] : C}\,(\Box\beta_{\mathsf{K4}}) \qquad \frac{\Delta\,;\Delta^{\perp} \vdash M^{\perp} = N^{\perp} : A}{\Delta\,;\Gamma \vdash \mathsf{box}\ M = \mathsf{box}\ N : \Box A}\,(\Box\mathsf{cong}_{\mathsf{K4}})$$

For $\mathsf{DS4}$:

$$\frac{\Delta\,;\cdot \vdash M : A \qquad \Delta, u : A\,;\Gamma \vdash N : C}{\Delta\,;\Gamma \vdash \mathsf{let\ box}\ u \Leftarrow \mathsf{box}\ M\ \mathsf{in}\ N = N[M/x] : C}\,(\Box\beta_{\mathsf{S4}}) \qquad \frac{\Delta\,;\cdot \vdash M = N : A}{\Delta\,;\Gamma \vdash \mathsf{box}\ M = \mathsf{box}\ N : \Box A}\,(\Box\mathsf{cong}_{\mathsf{S4}})$$

Fig. 6. Categorical Semantics

Definitions for all calculi

$$[\![\Delta\,;\Gamma \vdash \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N : C]\!] \stackrel{\text{def}}{=} [\![\Delta, u{:}A\,;\Gamma \vdash N : C]\!] \circ \langle \overrightarrow{\pi_{\Delta}}, [\![\Delta\,;\Gamma \vdash M : \Box A]\!]\,, \overrightarrow{\pi_{\Gamma}} \rangle$$

Definitions for various modalities

$$\left[\!\left[\Delta, u{:}A, \Delta'\,;\Gamma \vdash u : A\right]\!\right]_{\mathsf{T}} \stackrel{\text{def}}{=} \epsilon_A \circ \pi : \left[\!\left[\Delta, u{:}A, \Delta'\,;\Gamma\right]\!\right] \to [\![\Box A]\!] \to [\![A]\!]$$

$$[\![\Delta\,;\Gamma \vdash \mathsf{box}\ M : \Box A]\!]_{\mathcal{L}} \stackrel{\text{def}}{=} ([\![\cdot\,;\Delta \vdash M : A]\!])^{\bullet} \circ \pi^{\Delta;\Gamma}_{\Delta} \qquad (\text{for } \mathcal{L} \in \{\mathsf{K}, \mathsf{T}\})$$

$$[\![\Delta\,;\Gamma \vdash \mathsf{box}\ M : \Box A]\!]_{\mathsf{K4}} \stackrel{\text{def}}{=} \left(\left[\!\!\left[\Delta\,;\Delta^{\perp} \vdash M^{\perp} : A\right]\!\!\right]\right)^{\#} \circ \pi^{\Delta;\Gamma}_{\Delta}$$

$$[\![\Delta\,;\Gamma \vdash \mathsf{box}\ M : \Box A]\!]_{\mathsf{S4}} \stackrel{\text{def}}{=} ([\![\Delta\,;\cdot \vdash M : A]\!])^{*} \circ \pi^{\Delta;\Gamma}_{\Delta}$$

In order to achieve the first junction—that between logic and computation—we have employed a systematic pattern based on sequent calculus, namely a way to translate (right or single) modal sequent calculus rules to introduction rules for dual context systems. In all our cases this has worked remarkably well. It is our hope that there is a deeper aspect to this pattern—perhaps even a theorem to the effect that sequent calculi rules for which cut elimination is provable can be immediately translated to a strongly normalizing dual-context system. Of course, this is rather utopian at this stage, but we believe it is worth investigating.

We have also set the scene for a handful of different necessity modalities, and begun to elucidate their computational behaviour. The present author believes that modalities can be used to control the 'flow of data' in a programming language, in the sense that they create regions of the language which communicate in a very specific way. For example, one can handwavingly argue that $\mathsf{S4}$ guarantees that 'only modal variables flow into terms of modal type,' whereas K additionally ensures that no modal data flows into a term of non-modal type. However, these examples are—at this stage—mere intuitions. Making such intuitions rigorous and proving them should amount to a sort of *dataflow safety property*. A first result of this style is the free variables theorem (Theorem 2), but the author finds it rather weak. We believe that this might be made much stronger by making use of the second junction, that between computation and categories: investigating categorical models for these calculi can perhaps give a succinct and rigorous expression to these intuitions.

Having such safety properties can make these calculi extraordinarily useful for particular applications. For example, it seems that K is stratified in two levels: 'the world under a box,' and 'the world outside boxes.' These seemingly two layers of K resemble the two-level λ-calculi used in binding time analyses [49] that Davies and Pfenning [50] safely embedded in $\mathsf{DS4}$. In *op. cit.* the authors remark they remark that the necessary "fragment corresponds to a weaker modal logic, K, in which we drop the assumption in S4 that the accessibility relation is reflexive and transitive [...]." Thus, we may think of K as *the logic of program construction*, i.e. a form of metaprogramming that happens in one stage.

Another interpretation of K could be as *the logic of homomorphic encryption*. If we 'identify' box terms, i.e. consider the M in $\mathsf{box}\ M$ to be *invisible* and *indistinguishable*, then one may understand K as a server-side programming language for homomorphic encryption (see e.g. [51]). Indeed, the term ax_{K} that proves axiom K can be understood as the server-side routine that applies an *encrypted* function to an *encrypted* datum.

Let us also mention that the case of $\mathsf{S4}$ corresponds to *programming with comonads*, which are dual to monads. Whereas monads broadly correspond to *effectful computation* [4], comonads seem to correspond to *contextual computation*. A lot of work has been based on this intuition, culminating in the thesis of Orchard [52]. It is conceivable that there are also similar 'contextual' structures which are not equipped with either a Orchard's *current* (co-unit) or *disject* (co-multiplication) operation, and which could play the rôle of semantics for the calculi in this paper, corresponding to the cases of $\mathsf{K4}$ or T respectively.

Acknowledgments

The author acknowledges funding of his doctoral work by the EPSRC (award reference 1354534). Thanks are due to Sam Staton and Luke Ong for their encouragement, and Samson Abramsky for his advice.

References

[1] W. A. Howard, "The formulae-as-types notion of construction," in *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, J. P. Seldin and J. R. Hindley, Eds. Boston, MA: Academic Press, 1980, pp. 479–490. [Online]. Available: http://www.cs.cmu.edu/~crary/819-f09/Howard80.pdf

[2] J.-Y. Girard, Y. Lafont, and P. Taylor, *Proofs and Types*. Cambridge University Press, 1989.

[3] M. H. Sørensen and P. Urzyczyn, *Lectures on the Curry-Howard Isomorphism*. Elsevier, 2006.

[4] E. Moggi, "Notions of computation and monads," *Information and Computation*, vol. 93, no. 1, pp. 55–92, 1991. [Online]. Available: https://dx.doi.org/10.1016/0890-5401(91)90052-4

[5] G. M. Bierman and V. de Paiva, "On an Intuitionistic Modal Logic," *Studia Logica*, vol. 65, no. 3, pp. 383–416, 2000. [Online]. Available: https://dx.doi.org/10.1023/A:1005291931660

[6] V. de Paiva, R. Goré, and M. Mendler, "Editorial: Modalities in Constructive Logics and Type Theories," *Journal of Logic and Computation*, vol. 14, no. 4, pp. 439–446, 2004. [Online]. Available: http://logcom.oupjournals.org/cgi/doi/10.1093/logcom/14.4.439

[7] W. Taha and T. Sheard, "MetaML and multi-stage programming with explicit annotations," *Theoretical Computer Science*, vol. 248, no. 1-2, pp. 211–242, 2000. [Online]. Available: https://dx.doi.org/10.1016/S0304-3975(00)00053-0

[8] T. Tsukada and A. Igarashi, "A logical foundation for environment classifiers," *Logical Methods in Computer Science*, vol. 6, no. 4, pp. 1–43, 2010. [Online]. Available: https://dx.doi.org/10.2168/LMCS-6(4:8)2010

[9] M. Abadi, A. Banerjee, N. Heintze, and J. G. Riecke, "A core calculus of dependency," in *Proceedings of the 26th ACM SIGPLAN-SIGACT symposium on Principles of programming languages - POPL '99*. New York, New York, USA: ACM Press, 1999, pp. 147–160. [Online]. Available: https://dx.doi.org/10.1145/292540.292555

[10] T. Murphy, K. Crary, R. Harper, and F. Pfenning, "A symmetric modal lambda calculus for distributed computing," in *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science, 2004.* IEEE, 2004, pp. 286–295. [Online]. Available: https://dx.doi.org/10.1109/LICS.2004.1319623

[11] J.-Y. Girard, "On the unity of logic," *Annals of Pure and Applied Logic*, vol. 59, no. 3, pp. 201–217. [Online]. Available: https://dx.doi.org/10.1016/0168-0072(93)90093-S

[12] J.-M. Andreoli, "Logic Programming with Focusing Proofs in Linear Logic," *Journal of Logic and Computation*, vol. 2, no. 3, pp. 297–347, 1992. [Online]. Available: https://dx.doi.org/10.1093/logcom/2.3.297

[13] P. Wadler, "A taste of linear logic," in *Proceedings of Mathematical Foundations of Computer Science 1993: 18th International Symposium, MFCS'93 Gdańsk, Poland, August 30–September 3, 1993*, ser. LNCS, 1993, vol. 711, pp. 185–210. [Online]. Available: https://dx.doi.org/10.1007/3-540-57182-5_12

[14] ——, "A syntax for linear logic," in *Mathematical Foundations of Programming Semantics: 9th International Conference, New Orleans, LA, USA, April 7 - 10, 1993. Proceedings*, S. Brookes, M. Main, A. Melton, M. Mislove, and D. Schmidt, Eds. Springer-Verlag Berlin Heidelberg, 1994, pp. 513–529. [Online]. Available: http://link.springer.com/10.1007/3-540-58027-1_24

[15] G. D. Plotkin, "Type theory and recursion," in *Proceedings Eighth Annual IEEE Symposium on Logic in Computer Science*. IEEE Comput. Soc. Press, 1993, p. 374. [Online]. Available: https://dx.doi.org/10.1109/LICS.1993.287571

[16] A. G. Barber, "Dual Intuitionistic Linear Logic," ECS-LFCS-96-347, Laboratory for Foundations of Computer Science, University of Edinburgh, Tech. Rep., 1996. [Online]. Available: http://www.lfcs.inf.ed.ac.uk/reports/96/ECS-LFCS-96-347/

[17] F. Pfenning and R. Davies, "A judgmental reconstruction of modal logic," *Mathematical Structures in Computer Science*, vol. 11, no. 4, pp. 511–540, 2001. [Online]. Available: https://dx.doi.org/10.1017/S0960129501003322

[18] R. Davies and F. Pfenning, "A modal analysis of staged computation," *Journal of the ACM*, vol. 48, no. 3, pp. 555–604, 2001. [Online]. Available: https://dx.doi.org/10.1145/382780.382785

[19] F. Pfenning, "Decomposing Modalities," 2015. [Online]. Available: http://www.cs.cmu.edu/~fp/talks/lfmtp15-talk.pdf

[20] V. Danos and J. B. Joinet, "Linear logic and elementary time," *Information and Computation*, vol. 183, no. 1, pp. 123–137, 2003. [Online]. Available: https://dx.doi.org/10.1016/S0890-5401(03)00010-5

[21] G. Bellin, "A system of natural deduction for GL," *Theoria*, vol. 51, no. 2, pp. 89–114, 1985.

[22] G. A. Kavvos, "The Many Worlds of Modal λ-calculi: I. Curry-Howard for Necessity, Possibility and Time," *CoRR*, 2016. [Online]. Available: http://arxiv.org/abs/1605.08106

[23] S. A. Kripke, "Semantical Analysis of Modal Logic I. Normal Modal Propositional Calculi," *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, vol. 9, no. 5-6, pp. 67–96, 1963. [Online]. Available: https://dx.doi.org/10.1002/malq.19630090502

[24] A. K. Simpson, "The Proof Theory and Semantics of Intuitionistic Modal Logic," Ph.D. dissertation, The University of Edinburgh, 1994. [Online]. Available: http://hdl.handle.net/1842/407

[25] F. Pfenning, "Intensionality, extensionality, and proof irrelevance in modal type theory," *Proceedings 16th Annual IEEE Symposium on Logic in Computer Science*, 2001. [Online]. Available: https://dx.doi.org/10.1109/LICS.2001.932499

[26] R. Hakli and S. Negri, "Does the deduction theorem fail for modal logic?" *Synthese*, vol. 187, no. 3, pp. 849–867, 2012. [Online]. Available: https://dx.doi.org/10.1007/s11229-011-9905-9

[27] G. Gentzen, "Untersuchungen über das logische Schließen. I," *Mathematische Zeitschrift*, vol. 39, no. 1, pp. 176–210, 1935. [Online]. Available: http://link.springer.com/10.1007/BF01201353

[28] ——, "Untersuchungen über das logische Schließen. II," *Mathematische Zeitschrift*, vol. 39, no. 1, pp. 405–431, 1935. [Online]. Available: http://link.springer.com/10.1007/BF01201363

[29] G. Bellin, V. de Paiva, and E. Ritter, "Extended Curry-Howard correspondence for a basic constructive modal logic," in *Proceedings of Methods for Modalities*, 2001. [Online]. Available: http://www.cs.bham.ac.uk/~vdp/publications/m4m.pdf

[30] D. Leivant, "On the proof theory of the modal logic for arithmetic provability," *The Journal of Symbolic Logic*, vol. 46, no. 03, pp. 531–538, sep 1981. [Online]. Available: https://dx.doi.org/10.2307/2273755

[31] S. Valentini, "Cut-elimination in a modal sequent calculus for K," *Bolletino dell'Unione Mathematica Italiana*, vol. 1B, pp. 119–130, 1982.

[32] D. Wijesekera, "Constructive modal logics I," *Annals of Pure and Applied Logic*, vol. 50, no. 3, pp. 271–301, dec 1990. [Online]. Available: https://dx.doi.org/10.1016/0168-0072(90)90059-B

[33] G. Sambin and S. Valentini, "The modal logic of provability. The sequential approach," *Journal of Philosophical Logic*, vol. 11, no. 3, pp. 311–342, 1982. [Online]. Available: https://dx.doi.org/10.1007/BF00293433

[34] R. Goré and R. Ramanayke, "Valentini's Cut-Elimination for Provability Logic Resolved," *The Review of Symbolic Logic*, vol. 5, no. 02, pp. 212–238, 2012. [Online]. Available: https://dx.doi.org/10.1017/S1755020311000323

[35] H. Wansing, "Sequent Systems for Modal Logics," in *Handbook of Philosophical Logic*. Dordrecht: Springer Netherlands, 2002, pp. 61–145. [Online]. Available: https://dx.doi.org/10.1007/978-94-010-0387-2_2

[36] M. Ohnisi and K. Matsumoto, "Gentzen method in modal calculi," *Osaka Journal of Mathematics*, vol. 11, no. 2, pp. 113–130, 1957.

[37] J. Gallier, "Constructive logics Part I: A tutorial on proof systems and typed λ-calculi," *Theoretical Computer Science*, vol. 110, no. 2, pp. 249–339, mar 1993. [Online]. Available: https://dx.doi.org/10.1016/0304-3975(93)90011-H

[38] Y. Ohta and M. Hasegawa, "A Terminating and Confluent Linear Lambda Calculus," in *Lecture Notes in Computer Science*, 2006, vol. 4098, pp. 166–180. [Online]. Available: https://dx.doi.org/10.1007/11805618_13

[39] J.-Y. Girard, "Interprétation fonctionelle et élimination des coupures de l'arithmétique d'ordre supérieur," Ph.D. dissertation, Université Paris VII, 1972.

[40] G. Koletsos, "Church-Rosser theorem for typed functional systems," *The Journal of Symbolic Logic*, vol. 50, no. 03, pp. 782–790, sep 1985. [Online]. Available: https://dx.doi.org/10.2307/2274330

[41] J. Gallier, "On the Correspondence Between Proofs and Lambda Terms," in *The Curry-Howard Isomorphism*, P. de Groote, Ed. Louvain-la-Neuve: Academia, 1995, pp. 55–138.

[42] ——, "On Girard's "Candidats de Reductibilite"," in *Logic and Computer Science*, P. Odifreddi, Ed. Academic Press, 1990, pp. 123–203. [Online]. Available: ftp://ftp.cis.upenn.edu/pub/papers/gallier/sngirard1.pdfftp://ftp.cis.upenn.edu/pub/papers/gallier/sngirard2.pdfftp://ftp.cis.upenn.edu/pub/papers/gallier/sngirard3.pdfftp://ftp.cis.upenn.edu/pub/papers/gallier/sngirard4.pdf

[43] D. Prawitz, *Natural Deduction: a proof-theoretical study.* Almquist and Wiksell, 1965.

[44] J. Lambek and P. J. Scott, *Introduction to Higher-Order Categorical Logic*. Cambridge University Press, 1988.

[45] R. L. Crole, *Categories for Types*. Cambridge University Press, 1993.

[46] S. Abramsky and N. Tzevelekos, "Introduction to Categories and Categorical Logic," in *New Structures for Physics*, B. Coecke, Ed. Springer-Verlag, 2011, pp. 3–94. [Online]. Available: http://arxiv.org/abs/1102.1313

[47] S. Mac Lane, *Categories for the Working Mathematician*, ser. Graduate Texts in Mathematics. New York, NY: Springer New York, 1978, vol. 5. [Online]. Available: http://link.springer.com/10.1007/978-1-4757-4721-8

[48] P.-A. Melliès, "Categorical Semantics of Linear Logic," in *Panoramas et synthèses 27: Interactive models of computation and program behaviour*, P.-L. Curien, H. Herbelin, J.-L. Krivine, and P.-A. Melliès, Eds. Société Mathématique de France, 2009. [Online]. Available: http://www.pps.univ-paris-diderot.fr/~mellies/papers/panorama.pdf

[49] F. Nielson and H. R. Nielson, *Two-Level Functional Languages*, ser. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 1992.

[50] R. Davies and F. Pfenning, "A modal analysis of staged computation," in *Proceedings of the 23rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'96)*, 1996, pp. 258–270. [Online]. Available: https://dx.doi.org/10.1145/382780.382785

[51] C. Gentry, "Computing arbitrary functions of encrypted data," *Communications of the ACM*, vol. 53, no. 3, p. 97, mar 2010. [Online]. Available: https://dx.doi.org/10.1145/1666420.1666444

[52] D. Orchard, "Programming contextual computations," Ph.D. dissertation, University of Cambridge, 2014. [Online]. Available: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-854.pdf