Dual-context Calculi for Modal Logic (Technical Report)

G. A. Kavvos
St John's College
University of Oxford

Contents

List of Figures

This is version 1.0.1672 of this report, compiled on July 23, 2017.

Chapter 1

Prelude

The study of modal λ-calculi, and the modal logics associated with them through the Curry-Howard correspondence (Howard, 1980; Girard et al., 1989; Sørensen and Urzyczyn, 2006) began at the dawn of the 1990s, heralded by the developments in Linear Logic. Early milestones include Moggi's *monadic metalanguage* (Moggi, 1991), and the discovery of a constructive S4-like modality by Bierman and de Paiva (2000). This was followed by an explosion of developments, as well as some first applications. This era is surveyed by de Paiva et al. (2004).

Since the early 2000s this field has been commandeered by the programming language community, who may have focused less on theory, but have made great strides in applications—ranging from metaprogramming (Taha and Sheard, 2000; Tsukada and Igarashi, 2010) to 'dependency analysis' (Abadi et al., 1999), and even distributed computing and mobile code (Murphy et al., 2004).

The major issue with modal proof theory is that its methods are, at their best, kaleidoscopic: some types of calculi seemingly work better for specific logics, but fail to suit others. It is easy to develop an intuition about these patterns. However, 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, K4, GL and S4—are best suited to *dual-context calculi*, as pioneered by Girard (1993), Andreoli (1992), Wadler (1993, 1994), Plotkin (1993), Barber (1996), Pfenning and Davies (2001) and Davies and Pfenning (2001). 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. Then, we very briefly revisit previous attempts at presenting calculi for each of these.

This naturally leads us to a presentation of our systematic way for deriving dual context systems from sequent calculi. We define our calculi, prove that they are equivalent to the Hilbert systems, and delve into their metatheory. This is followed by a study of a simple notion of reduction on terms, which is shown to satisfy the usual properties. 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 and complete 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 its 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 Pfenning and Davies (2001), who introduced dual contexts to modal logic. However, their work mostly concerned the type system and its applications to binding-time analysis: they did not discuss reduction in any appreciable 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 (Pfenning, 2015) in the context of a *linear sequent calculus*. This 'linear K' of Pfenning seems to be closely related to the work of Danos and Joinet (2003) in *elementary linear logic*. However, the natural deduction formulation of the intuitionistic modal case, as well as the technical innovations regarding the term calculus that are needed for $\mathsf{K4}$ (and consequently GL), are independently due to the present author. The only previous approach to GL was the rather complicated natural deduction calculus of Bellin (1985), and the appreciably simpler dual-context formulation is our own invention. Finally, the approach to T is new. The reader is invited to consult the survey (Kavvos, 2016) for a more detailed history of 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 author has formalized most of the metatheoretic results in Agda; the proofs are available either from his website[1] or his GitHub repository.[2]

[1] `www.lambdabetaeta.eu`

[2] lambdabetaeta/modal-logics

Chapter 2

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

2.1 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-theoretic interpretation, 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. First, the de Morgan duality between necessity ($\Box$) and possibility ($\Diamond$) 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 respectively. Second, the principles $\Diamond(A \vee B) \to \Diamond A \vee \Diamond B$ and $\neg\Diamond\bot$ are not provable. These two principles are tautologies if we employ traditional Kripke semantics (Kripke, 1963). Thus, the step to constructivity necessitates that we eschew the Kripkean analysis, at least in its most popular form. 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. Simpson (1994)), it seems that its computational interpretation is not very crisp. Hence, we restrict our study to the more well-behaved and seemingly more applicable necessity modality (but see Pfenning (2001)).

As the history of modal proof theory and constructive modal logics is long and tumultuous, we shall try to avoid the subject as much as possible. An extensive survey and discussion of the history of constructive modal logic may be found in (**?**). For a broader survey of the proof theory for modal logic we recommend Negri (2011).

2.2 Preliminaries

All our modal logics shall be inductively defined sets of formulae—the *theorems* of the logic. These formulae 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. The sets of theorems will be generated by *axioms*, closed under some *inference rules*. The set of axioms will always contain (a) all the instances the axioms of intuitionistic propositional logic, but for modal formulae (abbrv. $\mathsf{IPL}_\Box$); and (b) all instances of the *normality* axiom, also known as axiom K:

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

The set of inference rules will contain—amongst others—of all instances the two rules necessary to capture $\mathsf{IPL}_\Box$, namely the *axiom rule*:

$$\frac{A \text{ is an axiom}}{A \in \mathcal{L}}$$

and the rule of *modus ponens*:

$$\frac{(A \to B) \in \mathcal{L} \quad A \in \mathcal{L}}{B \in \mathcal{L}}$$

As for the modal part, we include all instances of the *necessitation* rule, namely

$$\frac{A \in \mathcal{L}}{\Box A \in \mathcal{L}}$$

The only thing that will then vary between any two of our logics $\mathcal{L}$ will be the set of axioms.

2.3 Hilbert systems

There are two steps to passing from the definition of a logic to a *Hilbert system* for it. 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 second step is to include the rules of axiom and modus ponens in this system. We also add a rule that allows us to *use an assumption*; that is,

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

We need to be careful in adapting the rule of necessitation. Doing so in a straightforward manner may invalidate the deduction theorem, which was a source of confusion in early work on the proof theory of modal logic—see Hakli and Negri (2012) for a historical and technical account. To solve this issue, we need to recall that necessitation is often similar to universal quantification: $\Box A$ is a theorem just if A is a theorem, and there is no reason that this will be so if we need any assumptions to prove A to be a theorem. Hence, we should be able to infer $\Box A$ (under any assumptions) only if we can infer A without any assumptions at all. In symbols:

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

The full system may be found in Figure 2.1.

2.4 Axioms

To obtain the various 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 axioms $(A_1), \ldots, (A_n)$ under the rules in Figure 2.1.

Figure 2.1: Hilbert systems

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

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

We write $(\mathsf{IPL}_\Box)$ to mean all instances of the axiom schemata of intuitionistic propositional logic, but also including formulas of the form $\Box A$ in the syntax. We will use the following axiom schemata:

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

Constructive K is then defined as the minimal *normal* constructive modal logic. Constructive $\mathsf{K4}$ results from adding the axiom $\mathsf{4}$. Likewise, constructive T results from adding axiom T to CK. Constructive $\mathsf{S4}$ results from all these three axioms taken together. Finally, we obtain constructive GL from CK by adding the *Gödel-Löb* axiom GL. A summary in symbols is in order:

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

To indicate that we are using the Hilbert system for e.g. CK, we annotate the turnstile, like so:

$$\Gamma \vdash_{\mathsf{CK}} A$$

We simply write $\Gamma \vdash A$ or $\Gamma \vdash_{\mathcal{H}} A$ when the statement under discussion pertains to all of our Hilbert systems.

2.5 Metatheory for Hilbert

2.5.1 Structural rules

We establish the following basic facts about all our logics:

Theorem 1 (Structural & Cut)**.** *The following rules are admissible.*[1]

1. (Weakening)

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

2. (Exchange)

$$\frac{\Gamma, A, B, \Gamma' \vdash C}{\Gamma, B, A, \Gamma' \vdash C}$$

3. (Contraction)

$$\frac{\Gamma, A, A, \Gamma' \vdash C}{\Gamma, A, \Gamma' \vdash C}$$

4. (Cut)

$$\frac{\Gamma \vdash A \qquad \Gamma, A, \Gamma' \vdash C}{\Gamma \vdash C}$$

Proof. All by induction. □

Theorem 2 (Deduction Theorem)**.** *The following rule is admissible in all of our logics:*

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

Proof. By induction on the derivation of $\Gamma, A \vdash C$. □

2.5.2 Admissible Rules

We now consider some rules that are admissible in our Hilbert systems. These will prove useful when we tackle the equivalence of the Hilbert systems with the dual-context systems.

The first one is *Scott's rule*, which ensures that if we 'box' all our assumptions, we can get something 'boxed' in return. Categorically, Scott's rule expresses the fact that the box modality is a functor, and that this functor is monoidal. We write $\Box\Gamma$ to mean the context Γ which each assumption occurring in it boxed, i.e.

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

[1] Recall that a rule is *admissible* just if the existence of a proof of the antecedent implies the existence of a proof of the conclusion. In contrast, a rule is *derivable* just if a proof of the antecedent can be used verbatim to make a proof of the conclusion.

Theorem 3 (Admissibility of Scott's rule)**.** *The following rule is admissible in all of our logics:*

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

Proof. Induction on the derivation of $\Gamma \vdash A$. Most cases are straightforward, except perhaps the one for modus ponens. If the last step in the derivation of $\Gamma \vdash A$ is of the form

$$\frac{\begin{array}{cc}\vdots & \vdots \\ \Gamma \vdash B \to A & \Gamma \vdash B\end{array}}{\Gamma \vdash A}$$

then, by applying the induction hypotheses to the two subderivations, we obtain proofs of $\Box\Gamma \vdash \Box(B \to A)$ and $\Box\Gamma \vdash \Box B$. We can then use axiom K and use modus ponens twice to build the desired proof, like so:

$$\dfrac{\dfrac{\dfrac{}{\Box\Gamma \vdash \Box(B \to A) \to \Box B \to \Box A} \qquad \begin{array}{c}\vdots \\ \Box\Gamma \vdash \Box(B \to A)\end{array}}{\Box\Gamma \vdash \Box B \to \Box A} \qquad \begin{array}{c}\vdots \\ \Box\Gamma \vdash \Box B\end{array}}{\Box\Gamma \vdash \Box A}$$

□

Next, we deal with a rule that is only derivable if the system contains the axiom T. The gist of the rule is that $\Box A$ is stronger than A, as it implies it in any context.

Theorem 4 (Admissibility of the T Rule)**.** *If $\mathcal{L}$ is a logic that includes the T axiom, i.e. if $\mathcal{L} \in \{\mathsf{CT}, \mathsf{CS4}\}$, then the following rule is admissible:*

$$\frac{\Gamma \vdash_{\mathcal{L}} A}{\Box\Gamma \vdash_{\mathcal{L}} A}$$

Proof. By induction on the derivation of $\Gamma \vdash A$. All the cases are straightforward, except the assumption rule. If $\Gamma \vdash A$ because A occurs in Γ, then $\Box\Gamma \vdash \Box A$, and using modus ponens along with an instance of axiom T yields the result. □

Finally, we present a rule that we call the *Four rule*. As its name suggests, the Four rule deductively encapsulates the inclusion of axiom $\mathsf{4}$. In a nutshell, it expresses the fact that, if something is derivable from $\Box\Box A$, then it is derivable from $\Box A$ itself.

The Four rule only pertains to logics that include all instances of $\mathsf{4}$. One of these logics is CGL, but in its case $\mathsf{4}$ is a theorem, so we begin by deriving it:

Lemma 1. $\vdash_{\mathsf{CGL}} \Box A \to \Box\Box A$

Proof. We follow Boolos (1994). It is not hard to see that, by using the one of the product axioms and Scott's rule, $\Box(\Box A \wedge A) \vdash \Box A$, and hence that

$$A, \Box(\Box A \wedge A) \vdash \Box A \wedge A$$

again by using weakening and the one of the product axioms. Then, the deduction theorem and Scott's rule yield that

$$\Box A \vdash \Box\left(\Box\left(\Box A \wedge A\right) \rightarrow \Box A \wedge A\right)$$

Using that alongside modus ponens and the Gödel-Löb axiom yields

$$\Box A \vdash \Box\left(\Box A \wedge A\right)$$

and using the cut rule with $\Box\left(\Box A \wedge A\right) \vdash \Box\Box A$ followed by the deduction theorem yields the result. □

Thus:

Theorem 5 (Admissibility of the Four Rule)**.** *If $\mathcal{L}$ is a logic that includes $\mathsf{4}$ either as axiom or as theorem, i.e. if $\mathcal{L} \in \{\mathsf{CK4}, \mathsf{CGL}, \mathsf{CS4}\}$, then the following rule is admissible:*

$$\frac{\Box\Gamma, \Gamma \vdash_{\mathcal{L}} A}{\Box\Gamma \vdash_{\mathcal{L}} \Box A}$$

Proof. Induction on the derivation of $\Box\Gamma, \Gamma \vdash A$. Most cases are straightforward: it suffices to use necessitation. The case for modus ponens uses axiom K—see the proof for Scott's rule for details.

This leaves the case where $\Box\Gamma, \Gamma \vdash A$ by the assumption rule. It follows that A either occurs in $\Box\Gamma$, or it occurs in Γ. If it occurs in $\Box\Gamma$, then it is of the form $\Box A'$; thus $\Box\Gamma \vdash \Box A'$, and using modus ponens alongside an instance of axiom $\mathsf{4}$ yields $\Box\Gamma \vdash \Box\Box A' = \Box A$. If, on the other hand, A occurs in Γ, then $\Box\Gamma \vdash \Box A$ by the assumption rule, and we are done. □

A slightly weaker variant of the Four rule appears in Bierman and de Paiva (2000). It is a corollary to ours:

Corollary 1. *If $\mathcal{L}$ is a logic that includes $\mathsf{4}$ either as axiom or as theorem, i.e. if $\mathcal{L} \in \{\mathsf{CK4}, \mathsf{CGL}, \mathsf{CS4}\}$, then the following rule is admissible:*

$$\frac{\Box\Gamma \vdash_{\mathcal{L}} A}{\Box\Gamma \vdash_{\mathcal{L}} \Box A}$$

Proof. Use weakening and the Four rule. □

If the T rule is admissible as well—i.e. in the case of CS4—we can derive the theorem from the corollary. If $\Box\Gamma, \Gamma \vdash A$, then repeated uses of the T rule yield $\Box\Gamma, \Box\Gamma \vdash A$. Repeated uses of contraction then yield $\Box\Gamma \vdash A$, and then the corollary applies, yielding the conclusion of the theorem. However, if the axiom T is not present and Rule T is not admissible, we shall need the stronger version.

Finally, we show that *Löb's rule* is admissible in CGL. Again, we show a stronger version:

Theorem 6 (Löb's Rule)**.** *The following rule is admissible in CGL:*

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

Proof. By the deduction theorem, we can infer that $\Box\Gamma, \Gamma \vdash \Box A \to A$, and hence by the Four rule (Theorem 5), it follows that

$$\Box\Gamma \vdash \Box(\Box A \to A)$$

Using an instance of the Gödel-Löb axiom and modus ponens yields the conclusion of the rule. □

Again, we have a corollary that is weaker but corresponds to what is normally referred to as Löb's rule:

Corollary 2. *The following rule is admissible in CGL:*

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

Proof. Use weakening and Löb's rule. □

Chapter 3

From sequent calculi to dual contexts

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

3.1 The Perennial Issues

A brief perusal of the survey (**?**) 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 Bierman and de Paiva (1992, 1996, 2000); and (b) those employing *dual contexts*, a pattern that was imported into modal type theory by (Davies and Pfenning, 1996) and (Pfenning and Davies, 2001).

3.1.1 Explicit substitutions à la Bierman & de Paiva

The calculus introduced by Bierman and de Paiva made use of a trick that was previously employed in the context of Intuitionistic Linear Logic by Benton et al. (1993) to ensure that substitution is admissible. The trick is simple: *if cut is not admissible, then build it into the introduction rule.*

In the case of CS4 (Bierman and de Paiva, 2000), the resulting λ-calculus is a simple extension of the ordinary simply typed one with the following introduction rule:

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

In this example, $x_1, \ldots x_n$ comprise all the free variables that may occur in N. They must all be 'modal,' in that their type has to start with a box. But if we are to place a box in front of B then we must provide a substitute M_i for each of these free variables, and M_i must also be of modal type. In short: *all the data that goes into the*

making of something of type $\Box B$ *must be 'boxed.'* And, as if that were not enough, all these terms of type A_i must be provided *at once*, for they are 'frozen' as part of the term of type $\Box B$: they become an *explicit substitution* in the syntax. This is a combined introduction and cut rule: the introduction part ensures that modal data depend only on modal data, and the cut part allows for substitution.

By comparison, the elimination rule is much simpler, and incorporates axiom T ($\Box A \to A$):

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

In order to ensure admissibility of cut and hence subject reduction, the β-rule associated with these rules has the effect of unrolling the explicit substitutions *en masse*:

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

Calculi of this sort are notorious for suffering from two kinds of problems: (a) their need for multiple commutative conversions, and (b) the general lack of 'good symmetries' in the rules of the calculus. These two aspects we shall discuss in turn.

Commuting Conversions In order to maintain the validity of central proof-theoretic results, calculi with explicit subsitutions often need a large number of *commutative conversions*. Amongst other things, these conversions expose 'hidden' redexes, the existence of which spoil the so-called *subformula property*. The issue of commutative conversions is known to arise from rules for positive connectives, such as those for disjunction and existence; for a particularly perspicuous discussion, see (Girard et al., 1989, §10.1).

In calculi such as the above, commutative conversions are are invariably some kind of *structural rule* concerning the explicit substitutions. Structural rules are traditionally found in sequent calculi, but not in natural deduction where they are often admissible. Their presence in a natural deduction system is incompatible with the view that natural deduction proofs comprise the "real proof objects"—see (Girard et al., 1989, §5.4). In the case of Bierman and de Paiva's system for CS4, Goubault-Larrecq (1996) argues that systems like it obscure the computational meaning of modal proofs: if they didn't, they would need no structural rules at all.

'Good' symmetries The calculus of Bierman and de Paiva for CS4 exhibits reasonable symmetries: if we forget about the explicit substitutions for a moment,

then we can see an introduction and an elimination rule, the latter post-inverse to the former: there is reasonable *harmony*.

Things are not that simple when it comes to other calculi of this sort. To see that, we look at the the calculus of Bellin et al. (2001) for CK. Its introduction rule is only slightly different to the one for CS4, in that the free variables need not be of modal type. However, the substitutes for these free variables do not need to be of modal type. To wit:

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

In this calculus there can be no harmony, for there is no elimination rule at all. Indeed, the only plausible 'β-rule' one might adopt is actually just a commuting conversion that was previously studied in the context of CS4 by Goubault-Larrecq (1996). Its function is to unbox any 'canonical' terms in the explicit substitutions; e.g

$$\mathsf{box}\ yx\ \mathsf{with}\ y, (\mathsf{box}\ M\ \mathsf{with}\ z\ \mathsf{for}\ z)\ \mathsf{for}\ y, x \longrightarrow \mathsf{box}\ y(\mathsf{box}\ M)\ \mathsf{with}\ y, z\ \mathsf{for}\ y, z$$

in an appropriate context for y and z. It is thus evident that once we step out of the relatively harmonious patterns of CS4, the use of systems based on explicit subsitutions becomes less and less tenable.

It is thus evident that in order to reach a better solution we must overcome two problems: (a) we must 'decouple' the two flavours—introduction and cut—that are both present in introduction rules of this type; and (b) we must minimize as much as possible the commuting conversions—in particular, we should strive to make them free of any computational content. We should expect, though, that to do so one might have to sacrifice the apparent simplicity of this type of system.

3.1.2 Dual contexts

The right intuition for achieving this 'decoupling' was introduced by Girard (1993) in his attempt to combine classical, intuitionistic, and linear logic in one system, and also independently by Andreoli (1992) in the context of linear logic programming.

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 Barber (1996) and Plotkin (1993), where the primary context consists of *linear* assumptions, whereas the secondary consists of ordinary *intuitionstic* assumptions. The 'of course' modality (!) of Linear Logic is very much like a S4 modality, and—simply by lifting the linearity restrictions—(Pfenning and Davies, 2001; Davies and Pfenning, 2001) 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 chapter 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.

3.2 Deriving dual-context calculi

We shall start with the usual suspect, namely the *sequent calculus*. Gentzen introduced the sequent calculus in the 1930s (Gentzen, 1935a,b) in order to study normalisation of proofs, known as *cut elimination* in this context; see Girard et al. (1989) 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 in natural deduction.[1] The rules, however, are different: 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

[1]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 (Girard et al., 1989, §5.1.3).

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. See (Girard et al., 1989, §5.4) for a more in-depth discussion of the correspondence between natural deduction and sequent calculus.

The first attempts to forge sequent calculi for modal logics began in the 1950s, with the formulation of a sequent calculus for $\mathsf{S4}$ by Curry (1952) and Ohnisi and Matsumoto (1957, 1959). There was also some limited success for other simple modal logics, mainly involving the axioms we discuss here. Most of these are mentioned by Ono (1998) and are more thoroughly discussed in the survey by Wansing (2002); see also (Negri, 2011).

3.2.1 The Introduction Rules

Let us consider the right rule for the logic $\mathsf{S4}$. 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' (cf. §3.1.1).

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 $\mathsf{S4}$ 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, with weakening included. Incidentally, it is also exactly the introduction rule of Pfenning and Davies (2001) 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 §3.2.6.

3.2.2 K

The case for K is slightly harder to fathom at first sight. This is because its sequent 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 Bellin et al. (2001) 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. Leivant (1981) and Valentini (1982) showed that incorporating Scott's rule yields a system which admits cut elimination. Scott's rule also appears in the sequent calculus for CK studied by Wijesekera (1990).

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 must become modal, at once.* The final form is reached again by adding opportunities for weakening:

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

At this point, the reader may protest vehemently, arguing that this is not an introduction rule in the spirit of natural deduction at all: we are shamelessly messing with assumptions! So much is true. But it is also true that even the most well-behaved fragments of natural deduction are not really trees, but involve some 'back edges,' e.g. to record when and which assumptions are discharged—see (Girard et al., 1989, §2.1). The situation is even more involved when it comes to the not-so-well-behaving positive fragment ($\vee\exists$): for example, elimination rule for $\vee$, namely

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$$

involves the silent elimination of two 'temporary assumptions,' A and B. Rules involving such temporary assumptions have been of enough importance to warrant their own name: they are known as rules "in the style" of Schroeder-Heister (1984). The sum of it all is this: the proofs were never really trees.

Consequently, our shameless shuffling of assumptions from one context to another shall not weigh heavily on our conscience. In fact, there is a simple way to think about the 'jump' that the context Δ makes, from intuitionistic to modal. Suppose indeed that we are in the process of writing down an ordinary deduction, and we want to introduce a box in front of the conclusion. All we have to do, then, is to place a mark on *all* the assumptions that are open at that point. This does not discharge them, but it merely makes them modal: there shall be a fundamentally different way of substiting for them, and it shall be a little more complicated than the simple splicing of a proof tree at a leaf.[2]

3.2.3 K4

The right sequent calculus rule for the logic K4, as well as the proof of cut elimination, is due to Sambin and Valentini (1982). Using elements from his joint work with Sambin, as well some counterexamples found in the work of Leivant (1981) on GL, Valentini noticed that the key is to notice that, due to axiom 4, anything derivable by $\Box\Box A$ 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. This co-occurence of the same assumptions in two forms will cause some mild technical complications in the next section, but that will clarify the structure of the 'flow of data' in K4.

A direct translation, after adding opportunities for weakening, amounts to the introduction rule:

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

[2] In fact, in order to substitute, we will need to ensure that (a) the substitute must have no modal assumptions at all, and (b) after substitution, we need to mark all the assumptions of that substitute as modal. But we leave that for later.

3.2.4 GL

The correct formulation of sequent calculus for GL is a difficult problem that receives attention time and time again. There are simple solutions that guarantee that we can derive all and only theorems of GL, but they fail to satisfy cut elimination. There is also a very complicated system of natural deduction, due to Bellin (1985).

The first attempt at a cut-free sequent calculus was that of Leivant (1981). Soon thereafter Valentini (1983) showed that Leivant's proof of cut elimination was incorrect. Sambin and Valentini (1980) describe a procedure for building cut-free proofs for all provable sequents, but their proof is semantic and goes through Kripke structures, and hence does not rely on Gentzen-style cut elimination. Sambin and Valentini (1982) collect and describe in detail many early approaches, the reasons they do or do not work, and all relevant results. Finally, Valentini (1983) shows that the same rule admits cut elimination, but the proof is rather complicated, and derives from ideas due to Bellin (1985). Recent progress on clarifying that result may be found in Goré and Ramanayke (2012).

The Leivant-Valentini sequent calculus rule for GL is the following:

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

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:

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

3.2.5 The Elimination Rule

As discussed in §3.1.2, 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.[3] 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.*

One cannot help but notice that such rules are also in the infamous style of Schroeder-Heister (1984), and very similar to that for disjunction. This kind of rule is known to be problematic, as it automatically necessitates some commuting conversions: unavoidably, the conclusion C has no structural relationship with anything else in sight. See (Girard et al., 1989, §10) for a more in-depth discussion.

Can we live with this? Unless we are to engage in more complicated and radical schemes, the present author is afraid that we must. Put simply, there is no good way to do away with commuting conversions: they are part-and-parcel of any sufficiently complicated type theory. All we can hope for is to (a) minimize their number, and (b) state them systematically.

3.2.6 A second variable rule

We have conveniently avoided discussing two things up to this point: (a) the left rule for $\Box$ in $\mathsf{S4}$, 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 necessity in $\mathsf{S4}$ 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

[3] Alternative approaches have also been considered. For example, one could introduce another abstraction operator, i.e. a 'modal λ.' This has been adopted by Pfenning (2001), in a dependently-typed setting.

cut is admissible; this is mentioned by Wansing (2002) and attributed to Ohnisi and Matsumoto (1957).

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 following 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 Plotkin (1993) and Barber (1996) 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.

Chapter 4

Terms, Types and Metatheory

In this chapter we collect all the observations we made in §3 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 (Girard et al., 1989, §3) or (Gallier, 1993; Sørensen and Urzyczyn, 2006) for an introduction. We omit a treatment of $\vee$, for it is largely orthogonal.

The grammars defining types, terms and contexts, as well as the typing rules for all our systems can be found in Figure 4.1. When we are at risk of confusion, we annotate the turnstile with a subscript to indicate which system we are referring to; e.g. $\Delta\,;\Gamma \vdash_{\mathsf{GL}} M : A$ refers to the system consisting of the rules pertaining to all our calculi coupled with the introduction rule $(\Box\mathcal{I}_{\mathsf{GL}})$.

We also define

$$\Lambda_A \stackrel{\text{def}}{=} \{\, M \mid \exists \Delta, \Gamma.\ \Delta\,;\Gamma \vdash M : A \,\}$$

is the set of terms of type A, and we also write Λ for the set of all terms, well-typed or not.

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 mean 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.

Figure 4.1: Definition and Typing Judgments

$$\begin{array}{rrcl} \textbf{Types} & A, B & ::= & p_i \mid A \times B \mid A \to B \mid \Box A \\ \textbf{Typing Contexts} & \Gamma, \Delta & ::= & \cdot \mid \Gamma, x{:}A \\ \textbf{Terms} & M, N & ::= & x \mid \lambda x{:}A.\ M \mid MN \mid \langle M, N\rangle \mid \pi_1(M) \mid \pi_2(M) \\ & & & \mid \mathsf{box}\ M \mid \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N \end{array}$$

Rules for all calculi:

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

$$\frac{\Delta\,;\,\Gamma \vdash M : A \quad \Delta\,;\,\Gamma \vdash N : B}{\Delta\,;\,\Gamma \vdash \langle M, N\rangle : A \times B}\,(\times\mathcal{I}) \qquad \frac{\Delta\,;\,\Gamma \vdash M : A_1 \times A_2}{\Delta\,;\,\Gamma \vdash \pi_i\,(M) : A_i}\,(\times\mathcal{E}_i)$$

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

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

Rules for K, K4, GL:

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

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

Rules for S4:

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

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

4.1 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 are disjoint: the same variables will appear both at modal and intuitionistic positions. To overcome this we introduce the notion of *complementary variables*. Let $\mathcal{V}$ be the set of term variables for our calculi. 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, uniquely associated to u, and representing the same assumption, but without a box in front. 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 modify the rule, so as to maintain disjoint contexts. When we encounter an introduction rule for the box and the 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:

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

As an example, here is the derivation that $\cdot\,;\Box A \vdash \Box(A \wedge \Box A)$:

$$\dfrac{\cdot\,;x:\Box A \vdash x:\Box A \qquad \dfrac{\dfrac{}{u:A\,;u^\perp:A \vdash u:A} \qquad \dfrac{\dfrac{}{u:A\,;u^\perp:A \vdash u^\perp:A}}{u:A\,;u^\perp:A \vdash \mathsf{box}\,u:\Box A}}{u:A\,;u^\perp:A \vdash \langle u^\perp, \mathsf{box}\,u\rangle : A \times \Box A}}{u:A\,;x:\Box A \vdash \mathsf{box}\,\langle u, \mathsf{box}\,u\rangle : \Box(A \times \Box A)}}{\cdot\,;x:\Box A \vdash \mathsf{let\ box}\,u \Leftarrow x\ \mathsf{in\ box}\,\langle u, \mathsf{box}\,u\rangle : \Box(A \times \Box A)}$$

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) some common operations commute with $(-)^\perp$.

Lemma 2.

1. *For any context* Δ, $\left(\Delta^\perp\right)^\perp \equiv \Delta$.
2. *For any finite set of variabels* S, $\left(S^\perp\right)^\perp = S$.
3. *For any context* Δ, $\textsc{Vars}\left(\Delta^\perp\right) = (\textsc{Vars}\,(\Delta))^\perp$.
4. *If* S, T *are finite sets of variables, then*

$$S \subseteq T \quad \Longrightarrow \quad S^\perp \subseteq T^\perp$$

Proof. Trivial. □

There is a simple relationship between complementation and substitution:

Theorem 7. *If* $u^\perp \notin \textsc{fv}\,(M)$ *then*

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

Proof. By induction on M.

1. If M is a variable, then by assumption $M \not\equiv u^\perp$. There are then two cases:
   (a) $M \equiv u$: then

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

(b) $M \equiv v \not\equiv u, u^\perp$: then

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

2. If $M \equiv \lambda x{:}A.M'$, then, assuming $x \not\equiv u, u^\perp$, then we use the IH to calculate that

$$(M[N/u])^\perp \equiv \lambda x^\perp.(M'[N/u])^\perp \equiv \lambda x^\perp.M'^\perp[N, N^\perp/u, u^\perp] \equiv (\lambda x.M')^\perp[N, N^\perp/u, u^\perp]$$

3. If M is an application $M_1 M_2$ or a tuple $\langle M_1, M_2 \rangle$, we use the IH twice. Similarly if it is a projection $\pi_i(M')$.

4. If $M \equiv \mathsf{box}\, M'$, we calculate:

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

where the last step follows because $\mathsf{box}\, M' \equiv (\mathsf{box}\, M')^\perp$, and $u^\perp \notin \textsc{fv}\,(M')$.

5. If $M \equiv \mathsf{let\ box}\, v \Leftarrow M_1\ \mathsf{in}\ M_2$, we calculate

$$\begin{aligned}(M[N/u])^\perp &\equiv \mathsf{let\ box}\, v \Leftarrow (M_1[N/u])^\perp\ \mathsf{in}\ (M_2[N/u])^\perp \\ &\equiv \mathsf{let\ box}\, v \Leftarrow M_1^\perp[N, N^\perp/u, u^\perp]\ \mathsf{in}\ M_2^\perp[N, N^\perp/u, u^\perp] \\ &\equiv \left(\mathsf{let\ box}\, v \Leftarrow M_1^\perp\ \mathsf{in}\ M_2^\perp\right)[N, N^\perp/u, u^\perp] \\ &\equiv M^\perp[N, N^\perp/u, u^\perp]\end{aligned}$$

□

To conclude our discussion of complementary variables, 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. $\textsc{Vars}\,(\Delta) \cap \textsc{Vars}\,(\Gamma) = \emptyset$.

2. In the cases of $\mathsf{K4}$ and GL, no two complementary variables occur in the same context; that is

$$\begin{aligned}\textsc{Vars}\,(\Gamma) \cap \textsc{Vars}\left(\Gamma^\perp\right) &= \emptyset \\ \textsc{Vars}\,(\Delta) \cap \textsc{Vars}\left(\Delta^\perp\right) &= \emptyset\end{aligned}$$

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

4.2 Free variables: boxed and unboxed

Definition 2 (Free variables)**.**

1. The *free variables* $\mathrm{FV}\,(M)$ of a term M are defined by induction on the structure of the term:

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

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

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

2. The *unboxed free variables* $\mathrm{FV}_0\,(M)$ 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

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

   and, for GL,

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

3. The *boxed free variables* $\mathrm{FV}_{\geq 1}\,(M)$ 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 the following

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

   and, for GL,

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

Theorem 8 (Free variables)**.**

1. *For every term* M, $\mathrm{FV}(M) = \mathrm{FV}_0(M) \cup \mathrm{FV}_{\geq 1}(M)$.

2. *For every term* M, $\mathrm{FV}_0\left(M^{\perp}\right) = \mathrm{FV}_0(M)^{\perp}$.

3. *For every term* M, $\mathrm{FV}_{\geq 1}\left(M^{\perp}\right) = \mathrm{FV}_{\geq 1}(M)$.

4. *If* $\mathcal{S} \in \{\mathsf{DK}, \mathsf{DK4}, \mathsf{DGL}\}$ *and* $\Delta\,;\Gamma \vdash_{\mathcal{S}} M : A$, *then*

$$\begin{aligned}\mathrm{FV}_0(M) &\subseteq \mathrm{VARS}(\Gamma)\\ \mathrm{FV}_{\geq 1}(M) &\subseteq \mathrm{VARS}(\Delta)\end{aligned}$$

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

$$\begin{aligned}\mathrm{FV}_0(M) &\subseteq \mathrm{VARS}(\Gamma) \cup \mathrm{VARS}(\Delta)\\ \mathrm{FV}_{\geq 1}(M) &\subseteq \mathrm{VARS}(\Delta)\end{aligned}$$

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

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

Proof.

1. Trivial induction on M.

2. Trivial induction on M.

3. Trivial induction on M.

4. By induction on the derivation of $\Delta\,;\Gamma \vdash_{\mathcal{S}} M : A$. We show the cases for $(\Box\mathcal{I})$. The first statement follows trivially, as $\mathrm{FV}_0(\mathsf{box}\, M) = \mathrm{FV}_0(\mathsf{fix}\, z\, \mathsf{in}\, \mathsf{box}\, M) = \emptyset \subseteq \mathrm{VARS}(\Gamma)$, so it remains to show the second statement.

   For $(\Box\mathcal{I}_{\mathsf{K}})$, we have

$$\begin{aligned}& \mathrm{FV}_{\geq 1}(\mathsf{box}\, M)\\ =\ & \{\,\text{definition}\,\}\\ & \mathrm{FV}(M)\\ =\ & \{\,(1)\,\}\\ & \mathrm{FV}_0(M) \cup \mathrm{FV}_{\geq 1}(M)\\ \subseteq\ & \{\,\text{IH, twice}\,\}\\ & \mathrm{VARS}(\Delta) \cup \mathrm{VARS}(\cdot)\\ =\ & \{\,\text{definition}\,\}\\ & \mathrm{VARS}(\Delta)\end{aligned}$$

For $(\Box\mathcal{I}_{\mathsf{K4}})$, we have

$$
\begin{array}{rl}
 & \mathrm{FV}_{\geq 1}\left(\mathsf{box}\, M\right) \\
= & \{\, \text{definition} \,\} \\
 & \mathrm{FV}\left(M\right) \\
= & \{\ (1)\ \} \\
 & \mathrm{FV}_0\left(M\right) \cup \mathrm{FV}_{\geq 1}\left(M\right) \\
= & \{\, \text{Lemma 2(2)} \,\} \\
 & \left(\mathrm{FV}_0\left(M\right)^{\perp}\right)^{\perp} \cup \mathrm{FV}_{\geq 1}\left(M\right) \\
\subseteq & \{\, \text{(2), (3), and Lemma 2(4)} \ \} \\
 & \left(\mathrm{FV}_0\left(M^{\perp}\right)\right)^{\perp} \cup \mathrm{FV}_{\geq 1}\left(M^{\perp}\right) \\
\subseteq & \{\, \text{IH twice, and Lemma 2(4)} \,\} \\
 & \left(\textsc{Vars}\left(\Delta^{\perp}\right)\right)^{\perp} \cup \textsc{Vars}\left(\Delta\right) \\
= & \{\, \text{Lemma 2(2)} \,\} \\
 & \textsc{Vars}\left(\Delta\right)
\end{array}
$$

by the IH.

For $(\Box\mathcal{I}_{\mathsf{K4}})$, we have

$$
\begin{aligned}
& \textsc{fv}_{\geq 1}\left(\mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ M\right) \\
= \ & \{\,\text{definition}\,\} \\
& \textsc{fv}\left(M\right) \\
= \ & \{\ (1)\ \} \\
& \left(\textsc{fv}_0\left(M\right) \cup \textsc{fv}_{\geq 1}\left(M\right)\right) - \{z^{\perp}\} \\
= \ & \{\,\text{Lemma 2(2)}\,\} \\
& \left(\left(\textsc{fv}_0\left(M\right)^{\perp}\right)^{\perp} \cup \textsc{fv}_{\geq 1}\left(M\right)\right) - \{z^{\perp}\} \\
\subseteq \ & \{\,(2),\ (3),\ \text{Lemma 2(4), and monotonicity of subtraction.}\,\} \\
& \left(\left(\textsc{fv}_0\left(M^{\perp}\right)\right)^{\perp} \cup \textsc{fv}_{\geq 1}\left(M^{\perp}\right)\right) - \{z^{\perp}\} \\
\subseteq \ & \{\,\text{IH twice, and Lemma 2(4) and monotonicity of subtraction.}\,\} \\
& \left(\left(\textsc{Vars}\left(\Delta^{\perp}\right) \cup \{z\}\right)^{\perp} \cup \textsc{Vars}\left(\Delta\right)\right) - \{z^{\perp}\} \\
= \ & \{\,\text{Lemma 2(2)}\,\} \\
& \left(\textsc{Vars}\left(\Delta\right) \cup \{z^{\perp}\} \cup \textsc{Vars}\left(\Delta\right)\right) - \{z^{\perp}\} \\
= \ & \{\,z^{\perp} \notin \textsc{Vars}\left(\Delta\right)\,\} \\
& \textsc{Vars}\left(\Delta\right)
\end{aligned}
$$

5. By induction on the derivation of $\Delta\,;\Gamma \vdash_{\mathcal{S}} M : A$. We show the case for $(\Box\mathcal{I}_{\mathsf{S4}})$; the first statement is trivial, so we show the second:

$$
\begin{aligned}
& \textsc{fv}_{\geq 1}\left(\mathsf{box}\ M\right) \\
= \ & \{\,\text{definition}\,\} \\
& \textsc{fv}\left(M\right) \\
= \ & \{\,(1)\,\} \\
& \textsc{fv}_0\left(M\right) \cup \textsc{fv}_{\geq 1}\left(M\right) \\
\subseteq \ & \{\,\text{IH, twice}\,\} \\
& \left(\textsc{Vars}\left(\Delta\right) \cup \textsc{Vars}\left(\cdot\right)\right) \cup \textsc{Vars}\left(\Delta\right) \\
= \ & \{\,\text{definition}\,\} \\
& \textsc{Vars}\left(\Delta\right)
\end{aligned}
$$

6. Trivial induction on the typing derivation for M.

7. Trivial induction on the typing derivation for M.

□

4.3 Structural theorems

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

Theorem 9 (Structural & Cut)**.** *The following rules are admissible in all systems:*

1. *(Weakening)*

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

2. *(Exchange)*

$$\frac{\Delta\,;\,\Gamma, x{:}A, y{:}B, \Gamma' \vdash M : C}{\Delta\,;\,\Gamma, y{:}B, x{:}A, \Gamma' \vdash M : C}$$

3. *(Contraction)*

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

4. *(Cut)*

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

Proof. All by induction on the typing derivation of M. Most cases are standard. As an example, we show the case of $(\Box\mathcal{I}_{\mathsf{K}})$ for weakening. Suppose $\Delta\,;\,\Gamma, \Gamma' \vdash M : A$ by $(\Box\mathcal{I}_{\mathsf{K}})$. Then $M \equiv \mathsf{box}\, M'$ and $A \equiv \Box A'$ and $\cdot\,;\,\Delta \vdash M' : A'$. A single use of $(\Box\mathcal{I}_{\mathsf{K}})$ then yields $\Delta\,;\,\Gamma, x{:}A, \Gamma' \vdash M : A$. □

Theorem 10 (Modal Structural)**.** *The following rules are admissible:*

1. *(Modal Weakening)*

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

2. *(Modal Exchange)*

$$\frac{\Delta, x{:}A, y{:}B, \Delta'\,;\,\Gamma \vdash M : C}{\Delta, y{:}B, x{:}A, \Delta'\,;\,\Gamma \vdash M : C}$$

3. *(Modal Contraction)*

$$\frac{\Delta, x{:}A, y{:}A, \Delta'\,;\,\Gamma \vdash M : C}{\Delta, w{:}A, \Delta'\,;\,\Gamma \vdash M[w, w/x, y] : C}$$

Proof. All by induction on the typing derivation of M. Most cases are standard. As an example, we discuss the case of $(\Box\mathcal{I})$ for weakening.

If $\Delta, \Delta'\,;\,\Gamma \vdash M : A$ by $(\Box\mathcal{I}_{\mathsf{K}})$, then $M \equiv \mathsf{box}\, N$ and $A \equiv \Box B$ for N and B such that $\cdot\,;\,\Delta, \Delta' \vdash N : B$. We use Theorem 9 to deduce that $\cdot\,;\,\Delta, x{:}A, \Delta' \vdash N : B$, and then a single use of $(\Box\mathcal{I}_{\mathsf{K}})$ yields the result.

If $\Delta, \Delta'\,;\,\Gamma \vdash M : A$ by $(\Box\mathcal{I}_{\mathsf{K4}})$, then $M \equiv \mathsf{box}\, N$ and $A \equiv \Box B$ for N and B such that $\Delta, \Delta'; \Delta^{\perp}, \Delta'^{\perp} \vdash N^{\perp} : B$. By the IH, we have that $\Delta, u{:}A, \Delta'; \Delta^{\perp}, \Delta'^{\perp} \vdash N^{\perp} : B$. We use Theorem 9 to deduce that $\Delta, u{:}A, \Delta'\,;\,\Delta^{\perp}, u^{\perp}{:}A, \Delta'^{\perp} \vdash N^{\perp} : B$, and then a single use of $(\Box\mathcal{I}_{\mathsf{K4}})$ yields the result.

The cases for $(\Box\mathcal{I}_{\mathsf{GL}})$ and $(\Box\mathcal{I}_{\mathsf{S4}})$ are similar. □

Theorem 11 (Modal Cut)**.** *The following rules are admissible:*

1. *(Modal Cut for DK)*

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

2. *(Modal Cut for DK4)*

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

3. *(Modal Cut for DGL)*

$$\frac{\Delta\,;\Delta^{\perp}, z^{\perp} : \Box A \vdash_{DGL} N^{\perp} : A \quad \Delta, u{:}A, \Delta'\,;\Gamma \vdash_{DGL} M : C}{\Delta, \Delta'\,;\Gamma \vdash_{DGL} M\,[N\,[\mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ N/z]\,/u] : C}$$

4. *(Modal Cut for DS4)*

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

5. *(Modal Cut for DT)*

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

Proof. By induction on the typing derivation of M.

We show the case for ($\Box\mathcal{I}$), and—for DS4 and DT—the case for modal variables ($\Box$var).

1. (DK) If $\Delta, u{:}A, \Delta'\,;\Gamma \vdash M : C$ by ($\Box\mathcal{I}_{\mathsf{K}}$), then $M \equiv \mathsf{box}\ M'$, $C \equiv \Box C'$, and

$$\cdot\,;\Delta, u{:}A, \Delta' \vdash M' : C'$$

   By Theorem 9, we have

$$\cdot\,;\Delta, \Delta' \vdash M'[N/u] : C$$

   and hence $\Delta, \Delta'\,;\Gamma \vdash \mathsf{box}\,(M'[N/u]) : \Box C' \equiv C$ by an application of ($\Box\mathcal{I}_{\mathsf{K}}$). But

$$\mathsf{box}\ (M'[N/u]) \equiv (\mathsf{box}\ M')\,[N/u] \equiv M[N/u]$$

   and hence we have the result.

2. (DK4) If $\Delta, u{:}A, \Delta' ; \Gamma \vdash M : C$ by $(\Box\mathcal{I}_{\mathsf{K4}})$, then $M \equiv \mathsf{box}\ M'$, $C \equiv \Box C'$, and

$$\Delta, u{:}A, \Delta' ; \Delta^{\perp}, u^{\perp}{:}A, \Delta'^{\perp} \vdash M'^{\perp} : C'$$

By the IH, we have

$$\Delta, \Delta' ; \Delta^{\perp}, u^{\perp}{:}A, \Delta'^{\perp} \vdash M'^{\perp}[N/u] : C'$$

and by Theorem 9, that yields

$$\Delta, \Delta' ; \Delta^{\perp}, \Delta'^{\perp} \vdash M'^{\perp}[N, N^{\perp}/u, u^{\perp}] : C'$$

But, by Theorem 7, we have that $M'^{\perp}[N, N^{\perp}/u, u^{\perp}] \equiv (M'[N/u])^{\perp}$, and hence by a use of $(\Box\mathcal{I}_{\mathsf{K4}})$, we have

$$\Delta, \Delta' ; \Gamma \vdash \mathsf{box}\ (M'[N/u]) : \Box C' \equiv C$$

and hence the result.

3. (DGL) If $\Delta, u{:}A, \Delta' ; \Gamma \vdash M : C$ by $(\Box\mathcal{I}_{\mathsf{GL}})$, then $M \equiv \mathsf{fix}\ y\ \mathsf{in}\ \mathsf{box}\ M'$, $C \equiv \Box C'$, and

$$\Delta, u{:}A, \Delta' ; \Delta^{\perp}, u^{\perp}{:}A, \Delta'^{\perp}, y^{\perp} : \Box C' \vdash M'^{\perp} : C'$$

Write $N_* \stackrel{\text{def}}{=} N[\mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ N/z]$. By the first premise and the IH, we have that

$$\Delta, \Delta' ; \Delta^{\perp}, u^{\perp}{:}A, \Delta'^{\perp}, y^{\perp} : \Box C' \vdash M'^{\perp}\,[N_*/u] : C'$$

We now need to substitute for $u^{\perp}$. By an application of $(\Box\mathcal{I}_{\mathsf{GL}})$ to the first premise we have

$$\Delta ; \Delta^{\perp} \vdash \mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ N : \Box A$$

and hence by Theorem 9 we substitute this into the first premise itself to get

$$\Delta ; \Delta^{\perp} \vdash N^{\perp}[\mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ N/z^{\perp}] : A$$

But $N_*^{\perp} \equiv N^{\perp}[\mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ N/z^{\perp}]$, so by weakening and Theorem 9, we obtain

$$\Delta, \Delta' ; \Delta^{\perp}, \Delta'^{\perp}, y^{\perp} : \Box C \vdash M'^{\perp}[N_*, N_*^{\perp}/u, u^{\perp}] : C'$$

But by well-definedness of contexts, $u^{\perp} \notin \mathrm{FV}\,(M)$, so by Theorem 7 we have that $M'^{\perp}[N_*, N_*^{\perp}/u, u^{\perp}] \equiv (M'[N_*/u])^{\perp}$, and hence by a use of $(\Box\mathcal{I}_{\mathsf{GL}})$, we have

$$\Delta, \Delta' ; \Gamma \vdash \mathsf{fix}\ y\ \mathsf{in}\ \mathsf{box}\ (M'[N_*/u]) : \Box C' \equiv C$$

and hence the result.

4. (DS4)

   - If $\Delta, u{:}A, \Delta' ; \Gamma \vdash M : C$ by $(\Box\mathcal{I}_{\mathsf{S4}})$ then $M \equiv \mathsf{box}\, M'$ and $C \equiv \Box C'$ with

     $$\Delta, u{:}A, \Delta' ; \cdot \vdash M' : C$$

     The IH then yields $\Delta, \Delta' ; \cdot \vdash M'[N/u] : C$, and a single use of $(\Box\mathcal{I}_{\mathsf{S4}})$ yields the result.

   - If $\Delta, u{:}A, \Delta' ; \Gamma \vdash M : C$ by $(\Box\mathsf{var})$ then $M \equiv v$ for some v such that $(v : C) \in \Delta, u{:}A, \Delta'$. There are two cases:
     - $u \equiv v$: then $M[N/u] \equiv N$ and $A \equiv C$. The premise $\Delta ; \cdot \vdash N : A$ along with weakening for both contexts yields the result.
     - $u \not\equiv v$: then $M[N/u] \equiv M$, and u does not occur in M. It is easy to show that if $\Delta, u{:}A, \Delta' ; \Gamma \vdash M : C$ and $u \notin \mathrm{FV}_{\geq 1}(M)$ then $\Delta, \Delta' ; \Gamma \vdash M : C$.

5. (DT)

   - If $\Delta, u{:}A, \Delta' ; \Gamma \vdash M : C$ by $(\Box\mathcal{I}_{\mathsf{K}})$ then we proceed as in the case of DK.
   - If $\Delta, u{:}A, \Delta' ; \Gamma \vdash M : C$ by $(\Box\mathsf{var})$ then $M \equiv v$ for some v such that $v : C \in \Delta, u{:}A, \Delta'$. There are two cases:
     - $u \equiv v$: then $M[N/u] \equiv N$ and $A \equiv C$. The premise $\cdot ; \Delta \vdash N : A$ along with Theorem 12 yields $\Delta ; \cdot \vdash N : A$. A series of weakenings for both contexts then yields the result.
     - $u \not\equiv v$: then $M[N/u] \equiv M$, and u does not occur in M. It is easy to show that if $\Delta, u{:}A, \Delta' ; \Gamma \vdash M : C$ and $u \notin \mathrm{FV}_{\geq 1}(M)$ then $\Delta, \Delta' ; \Gamma \vdash M : C$.

□

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

Theorem 12 (Modal Dereliction)**.** *If $\mathcal{S} \in \{DS4, DT\}$, then the following rule is admissible:*

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

Proof. By induction on the derivation of $\Delta\,;\Gamma,\Gamma' \vdash M : A$. Most cases are straightfoward, except (var) and ($\Box\mathcal{I}_{\mathsf{S4}}$)/($\Box\mathcal{I}_{\mathsf{K}}$)

If the judgment holds by (var), then $M \equiv x$ for some $(x : A) \in \Gamma, \Gamma'$. If $(x : A) \in \Gamma$, we use ($\Box\mathsf{var}$) to conclude that $\Delta, \Gamma\,;\Gamma' \vdash x : A$. If $(x : A) \in \Gamma'$, then another use of (var) suffices.

If the judgment holds by ($\Box\mathcal{I}_{\mathsf{S4}}$) then $M \equiv \mathsf{box}\ M'$ and $A \equiv \Box A'$ for some M', A' with $\Delta\,;\cdot \vdash M' : A'$. Repeated use of weakening for the modal context followed by an application of ($\Box\mathcal{I}_{\mathsf{S4}}$) yields the result.

The case of ($\Box\mathcal{I}_{\mathsf{K}}$) is similar, but uses weakening for the intuitionistic context. □

4.4 Equivalence with Hilbert systems

In this section we prove that our dual-context λ-calculi correspond to the negative fragment of the Hilbert systems for the logics we defined in §2. An extension to the full fragment should be straightforward. This ties the knot with respect to the Curry-Howard isomorphism.

The translation under which this equivalence is shown is indeed the same one that we used in §3 to derive our calculi:

$$\Delta\,;\Gamma \vdash M : A \qquad \rightsquigarrow \qquad \Box\hat{\Delta}, \hat{\Gamma} \vdash_{\mathcal{H}} A$$

The only difference is that now the proof term M is visible, and we write $\hat{\Gamma}$ to mean the context Γ with all the variables removed: if $\Gamma \equiv x_1 : A_1, \ldots, x_n : A_n$, then

$$\hat{\Gamma} \stackrel{\text{def}}{=} A_1, \ldots, A_n$$

One direction of the proof involves showing that the axioms are indeed derivable in the dual-context systems. The other direction involves showing the admissibility of the dual-context rules in the Hilbert systems.

4.4.1 Hilbert to Dual

First and foremost, we need to show that axiom (K) is derivable. It is easy to check that the term

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

has type $\Box(A \to B) \to \Box A \to \Box B$ in all our systems. For the case of GL, we instead use

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

It is also not hard to see that in DK4 and DS4 the terms

$$\mathsf{ax_4} \stackrel{\text{def}}{=} \lambda x : \Box A.\ \mathsf{let\ box}\ y \Leftarrow x\ \mathsf{in\ box}\ (\mathsf{box}\ y)$$

have type $\Box A \to \Box\Box A$; that is, axiom 4.

In the case of DGL, we need to show that the term

$$\mathsf{ax_{GL}} \stackrel{\text{def}}{=} \lambda x : \Box(\Box A \to A).\ \mathsf{let\ box}\ f \Leftarrow x\ \mathsf{in}\ (\mathsf{fix}\ z\ \mathsf{in\ box}\ (f\ z))$$

has type $\Box(\Box A \to A) \to \Box A$. The most interesting part of the derivation can be found in Figure 4.2.

Figure 4.2: Derivation of the Gödel-Löb axiom in DGL

$$\dfrac{\dfrac{}{\cdots \vdash x : \Box(\Box A \to A)} \quad \dfrac{\begin{array}{c}\vdots \\ \Delta, f : \Box A \to A\,;\, \Delta, f^{\perp} : \Box A \to A, z^{\perp} : \Box A \vdash f^{\perp}\ z^{\perp} : A\end{array}}{\Delta, f : \Box A \to A\,;\, \Gamma, x : \Box(\Box A \to A) \vdash \mathsf{fix}\ z\ \mathsf{in\ box}\ (f\ z) : \Box A}}{\Delta\,;\, \Gamma, x : \Box(\Box A \to A) \vdash \mathsf{let\ box}\ f \Leftarrow x\ \mathsf{in}\ (\mathsf{fix}\ z\ \mathsf{in\ box}\ (f\ z)) : \Box(\Box A \to A) \to \Box A}$$
$$\Delta\,;\, \Gamma \vdash \lambda x : \Box(\Box A \to A).\ \mathsf{let\ box}\ f \Leftarrow x\ \mathsf{in}\ (\mathsf{fix}\ z\ \mathsf{in\ box}\ (f\ z)) : \Box(\Box A \to A) \to \Box A$$

Finally, in DT and DS4, the term

$$\mathsf{ax_T} \stackrel{\text{def}}{=} \lambda x : \Box A.\ \mathsf{let\ box}\ y \Leftarrow x\ \mathsf{in}\ y$$

has type $\Box A \to A$, i.e. axiom T.

With all that, we can show:

Theorem 13 (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 $\cdot\,;\Gamma \vdash_{D\mathcal{L}} M : A$.*

Proof. By induction on the derivation of $\hat{\Gamma} \vdash_{\mathcal{L}} A$. In the case of the assumption rule, we use (var) to type the associated variable in $\hat{\Gamma}$. The cases for axioms of IPL are easy. For the modal axioms, we use the terms derived above. For modus ponens, we use application, i.e. $(\to \mathcal{E})$.

This leaves the case of necessitation. Suppose $\hat{\Gamma} \vdash_{\mathcal{L}} A$. Then $A \equiv \Box A'$, and $\vdash_{\mathcal{L}} A'$. By the IH, there is a term M' such that $\cdot\,;\cdot \vdash_{\mathsf{D}\mathcal{L}} M' : A'$. We then use the appropriate introduction rule for box—e.g. $(\Box\mathcal{I}_{\mathsf{K}})$, and so on—to yield the result. □

4.4.2 Dual to Hilbert

For the opposite direction, the essence lies in showing that the rules of the dual-context are admissible in the Hilbert system—that is, after erasing the proof terms. We have done most of the required work in §2.5.2.

Theorem 14 (Dual to Hilbert)**.** *If* $\Delta\,;\Gamma \vdash_{D\mathcal{L}} M : A$ *then* $\Box\hat{\Delta}, \hat{\Gamma} \vdash_{\mathcal{L}} A$.

Proof. By induction on the derivation of $\Delta\,;\Gamma \vdash_{\mathsf{D}\mathcal{L}} M : A$.

If the premise holds by (var), then we use the assumption rule of the Hilbert system. If the last step in the derivation of the premise is the rule ($\to \mathcal{I}$), we use the IH followed by the Deduction Theorem (Theorem 2). If the last step is by ($\to \mathcal{E}$), we use modus ponens. It is simple to translate the rules that pertain to the product, namely ($\times\mathcal{I}$) and ($\times\mathcal{E}_i$) to uses of the IPL axioms pertaining to the product along with modus ponens. It is also not hard to see that, under the given translation, ($\Box\mathcal{E}$) can also be matched by a use of the IH along with an invocation of the admissibility of cut for Hilbert systems (Theorem 1). Uses of the modal variable rule ($\Box\mathsf{var}$) can be imitated by a use of the assumption rule, modus ponens, and an instance of the T axiom.

This leaves the introduction rules for the box. The rule ($\Box\mathcal{I}_{\mathsf{K}}$) is matched with Scott's rule (Theorem 3). The rule ($\Box\mathcal{I}_{\mathsf{K4}}$) is matched with the Four rule (Theorem 5). The rule ($\Box\mathcal{I}_{\mathsf{GL}}$) is matched with the generalized Löb rule (Theorem 6). Finally, the rule ($\Box\mathcal{I}_{\mathsf{S4}}$) is matched with the corollary to the Four rule (Corollary 1). □

Chapter 5

Reduction

In this chapter we study a notion of reduction for the dual-context calculi we introduced in §4. Our reduction relation,

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

is defined in Figure 5.1, and it is essentially the standard notion of reduction previously considered by Pfenning and Davies (2001). A similar notion of reduction was studied in the context of Dual Intuitionistic Linear Logic (DILL) by Ohta and Hasegawa (2006). Unlike the work in *op. cit.* we do not study the full reduction including η-contractions and commuting conversions, and hence our work does not immediately yield a decision procedure for the equality that we will study in §8.1. However, the necessary extensions to the full reduction should be straightforward.

We first show that typing is preserved under reduction, and that reduction is largely preserved under complementation—that is, if the types are right. Furthermore, we show that the notion under consideration is confluent. We then briefly introduce the method of *candidates of reducibility*, and show that it can be used to demonstrate strong normalization. Finally, we discuss and introduce some *commuting conversions*, which are necessary for the subformula property to hold.

5.1 Preservation theorems

Theorem 15 (Subject reduction)**.** *If* $\Delta;\Gamma \vdash M : A$ *and* $M \longrightarrow N$*, then* $\Delta;\Gamma \vdash N : A$*.*

Proof. By induction on the generation of $M \longrightarrow N$. Most cases follow straightforwardly from the IH. The cases for the β rules follow from Theorems 9 and 11. □

Figure 5.1: Reduction

Rules for all calculi:

$$\frac{}{(\lambda x{:}A.\ M)N \longrightarrow M[N/x]}\ (\longrightarrow \beta) \qquad \frac{}{\pi_i(\langle M_1, M_2\rangle) \longrightarrow M_i}\ (\longrightarrow \beta_\times)$$

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

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

$$\frac{M \longrightarrow N}{MP \longrightarrow NP}\ (\mathsf{app}_1) \qquad \frac{P \longrightarrow Q}{MP \longrightarrow MQ}\ (\mathsf{app}_2)$$

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

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

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

Beta rule for non-GL:

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

Beta rule for GL:

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

The following theorem shall prove useful toward the end of the chapter, where we show that strong normalization satisfies the properties necessary for the *candidates of reducibility* method to apply.

Theorem 16 (Complement reduction)**.** *If* $\Delta\,;\,\Delta^\perp \vdash_{\mathsf{DK4}} M^\perp : A$ *or* $\Delta\,;\,\Delta^\perp, z^\perp : \Box A \vdash_{\mathsf{DGL}} M^\perp : A$*, then* $M \longrightarrow N$ *implies* $M^\perp \longrightarrow N^\perp$*.*

Proof. By induction on the generation of $M \longrightarrow N$. Most cases follow straightforwardly from the IH. In some cases we need to use renaming, weakening and then strengthening. The rest we show.

Case($\longrightarrow \beta$). It is easy to see that

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

But we have $\Delta\,;\,\Delta^\perp, x^\perp{:}A \vdash M^\perp : B$ for some A and B. Thus, $x^\perp \notin \textsc{Vars}\,(\Delta)$, and hence, by Theorem 8(4), $x^\perp \notin \textsc{fv}_{\geq 1}\left(M^\perp\right)$, which is equal to $\textsc{fv}_{\geq 1}\,(M)$ by Theorem 8(3). Also, $x^\perp \notin \textsc{fv}_0\,(M)$, for then we would have $x \in \textsc{fv}_0\left(M^\perp\right)$ and thus $x \in \textsc{Vars}\left(\Delta^\perp\right)$, contradicting well-formedness of contexts. It thus follows that $x^\perp \notin \textsc{fv}\,(M)$, and hence, by Theorem 7,

$$(M[N/x])^\perp \equiv M^\perp[N, N^\perp/x, x^\perp] \equiv M^\perp[N^\perp/x^\perp]$$

where the last α-equivalence follows because x is not free in $M^\perp$, for as $x^\perp \notin \textsc{Vars}\left(\Delta^\perp\right)$ we have $x \notin \textsc{Vars}\,(\Delta) \cup \textsc{Vars}\left(\Delta^\perp\right)$, and thus $x \notin \textsc{fv}\left(M^\perp\right)$, by Theorem 8(1, 4). The reasoning is similar for GL.

Case($\longrightarrow \beta_\Box$). It is easy to see that

$$\begin{aligned}(\mathsf{let\ box}\ u \Leftarrow \mathsf{box}\ M\ \mathsf{in}\ N)^\perp &\equiv \mathsf{let\ box}\ u \Leftarrow (\mathsf{box}\ M)^\perp\ \mathsf{in}\ N^\perp \\ &\equiv \mathsf{let\ box}\ u \Leftarrow \mathsf{box}\ M\ \mathsf{in}\ N^\perp \\ &\longrightarrow N^\perp[M/u]\end{aligned}$$

It now suffices to show that (a) $u^\perp \notin \textsc{fv}\,(N)$, and that (b) $u^\perp \notin \textsc{fv}\left(N^\perp\right)$. For, by (a), Theorem 7 applies and hence

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

But then, as $u^\perp \notin \textsc{fv}\left(N^\perp\right)$, the RHS is α-equivalent to $N^\perp[M/u]$, concluding the argument. Luckily, the restrictions we have put on contexts put together with the fact that

$$\Delta, u{:}A\,;\,\Delta^\perp \vdash N^\perp : A$$

suffice to yield the two desiderata.

For (a): by well-formedness of contexts, as $u \in \textsc{Vars}(\Delta, u{:}A)$, then $u^\perp \notin \textsc{Vars}(\Delta, u{:}A)$, and hence, $u^\perp \notin \textsc{fv}_{\geq 1}\left(N^\perp\right) = \textsc{fv}_{\geq 1}(N)$. Also, $u \notin \textsc{Vars}\left(\Delta^\perp\right)$, so $u \notin \textsc{fv}_0\left(N^\perp\right)$, and hence $u^\perp \notin \textsc{fv}_0(N)$. It follows that $u^\perp \notin \textsc{fv}(N)$.

For (b): by well-formedness of contexts again, $u \notin \textsc{Vars}(\Delta)$ and $u^\perp \notin \textsc{Vars}(\Delta)$. Hence $u^\perp \notin \textsc{Vars}\left(\Delta^\perp\right) \cup \textsc{Vars}(\Delta)$, and thus by Theorem 8 we have $u^\perp \notin \textsc{fv}\left(N^\perp\right)$.

$\textsc{Case}(\longrightarrow \beta_{\mathsf{GL}})$. Similarly to $(\longrightarrow \beta_{\Box})$.

□

5.2 Confluence

We will prove that

Theorem 17. *The reduction relation* $\longrightarrow$ *is confluent.*

There are many ways to do so. A classic strategy is to exploit the fact we prove in the next section, *viz.* that $\longrightarrow$ is strongly normalizing, and show *local confluence* followed by an appeal to *Newman's Lemma* (Newman, 1942; Mitchell, 1996; Terese, 2003).

We will use another method, namely that of *parallel reduction*, discovered by Tait and Martin-Löf. The basic outline of this method for the untyped λ-calculus is presented in (Barendregt, 1984, §3.2). Variations of it, as well as its history, are covered by Takahashi (1995). The idea is simple: we will introduce a second notion of reduction,

$$\Longrightarrow \subseteq \Lambda \times \Lambda$$

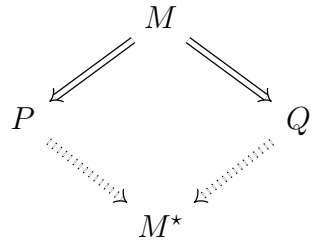
which we will 'sandwich' between reduction proper and its transitive closure:

$$\longrightarrow \;\subseteq \Longrightarrow \subseteq \longrightarrow^*$$

We will then show that $\Longrightarrow$ has the diamond property. By the above inclusions, the transitive closure $\Longrightarrow^*$ of $\Longrightarrow$ is then equal to $\longrightarrow^*$, and hence $\longrightarrow$ is Church-Rosser.

In fact, we will follow Takahashi (1995) in doing something better: we will define for each term M its *complete development*, $M^\star$. The complete development is intuitively defined by 'unrolling' all the redexes of M at once. We will then show that if

$M \Longrightarrow N$, then $N \Longrightarrow M^\star$. $M^\star$ will then suffice to close the diamond:



The parallel reduction $\Longrightarrow$ is defined in Figure 5.2. It is immediate that

Lemma 3. $\Longrightarrow$ *is reflexive.*

Proof. It is easy to show that $M \Longrightarrow M$ by induction on M. □

We define

Definition 3 (Complete development)**.** The *complete development* $M^\star$ of a term M is defined by the following clauses:

$$
\begin{aligned}
x^\star &\stackrel{\text{def}}{=} x \\
(\langle M, N\rangle)^\star &\stackrel{\text{def}}{=} \langle M^\star, N^\star\rangle \\
(\pi_i(\langle M_1, M_2\rangle))^\star &\stackrel{\text{def}}{=} M_i^\star \\
(\pi_i\,(M))^\star &\stackrel{\text{def}}{=} \pi_i(M^\star) \\
(\lambda x{:}A.\ M)^\star &\stackrel{\text{def}}{=} \lambda x{:}A.\ M^\star \\
((\lambda x{:}A.\ M)\,N)^\star &\stackrel{\text{def}}{=} M^\star[N^\star/x] \\
(MN)^\star &\stackrel{\text{def}}{=} M^\star N^\star \\
(\mathsf{box}\ M)^\star &\stackrel{\text{def}}{=} \mathsf{box}\ M^\star \\
(\mathsf{let\ box}\ u \Leftarrow \mathsf{box}\ M\ \mathsf{in}\ N)^\star &\stackrel{\text{def}}{=} N^\star[M^\star/u] \\
(\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N)^\star &\stackrel{\text{def}}{=} \mathsf{let\ box}\ u \Leftarrow M^\star\ \mathsf{in}\ N^\star
\end{aligned}
$$

and, in the case of GL,

$$
\begin{aligned}
(\mathsf{fix}\ z\ \mathsf{in\ box}\ M)^\star &\stackrel{\text{def}}{=} \mathsf{fix}\ z\ \mathsf{in\ box}\ M^\star \\
(\mathsf{let\ box}\ u \Leftarrow \mathsf{fix}\ z\ \mathsf{in\ box}\ M\ \mathsf{in}\ N)^\star &\stackrel{\text{def}}{=} N^\star\,[M^\star[\mathsf{fix}\ z\ \mathsf{in\ box}\ M^\star/z]/u]
\end{aligned}
$$

First, a little lemma capturing the essence of parallel reduction:

Lemma 4. *If* $M \Longrightarrow N$ *and* $P \Longrightarrow Q$*, then*

$$M[P/x] \Longrightarrow N[Q/x]$$

Figure 5.2: Parallel Reduction

Rules for all calculi:

$$\frac{}{x \Longrightarrow x}\ (\mathsf{var})$$

$$\frac{M \Longrightarrow N \qquad P \Longrightarrow Q}{(\lambda x{:}A.\ M)P \Longrightarrow N[Q/x]}\ (\to \beta) \qquad \frac{M_i \Longrightarrow N}{\pi_i(\langle M_1, M_2\rangle) \Longrightarrow N}\ (\times\beta)$$

$$\frac{M \Longrightarrow N}{\pi_i(M) \Longrightarrow \pi_i(N)}\ (\mathsf{cong}_{\pi_i}) \qquad \frac{M_1 \Longrightarrow N_1 \qquad M_2 \Longrightarrow N_2}{\langle M_1, M_2\rangle \Longrightarrow \langle N_1, N_2\rangle}\ (\mathsf{cong}_{\times})$$

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

$$\frac{M \Longrightarrow N \qquad P \Longrightarrow Q}{MP \Longrightarrow NQ}\ (\mathsf{app}) \qquad \frac{M \Longrightarrow N}{\mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ M \Longrightarrow \mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ N}\ (\mathsf{cong}_{\mathsf{fix}})$$

$$\frac{M \Longrightarrow N \qquad P \Longrightarrow Q}{\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ P \Longrightarrow \mathsf{let\ box}\ u \Leftarrow N\ \mathsf{in}\ Q}\ (\mathsf{letbox})$$

Beta rule for non-GL:

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

Beta rule for GL:

$$\frac{M \Longrightarrow N \qquad P \Longrightarrow Q}{\mathsf{let\ box}\ u \Leftarrow \mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ P\ \mathsf{in}\ M \Longrightarrow N\left[Q\left[\mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ Q/z\right]/u\right]}\ (\Box\beta_{\mathsf{GL}})$$

Proof. By induction on the generation of $M \Longrightarrow N$. The cases for congruence rules and ($\Longrightarrow \beta_\times$) follow simply by the IH, so we omit them.

CASE(var). Then $M \Longrightarrow N$ is $z \Longrightarrow z$ for some z. If $z \equiv x$, we have $M[P/x] \equiv P$ and $N[Q/x] \equiv Q$, and the result follows because $P \Longrightarrow Q$. Otherwise, $M[P/x] \equiv z \equiv N[Q/x]$ and the result follows by Lemma 3.

CASE($\to \beta$). Then $(\lambda x'{:}A.\ M)N \Longrightarrow N'[M'/x']$, where $M \Longrightarrow M'$ and $N \Longrightarrow N'$. Then

$$((\lambda x'{:}A.\ M)N)\,[P/x] \equiv (\lambda x'{:}A.\ M[P/x])(N[P/x])$$

But, by the IH, $M[P/x] \Longrightarrow M'[Q/x]$ and $N[P/x] \Longrightarrow N'[Q/x]$. So, by the rules ($\mathsf{cong}_\lambda$) and ($\mathsf{app}$), and then rule ($\Longrightarrow \beta$), we have

$$(\lambda x'{:}A.\ M[P/x])(N[P/x]) \Longrightarrow M'[Q/x]\,[N'[Q/x]/x']$$

But this last is α-equivalent to $(M'[N'/x'])\,[Q/x]$ by the substitution lemma.

CASE($\Box\beta$). Similar to ($\Longrightarrow \beta$).

CASE($\Box\beta_{\mathsf{GL}}$). Then

$$\mathsf{let\ box}\ u \Leftarrow \mathsf{fix}\ z\ \mathsf{in\ box}\ M\ \mathsf{in}\ N \Longrightarrow N'[M'[\mathsf{fix}\ z\ \mathsf{in\ box}\ M'/z]/u]$$

with $M \Longrightarrow M'$ and $N \Longrightarrow N'$. We have

$$\begin{aligned}
&(\mathsf{let\ box}\ u \Leftarrow \mathsf{fix}\ z\ \mathsf{in\ box}\ M\ \mathsf{in}\ N)\,[P/x] \\
\equiv\ &\mathsf{let\ box}\ u \Leftarrow \mathsf{fix}\ z\ \mathsf{in\ box}\ M[P/x]\ \mathsf{in}\ N[P/x] \\
\Longrightarrow\ &N'[Q/x]\,[M'[Q/x]\,[\mathsf{fix}\ z\ \mathsf{in\ box}\ M'[Q/x]/z]\,/u]
\end{aligned}$$

where the last step follows because, by the IH, $M[P/x] \Longrightarrow M'[Q/x]$ and $N[P/x] \Longrightarrow N'[Q/x]$. This last—by two uses of the substitution lemma—is α-equivalent to

$$N'[M'[\mathsf{fix}\ z\ \mathsf{in\ box}\ M'/z]/u][Q/x]$$

□

And here is the main result:

Theorem 18. *If $M \Longrightarrow P$, then $P \Longrightarrow M^\star$.*

Proof. By induction on the generation of $M \Longrightarrow P$. The case of the variable rule is trivial, and the cases of congruence rules follow from the IH. We show the rest.

Case($\to \beta$). Then we have $(\lambda x{:}A.\ M)N \Longrightarrow M'[N'/x]$, with $M \Longrightarrow M'$ and $N \Longrightarrow N'$. By the IH, $M' \Longrightarrow M^\star$ and $N' \Longrightarrow N^\star$. Then, by Lemma 4, $M'[N'/x] \Longrightarrow M^\star[N^\star/x] \equiv (\lambda x{:}A.\ M)N)^\star$.

Case($\times\beta$). Then we have $\pi_i(\langle M_1, M_2\rangle) \Longrightarrow M_i'$, with $M_i \Longrightarrow M_i'$. By the IH, $M_i' \Longrightarrow M_i^\star \equiv (\pi_i(\langle M_1, M_2\rangle))^\star$.

Case(). Then we have

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

where $M \Longrightarrow M'$ and $N \Longrightarrow N'$. By the IH, $M' \Longrightarrow M^\star$ and $N' \Longrightarrow N^\star$. It follows that

$$N'[M'/u] \Longrightarrow N^\star[M^\star/u] \equiv (\mathsf{let\ box}\ u \Leftarrow \mathsf{box}\ M\ \mathsf{in}\ N)^\star$$

by Lemma 4.

Case($\Box\beta_{\mathsf{GL}}$). Then we have

$$\mathsf{let\ box}\ u \Leftarrow \mathsf{fix}\ z\ \mathsf{in\ box}\ M\ \mathsf{in}\ N \Longrightarrow N'[M'[\mathsf{fix}\ z\ \mathsf{in\ box}\ M'/z]/u]$$

with $M \Longrightarrow M'$ and $N \Longrightarrow N'$. By the IH, $M' \Longrightarrow M^\star$ and $N' \Longrightarrow N^\star$. It follows by ($\mathsf{cong}_{\mathsf{fix}}$) that $\mathsf{fix}\ z\ \mathsf{in\ box}\ M' \Longrightarrow \mathsf{fix}\ z\ \mathsf{in\ box}\ M^\star$, and thus, by Lemma 4, that

$$M'[\mathsf{fix}\ z\ \mathsf{in\ box}\ M'/z] \Longrightarrow M^\star[\mathsf{fix}\ z\ \mathsf{in\ box}\ M^\star/z]$$

Hence, by Lemma 4 again, we have that

$$N'[M'[\mathsf{fix}\ z\ \mathsf{in\ box}\ M'/z]/u] \Longrightarrow N^\star[M^\star[\mathsf{fix}\ z\ \mathsf{in\ box}\ M^\star/z]/u]$$

□

5.3 Strong Normalization

In this section, we will prove that

Theorem 19. *The reduction relation $\longrightarrow$ is strongly normalizing.*

We shall do 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 relations*—or, in this particular case, logical predicates. 'Candidats'

was invented primarily by Girard (1972) to prove strong normalization for System F, which is covered in (Girard et al., 1989, §14). The particular variant we use is a mixture of the versions of Girard and Koletsos (1985). An elementary presentation of the latter may be found in (Gallier, 1995). For a discussion of other closely related variants see Gallier (1990).

The overall structure of the method is the following: Suppose we have a family of nonempty *sets of typing judgments*,

$$\mathcal{P} = \{P_A\}_A$$

indexed by the type A they assign to the term they carry. We will state six properties, (P0)–(P5), that such a family should satisfy. In case it does indeed satisfy them, we show that P_A contains all judgments $\Delta\,;\Gamma \vdash M : A$ with type A.

In our case, we show that the family of derivable typing judgments

$$\mathcal{SN} \stackrel{\text{def}}{=} \{SN_A\}_A$$

satisfies the properties (P0) through (P5), where SN_A consists of all the judgments $\Delta;\Gamma \vdash M : A$ just if M is strongly normalizing with respect to $\longrightarrow$. Then $SN_A = \Lambda_A$, and all typable terms are strongly normalizing.

The requisite properties follow. If $C \subseteq P_A$, we write

$$\Delta\,;\Gamma \vdash M \in C$$

as a shorthand for $(\Delta\,;\Gamma \vdash M : A) \in C$.

Definition 4.

1. A term is a *I-term* just if it is an introduction form, i.e. of the form

$$\lambda x{:}A.\ M, \qquad \langle M, N\rangle, \qquad \mathsf{box}\ M, \qquad \mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ M \quad (\text{for } \mathsf{GL} \text{ only})$$

2. A term is a *simple term*[1] just if it is a variable or an elimination form, i.e. of the form

$$x, \qquad MN, \qquad \pi_i(M), \qquad \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N$$

3. A *stubborn* term is a simple term that is either a normal form, or a term that does not reduce to a I-term.

[1]Girard (Girard et al., 1989) calls these *neutral terms*, which also means something entirely different in the programming language literature.

Definition 5 (Properties P0-P3)**.** We define the following properties pertaining to the family $\mathcal{P}$.

(P0) (a) $\Delta\,;\Gamma \vdash M \in P_A$ and $\Gamma \sqsubseteq \Gamma'$ imply $\Delta\,;\Gamma' \vdash M \in P_A$

(b) $\Delta\,;\Gamma \vdash M \in P_A$ and $\Delta \sqsubseteq \Delta'$ imply $\Delta'\,;\Gamma \vdash M \in P_A$

(c) (for T and S4 only) $\Delta\,;\Gamma,\Gamma' \vdash M \in P_A$ implies $\Delta,\Gamma\,;\Gamma' \vdash M \in P_A$

(P1) $\Delta\,;\Gamma \vdash x \in P_A$ for all variables x.

(P2) $M \in P_A$ and $M \longrightarrow N$ imply $N \in P_A$.

(P3) For simple terms M,

(a) If

- $\Delta\,;\Gamma \vdash M \in P_{A\to B}$,
- $\Delta\,;\Gamma \vdash N \in P_A$, and
- whenever $M \longrightarrow^* \lambda x{:}A.M'$ then $\Delta\,;\Gamma \vdash (\lambda x{:}A.M')N \in P_B$

then this implies $\Delta\,;\Gamma \vdash MN \in P_B$.

(b) If

- $\Delta\,;\Gamma \vdash M \in P_{A\times B}$, and
- whenever $M \longrightarrow^* \langle M_1, M_2\rangle$ then $\Delta\,;\Gamma \vdash \pi_1(\langle M_1, M_2\rangle) \in P_A$ and $\Delta\,;\Gamma \vdash \pi_2(\langle M_1, M_2\rangle) \in P_B$,

then this implies that $\Delta\,;\Gamma \vdash \pi_1(M) \in P_A$ and $\Delta\,;\Gamma \vdash \pi_2(M) \in P_B$.

Definition 6 (Properties P4-P5)**.**

(P4) (a) If $\Delta\,;\Gamma, x{:}A \vdash M \in P_B$ then $\Delta\,;\Gamma \vdash \lambda x{:}A.\ M \in P_{A\to B}$.

(b) $\Delta\,;\Gamma \vdash M \in P_A$ and $\Delta\,;\Gamma \vdash N \in P_B$ imply $\Delta\,;\Gamma \vdash \langle M, N\rangle \in P_{A\times B}$.

(c)

i. (for K and T) $\cdot\,;\Delta \vdash M \in P_A$ implies $\Delta\,;\Gamma \vdash \mathsf{box}\ M \in P_{\Box A}$

ii. (for K4) $\Delta\,;\Delta^\perp \vdash M^\perp \in P_A$ implies $\Delta\,;\Gamma \vdash \mathsf{box}\ M \in P_{\Box A}$

iii. (for GL) $\Delta\,;\Delta^\perp, z^\perp : \Box A \vdash M^\perp \in P_A$ implies $\Delta\,;\Gamma \vdash \mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ M \in P_{\Box A}$

iv. (for S4) $\Delta\,;\cdot \vdash M \in P_A$ implies $\Delta\,;\Gamma \vdash \mathsf{box}\ M \in P_{\Box A}$

(P5) (a) If $\Delta' \sqsupseteq \Delta$ and $\Gamma' \sqsupseteq \Gamma$ satisfy $\Delta'\,;\Gamma' \vdash N \in P_A$ and $\Delta'\,;\Gamma' \vdash M[N/x] \in P_B$, then $\Delta'\,;\Gamma' \vdash (\lambda x{:}A.\ M)N \in P_B$.

(b) $\Delta\,;\Gamma \vdash M \in P_A$ and $\Delta\,;\Gamma \vdash N \in P_B$ imply $\Delta\,;\Gamma \vdash \pi_1(\langle M, N\rangle) \in P_A$ and $\Delta\,;\Gamma \vdash \pi_2(\langle M, N\rangle) \in P_B$.

(c) i. (for non-GL) If we have $\Delta\,;\Gamma \vdash M \in P_{\Box A}$ and $\Delta, u{:}A\,;\Gamma \vdash N \in P_C$, and whenever $M \longrightarrow^* \mathsf{box}\, Q$ then $\Delta\,;\Gamma \vdash N[Q/u] \in P_C$, then we have that $\Delta\,;\Gamma \vdash \mathsf{let\ box}\, u \Leftarrow M\ \mathsf{in}\ N \in P_C$.

ii. (for GL only) If we have $\Delta;\Gamma \vdash M \in P_{\Box A}$ and $\Delta, u{:}A;\Gamma \vdash N \in P_C$, and whenever $M \longrightarrow^* \mathsf{fix}\, z\ \mathsf{in\ box}\, Q$ then $\Delta;\Gamma \vdash N\,[Q[\mathsf{fix}\, z\ \mathsf{in\ box}\, Q/z]/u] \in P_C$, then we have that $\Delta\,;\Gamma \vdash \mathsf{let\ box}\, u \Leftarrow M\ \mathsf{in}\ N \in P_C$.

Showing that these properties indeed guarantee that $P_A = \Lambda_A$ consists of a laborious inductive argument that employs multiple lemmata. The full argument in all its tediousness may be found in §6. In this chapter we shall content ourselves by showing that the family $\mathcal{SN}$ indeed satisfies the properties (P0)-(P5).

In carrying out the proof we shall often proceed by induction on $d(M)$, the *depth of the term* M. Let there be a tree consisting of M and all its reducts, with an edge from reduct M_1 to reduct M_2 just if $M_1 \longrightarrow M_2$. This is the *reduction tree* of M. As M has at most finite redexes, the reduction tree is finitely branching: there can only be a finite number of terms M_i such that $N \longrightarrow^* M_i$ for any term N. Furthermore, if M is strongly normalizing, then the reduction tree has no infinite paths. By König's Lemma, the tree is then finite, and $d(M)$ is the depth of the reduction tree of M—i.e. the longest path in the tree that is rooted at M.

(P0)–(P2) Trivial.

(P3)

(a) We prove that MN is strongly normalizing, by induction on $d(M)+d(N)$.

Suppose $MN \longrightarrow P$. As M is simple, MN cannot be a redex, so it is of the form $P \equiv M'N'$ such that either (a) $M \longrightarrow M'$ and $N' \equiv N$, or (b) $N \longrightarrow N'$ and $M' \equiv M$.

If either M' is simple, or if $M' \equiv M$ and the reduction $N \longrightarrow N'$ took place, then

$$d(M') + d(N') < d(M) + d(N)$$

and so, by the IH, $P \equiv M'N'$ is strongly normalizing.

Otherwise, we have $M' \equiv \lambda x{:}A.M''$ and $N' \equiv N$. The assumption applies, and $M'N$ is strongly normalizing.

(b) Similar to (P3)(a).

(P4) All cases are very similar; we show (c)(ii), namely the case for $\mathsf{K4}$.

If $\mathsf{box}\, M \longrightarrow P$, then $P \equiv \mathsf{box}\, N$ for some N, and $M \longrightarrow N$. Hence $d(\mathsf{box}\, M) \leq d(M)$. But the last one is, by Theorem 16, equal to $d(M^{\perp})$, which is finite as $M^{\perp}$ is strongly normalizing.

(P5)

(a) First, we note that by substituting x for N, the premise implies that M is strongly normalizing, and thus that both $d(M)$ and $d(N)$ are finite.

We now proceed by induction on $d(M) + d(N)$. If $(\lambda x{:}A.\ M)N \longrightarrow P$, then there are three possibilities:

- $P \equiv (\lambda x{:}A.\ M')N$ and $M \longrightarrow M'$. Then

$$d(M') + d(N) < d(M) + d(N)$$

  and so, by the IH, P is strongly normalizing.
- $P \equiv (\lambda x{:}A.\ M)N'$ and $N \longrightarrow N'$. Then

$$d(M) + d(N') < d(M) + d(N)$$

  and so, by the IH, P is strongly normalizing.
- $P \equiv M[N/x]$. Then, by assumption, P is strongly normalizing.

In all cases, if $(\lambda x{:}A.\ M)N \longrightarrow P$, then P is strongly normalizing. We conclude that the original term itself is strongly normalizing.

(b) Similar to (a).

(c)

(i) First, we note that by substituting u for Q, the premise implies that N is strongly normalizing, and thus that both $d(M)$ and $d(N)$ are finite. We now proceed by induction on $d(M)+d(N)$. If $\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N \longrightarrow P$, then there are three possibilities:

- $P \equiv \mathsf{let\ box}\ u \Leftarrow M'\ \mathsf{in}\ N$ and $M \longrightarrow M'$. Then

$$d(M') + d(N) < d(M) + d(N)$$

  and so, by the IH, P is strongly normalizing.
- Likewise for N.

– $M \equiv \mathsf{box}\, Q$ and $P \equiv N[Q/u]$. Then, by assumption, P is strongly normalizing.

In all cases, if $\mathsf{let\ box}\, u \Leftarrow M\ \mathsf{in}\ N \longrightarrow P$, then P is strongly normalizing. We conclude that the original term itself is strongly normalizing.

(ii) Similar to (i).

5.4 Subformula Property

The notion of reduction we have studied in this chapter 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 Prawitz (1965) and Girard et al. (1989) for a fuller discussion of these points.

Let us return to our systems: they do not satisfy the subformula property because of the elimination rule:

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

Notice that the conclusion C is given to us by the *minor premise* $\Delta, u{:}A\,;\Gamma \vdash N : C$, and it is *structurally unrelated* to $\Box A$, the major premise that is being eliminated: in Girard's terminology, it is *parasitic*. This is so because the elimination rule is secretly a kind of *cut rule*, or a rule in the style of Schroeder-Heister (1984).

It is not so easy at first to see where the actual trouble with this kind of rule is; the point is that the $\mathsf{let\ box}\, u \Leftarrow (-)\ \mathsf{in}\ (-)$ construct may 'hide redexes' that should be reduced. Once we introduce the extra reductions that are needed and prove the subformula property this will become quite clear. But—in the meantime—let us consider three examples.

Suppose that $\Delta, u{:}A\,;\Gamma \vdash \langle N_1, N_2\rangle : A_1 \times A_2$, and that $\Delta\,;\Gamma \vdash M : \Box A$. We may use $(\Box\mathcal{E})$ to obtain

$$\Delta\,;\Gamma \vdash \mathsf{let\ box}\, u \Leftarrow M\ \mathsf{in}\ \langle N_1, N_2\rangle : A_1 \times A_2$$

This is indeed—and should be!—a normal form. But what if we just want to prove A_1? We may apply the elimination rule:

$$\Delta\,;\Gamma \vdash \pi_1\,(\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ \langle N_1, N_2\rangle) : A_1$$

Now, this is a proof of A_1, but it surreptitiously contains a proof N_2 of A_2 as well, which is entirely unrelated to A_1 (neither needs to be a subexpression of the other). But, according to our notion of reduction, it is normal! The problem is that the $\mathsf{let\ box}\ u \Leftarrow (-)\ \mathsf{in}\ (-)$ obstructs the meeting of the destructor $\pi_1(-)$ with the constructor $\langle N_1, N_2\rangle$. The solution is to allow a *commuting conversion* that allows the two to meet, by 'pulling the let construct outside:'

$$\pi_1\,(\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ \langle N_1, N_2\rangle) \longrightarrow \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ \pi_1(\langle N_1, N_2\rangle)$$

A similar situation occurs when $\Delta, u{:}A\,;\Gamma \vdash \lambda x{:}A.P : A \to B$: we can form

$$\Delta\,;\Gamma \vdash \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ \lambda x{:}A.P : A \to B$$

which is a perfectly reasonable normal form, but if $\Delta\,;\Gamma \vdash Q : A$ then

$$\Delta\,;\Gamma \vdash (\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ \lambda x{:}A.P)\,Q : B$$

is not: we should be able to reduce

$$(\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ \lambda x{:}A.P)\,Q \longrightarrow \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ (\lambda x{:}A.P)Q$$

Finally, there is third, less visible case of this phenomenon. If we understand $(\Box\mathcal{E})$ to be a *'bad'* elimination, we have considered the cases of *'good'* elimination ($\pi_i(-)$, application) following 'bad' elimination. The final case is that of 'bad' elimination following another 'bad' elimination. To give an example, let's consider an elimination after a $\mathsf{box}\ (-)$ introduction:

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

If we then have a term $\Delta, v{:}A\,;\Gamma \vdash P : C$, we can plug this in by eliminating the box:

$$\Delta\,;\Gamma \vdash \mathsf{let\ box}\ v \Leftarrow (\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in\ box}\ N)\ \mathsf{in}\ P : C$$

Now things are clear: the second let-construct is obstructing the meeting of the first let-construct with the introduction form $\mathsf{box}\ N$. We need to convert:

$$\begin{aligned} &\mathsf{let\ box}\ v \Leftarrow (\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in\ box}\ N)\ \mathsf{in}\ P \\ \longrightarrow\ &\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in\ let\ box}\ v \Leftarrow \mathsf{box}\ N\ \mathsf{in}\ P \end{aligned}$$

but we should take care to rename u so that it does not occur in P—as it would be wrongly bound otherwise.

These examples actually cover all cases. We define $\longrightarrow_c \subseteq \Lambda \times \Lambda$ to be the compatible closure of $\longrightarrow$ that includes the following clauses:

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

We can now prove the requisite property for this reduction relation: one only needs to take enough care to strengthen the induction hypothesis sufficiently.

Theorem 20 (Subformula Property)**.** *Let $\Delta\,;\Gamma \vdash M : A$, and suppose M is a $(\longrightarrow_c)$-normal form. Then,*

1. *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.*

2. *If M is an elimination construct that is* not *of the form $\mathsf{let\ box}\ u \Leftarrow P\ \mathsf{in}\ Q$—i.e. if it is a projection $\pi_i(N)$ or an application PQ—then it entirely consists of a sequence of eliminations: that is, there is a sequence of types,*

$$A_0, \ldots, A_n$$

such that

- *A_0 occurs in either Δ or Γ,*
- *A_n is A, and*
- *A_i is the* major premise *of an elimination whose conclusion is A_{i+1} for $i = 0, \ldots, n$. In particular, A_n is a subexpression of A_0.*

This is called a principal branch.

Proof. By induction on the derivation of $\Delta\,;\Gamma \vdash M : A$.

Case(x). Then $\Delta\,;\Gamma \vdash x : A$ and hence $(x : A) \in \Gamma$. This is the complete derivation, and satisfies both desiderata.

Case(u). Then $\Delta\,;\Gamma \vdash u : A$ and hence $(u : A) \in \Delta$. This is the complete derivation, and satisfies both desiderata.

CASE($\lambda x{:}A.\ M$). Then the immediate premise is of the form $\Delta;\Gamma, x{:}A \vdash M : B$. By the IH, all types that occur in that are either (a) subexpressions of types in Δ or Γ, (b) subexpressions of A, or (c) subexpressions of B. Thus any of the types occuring in the derivation of the premise are indeed subexpressions of either Δ, Γ, or $A \to B$. Let us now look at the complete derivation. The only new type that occurs in it is $A \to B$, and that is trivially a subexpression of itself.

CASE($\langle M, N \rangle$). Similar.

CASE($\mathsf{box}\ M$). Similar.

CASE(MN). Then the major premise is $\Delta\,;\Gamma \vdash M : B \to A$ and the minor premise is $\Delta\,;\Gamma \vdash N : B$ for some type B.

Let us look at the term M. It cannot be a lambda-abstraction, for that would make MN a redex. It also cannot be any other introduction rule, for they introduce types of a different shape (e.g. $A \times B$ or $\Box A$). Hence, it must be an elimination. Of the eliminations, it cannot be a let-expression, for our newly introduced commuting conversion would make that a redex.

It follows that M is a 'good' elimination, either $\pi_i(-)$ or PQ. We can thus apply (2) from the inductive hypothesis to conclude that there is a principal branch beginning with an assumption in Δ or Γ, and ending with $B \to A$. We can extend that principal branch to a principal branch for M, ending with A. This proves (2), and furthermore implies that $B \to A$ is a subexpression of some premise in either Δ or Γ.

Over to (1): applying the IH to the major premise, we know that every type that occurs in the derivation of $\Delta\,;\Gamma \vdash M : B \to A$ is either a subexpression of a type in Δ or Γ, or a subexpression of $B \to A$. But we have already deduced that $B \to A$ is a subexpression of some premise in either Δ or Γ, so that all types occuring in the derivation of the major premise satisfy the desideratum.

Applying the IH to the minor premise, every type that occurs in the derivation of $\Delta\,;\Gamma \vdash N : B$ is either a subexpression of some type in Δ or Γ, or a subexpression of B. But B is a subexpression of $B \to A$, which in turn is a subexpression of a premise in one of the contexts. Hence all types occurring in that branch also occur in either Δ or Γ. This concludes the proof of this case, for we have examined all types appearing in the derivation.

CASE($\pi_i(M)$). Similar.

CASE($\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N$). The major premise is then $\Delta\,;\Gamma \vdash M : \Box B$ and the minor premise is $\Delta, u{:}B\,;\Gamma \vdash N : A$ for some B. (2) does not apply to let-constructs, so we only need to show (1).

Consider the term M. It cannot be a $\mathsf{box}\,(-)$, for that would make the entire term a redex. It also cannot be any other introductory form, because they introduce types of a different shape. It therefore must be an elimination form; but not another let-construct, for that would be a redex too, due to our commuting conversion. Hence, it must be a 'good' elimination, either of the form $\pi_i(M')$ or of the form PQ. It follows that (2) of the IH applies: there is a principal branch beginning with a premise and ending with $\Box B$. In particular, $\Box B$ is a subexpression of some type in Δ or Γ.

By the IH, any type that occurs in the derivation of the major premise is either a subexpression of a type in Δ or Γ, or a subexpression of $\Box B$. But $\Box B$ is a subexpression of some type in one of those two contexts, so every type that occurs in the derivation of the major premise is actually a subexpression of a type in Δ or Γ.

As for the minor premise, any type that occurs in it is either a subexpression of a type in Δ or Γ, or a subexpression of the types B or A. But B is a subexpression of $\Box B$, which by our previous reasoning is in turn a subexpression of some type in either Δ or Γ. Thus all types occuring in it are either subexpressions of some type in Δ or Γ, or subexpressions of A. This concludes the proof of this case.

□

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. A full analysis would follow the lines of the one in Ohta and Hasegawa (2006), whilst keeping in mind that we are not trying to decide an equality like in *op. cit.*, but that we are merely eliminating parasitic formulae.

Chapter 6

Candidates of Reducibility

In this chapter we adapt the method of *candidats de reducibilité* to our modal λ-calculi. The method of candidats originated in Girard's proof of strong normalization for System F (Girard, 1972).

Our variant of "candidats" is a combination of two versions. The main structure of the proof is due to by Koletsos (1985), as presented in simplified form by Gallier (1995). However, the Koletsos-Gallier presentation does not carry typing information in the proof, whereas in our calculi typing is vital. Thus, we enhance their method, insofar as our can candidates consist of typing judgments $\Delta\,;\Gamma \vdash M : A$ rather than simply terms $M : A$. Ideas on how this is done were drawn from another chapter by Gallier (1990), which also surveys multiple variants of the *candidats* method.

The overall structure of the proof is the following. Suppose we have a family of nonempty *sets of typing judgments*,

$$\mathcal{P} = \{P_A\}_A$$

indexed by the type A they assign to the term they carry. We will state six properties, P0–P5, that such a family should satisfy. In case it does indeed satisfy them, we show that P_A contains all judgments $\Delta\,;\Gamma \vdash M : A$ with type A.

In §5.3 we verified that the family $\{P_A\}_A$ where P_A contains all judgments $\Delta\,;\Gamma \vdash M : A$ for which the term M is strong normalizing indeed satisfies P0–P5, and it thus followed that all terms strongly normalizing.

We now give a brief summary of the proof. To begin, we will state the first four properties, namely P0–P4. We also define what it means for a set C of derivable judgments to be a *candidate*. Then, we define a subset $[\![A]\!]$ of P_A, for each type A. We call judgments in $[\![A]\!]$ *reducible*. It so happens that $[\![A]\!]$ is a candidate. Finally, we introduce two further properties, P4 and P5. If these hold of P_A, then we show that $[\![A]\!]$ contains all derivable judgments.

But before we begin, we need to differentiate between introduction and elimination forms. The first we call *I-terms*, and the latter *simple*:

Definition 7.

1. A term is a *I-term* just if it is an introduction form, i.e. of the form

$$\lambda x{:}A.\ M, \qquad \langle M, N\rangle, \qquad \mathsf{box}\ M, \qquad \mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ M \quad \text{(for GL only)}$$

2. A term is a *simple term* just if it is a variable or an elimination form, i.e. of the form

$$x, \qquad MN, \qquad \pi_i(M), \qquad \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N$$

3. A *stubborn* term is a simple term that is either a normal form, or a term that does not reduce to a I-term.

6.1 Candidates: the first four properties

We now define the first four properties that we shall consider. The first one is our addition to Gallier (1995), and solely refers to typing: in particular, it requires that weakening, modal weakening, and modal dereliction are admissible rules in the family $\mathcal{P}$. The second and third require that all variables be in $\mathcal{P}$, and that $\mathcal{P}$ be closed under reduction respectively. Finally, the fourth is a funny closure condition: if a term reduces to a I-term, then eliminating this introduction by something of appropriate type present in $\mathcal{P}$ again yields something in $\mathcal{P}$.

Definition 8 (Properties P0-P3)**.** We define the following properties pertaining to the family $\mathcal{P}$.

(P0) (a) $\Delta\,;\Gamma \vdash M \in P_A$ and $\Gamma \sqsubseteq \Gamma'$ imply $\Delta\,;\Gamma' \vdash M \in P_A$

(b) $\Delta\,;\Gamma \vdash M \in P_A$ and $\Delta \sqsubseteq \Delta'$ imply $\Delta'\,;\Gamma \vdash M \in P_A$

(c) (for T and S4 only) $\Delta\,;\Gamma,\Gamma' \vdash M \in P_A$ implies $\Delta,\Gamma\,;\Gamma' \vdash M \in P_A$

(P1) $\Delta\,;\Gamma \vdash x \in P_A$ for all variables x.

(P2) $M \in P_A$ and $M \longrightarrow N$ imply $N \in P_A$.

(P3) For simple terms M,

(a) If

– $\Delta\,;\Gamma \vdash M \in P_{A\to B}$,
– $\Delta\,;\Gamma \vdash N \in P_A$, and
– whenever $M \longrightarrow^* \lambda x{:}A.M'$ then $\Delta\,;\Gamma \vdash (\lambda x{:}A.M')N \in P_B$

then this implies $\Delta\,;\Gamma \vdash MN \in P_B$.

(b) If

– $\Delta\,;\Gamma \vdash M \in P_{A\times B}$, and
– whenever $M \longrightarrow^* \langle M_1, M_2\rangle$ then $\Delta\,;\Gamma \vdash \pi_1(\langle M_1, M_2\rangle) \in P_A$ and $\Delta\,;\Gamma \vdash \pi_2(\langle M_1, M_2\rangle) \in P_B$,

then this implies that $\Delta\,;\Gamma \vdash \pi_1(M) \in P_A$ and $\Delta\,;\Gamma \vdash \pi_2(M) \in P_B$.

We now define what it means to be a candidate $C \subseteq P_A$. The gist is this: a candidate is closed under our useful admissible rules; it is closed under reduction; and, a term is necessarily in the candidate if all the I-terms it reduces to are in the candidate as well.

Definition 9 ($\mathcal{P}$-candidate)**.** A set C of derivable judgments of type A is a *$\mathcal{P}$-candidate* just if

(R0) (a) $\Delta\,;\Gamma \vdash M \in C$ and $\Gamma \sqsubseteq \Gamma'$ imply $\Delta\,;\Gamma' \vdash M \in C$.

(b) $\Delta\,;\Gamma \vdash M \in C$ and $\Delta \sqsubseteq \Delta'$ imply $\Delta'\,;\Gamma \vdash M \in C$.

(c) (for T and S4 only) $\Delta\,;\Gamma,\Gamma' \vdash M \in C$ implies $\Delta,\Gamma\,;\Gamma' \vdash M \in C$

(R1) $C \subseteq P_A$.

(R2) $\Delta\,;\Gamma \vdash M \in C$ and $M \longrightarrow N$ imply $\Delta\,;\Gamma \vdash N \in C$.

(R3) If $\Delta\,;\Gamma \vdash M \in P_A$ is simple, and whenever $M \longrightarrow^* N$ and N is a I-term implies that $\Delta\,;\Gamma \vdash N \in C$ then it follows that $\Delta\,;\Gamma \vdash M \in C$.

The definition implies that all variables are in a candidate:

Lemma 5. *For any $\mathcal{P}$-candidate C, $\Delta\,;\Gamma \vdash x \in C$.*

Proof. By (P1), we have that $\Delta\,;\Gamma \vdash x \in P_A$, and by definition x is simple, and a normal form, so it cannot ever reduce to a I-term. All the premises of (R3) are satisfied, so $\Delta\,;\Gamma \vdash x \in C$. □

We now define the set $[\![A]\!]$ of reducible judgments for each type A. This definition has a flavour that is familiar to those acquainted with *logical relations*, or logical predicates in this case. $[\![\Box A]\!]$ is defined differently for each system, and so is $[\![A \to B]\!]$, in order to ensure admissibility of the dereliction rule when needed.

Definition 10 (Reducible judgments)**.** We define for each type A a set of derivable judgments $[\![A]\!] \subseteq P_A$ by induction on A.

$$[\![p_i]\!] \stackrel{\text{def}}{=} P_{p_i}$$

$$[\![A \times B]\!] \stackrel{\text{def}}{=} \{\, \Delta\,;\Gamma \vdash M \in P_{A\times B} \mid \Delta\,;\Gamma \vdash \pi_1(M) \in [\![A]\!] \ \wedge\ \Delta\,;\Gamma \vdash \pi_2(M) \in [\![B]\!] \,\}$$

$$[\![A \to B]\!] \stackrel{\text{def}}{=} \begin{cases} \{\, \Delta\,;\Gamma \vdash M \in P_{A\to B} \mid \\ \quad \forall \text{ splittings } \Gamma \equiv \Gamma_1, \Gamma_2. \\ \quad \forall \Delta' \sqsupseteq \Delta, \Gamma_1.\ \forall \Gamma' \sqsupseteq \Gamma_2. \\ \qquad \forall \Delta'\,;\Gamma' \vdash N \in [\![A]\!]\,.\ \Delta'\,;\Gamma' \vdash MN \in [\![B]\!] \} & \text{for } \mathsf{T},\ \mathsf{S4} \\ \{\, \Delta\,;\Gamma \vdash M \in P_{A\to B} \mid \\ \quad \forall \Delta' \sqsupseteq \Delta.\ \forall \Gamma' \sqsupseteq \Gamma. \\ \qquad \forall \Delta'\,;\Gamma' \vdash N \in [\![A]\!]\,.\ \Delta'\,;\Gamma' \vdash MN \in [\![B]\!] \} & \text{otherwise} \end{cases}$$

$$[\![\Box A]\!] \stackrel{\text{def}}{=} \begin{cases} \{\, \Delta\,;\Gamma \vdash M \in P_{\Box A} \mid M \longrightarrow^* \mathsf{box}\, Q \Longrightarrow \cdot\,;\Delta \vdash Q \in [\![A]\!] \,\} & \text{for } \mathsf{K},\ \mathsf{T} \\ \{\, \Delta\,;\Gamma \vdash M \in P_{\Box A} \mid M \longrightarrow^* \mathsf{box}\, Q \Longrightarrow \Delta\,;\Delta^\perp \vdash Q^\perp \in [\![A]\!] \,\} & \text{for } \mathsf{K4} \\ \{\, \Delta\,;\Gamma \vdash M \in P_{\Box A} \mid M \longrightarrow^* \mathsf{box}\, Q \Longrightarrow \Delta\,;\cdot \vdash Q \in [\![A]\!] \,\} & \text{for } \mathsf{S4} \\ \{\, \Delta\,;\Gamma \vdash M \in P_{\Box A} \mid \\ \quad M \longrightarrow^* \mathsf{fix}\, z\ \mathsf{in}\ \mathsf{box}\, Q \Longrightarrow \Delta\,;\Delta^\perp, z^\perp : A \vdash Q^\perp \in [\![A]\!] \} & \text{for } \mathsf{GL} \end{cases}$$

We can now prove that $[\![A]\!]$ is a candidate. We will need a slightly stronger induction hypothesis in order to complete the proof.

Theorem 21. *If $\mathcal{P} = \{P_A\}$ satisfies properties P0-P3, then*

1. *For any A, $[\![A]\!]$ is a $\mathcal{P}$-candidate.*
2. *For any A, $[\![A]\!]$ contains all the stubborn terms in P_A.*

Proof. By induction on types.

1. Case(p_i). Then $[\![A]\!] = P_{p_i}$, so it trivially contains all stubborn terms in P_{p_i}, hence (2). To verify (1), we need to show properties R0–R3. R0 is exactly P0. R1 is trivially satisified. R2 is exactly P2. R3 also trivially holds as $[\![A]\!]$ contains all terms in P_{p_i}.

2. CASE($A \times B$). For (1), we verify R0-R3.

   (R0) For (a): let $\Delta;\Gamma \vdash M \in [\![A \times B]\!]$ and $\Gamma \sqsubseteq \Gamma'$. Then $\Delta;\Gamma \vdash \pi_1(M) \in [\![A]\!]$ by the definition of $[\![A \times B]\!]$, and—by the IH—we have $\Delta\,;\Gamma' \vdash \pi_1(M) \in [\![A]\!]$, and similarly for B, which yields the result. The reasoning is similar for (b) and (c).

   (R1) Trivially $[\![A \times B]\!] \subseteq P_{A\times B}$.

   (R2) Let $\Delta\,;\Gamma \vdash M \in [\![A \times B]\!]$, and suppose $M \longrightarrow N$. By (P2), we have $\Delta\,;\Gamma \vdash N \in P_{A\times B}$. It remains to show $\Delta\,;\Gamma \vdash \pi_1(N) \in [\![A]\!]$ and $\Delta\,;\Gamma \vdash \pi_2(N) \in [\![B]\!]$. But as $\Delta\,;\Gamma \vdash M \in [\![A \times B]\!]$, we have $\Delta\,;\Gamma \vdash \pi_1(M) \in [\![A]\!]$. Thus, as $\pi_1(M) \longrightarrow \pi_1(N)$, we use (R2) from the IH to obtain $\Delta\,;\Gamma \vdash \pi_1(N) \in [\![A]\!]$. Similarly for $\pi_2(N)$.

   (R3) Suppose that $M \in P_{A\times B}$ is a simple term, and whenever $M \longrightarrow^* \langle P, Q\rangle$, then $\langle P, Q\rangle \in [\![A \times B]\!]$. We want to show that $\pi_1(M) \in [\![A]\!]$ and $\pi_2(M) \in [\![B]\!]$.

   First, we show they are in P_A and P_B respectively, and we do this by invoking (P3)(b). Suppose then that $M \longrightarrow^* \langle P, Q\rangle$ for some P and Q. By assumption, we have $\langle P, Q\rangle \in [\![A \times B]\!]$, and hence—by definition—$\pi_1(\langle P, Q\rangle) \in [\![A]\!] \subseteq P_A$ and $\pi_2(\langle P, Q\rangle) \in [\![B]\!] \subseteq P_B$. So, as M is simple, we obtain by (P3)(b) that $\pi_1(M) \in P_A$ and $\pi_2(M) \in P_B$.

   There are now two cases:

   CASE(M stubborn). Then M never reduces to a I-term. It follows that $\pi_1(M) \in P_A$ and $\pi_2(M) \in P_B$ are also stubborn, as M never reduces to a pair so that the outermost projections become a redex. By (2) of the IH, $\pi_1(M) \in [\![A]\!]$ and $\pi_2(M) \in [\![B]\!]$ as each contains all stubborn terms in P_A and P_B respectively.

   CASE(M not stubborn). We only show this for A, the reasoning for B being similar.

   CASE($A \equiv p_i$). Then have the result, as $[\![A]\!] = P_A$.

   CASE($A \not\equiv p_i$). We use (R3) from the IH: it suffices to show that $\pi_1(M) \longrightarrow^* U$ for some I-term U implies $U \in [\![A]\!]$.
   If $\pi_1(M)$ is stubborn, then the desideratum holds vacuously.
   Suppose otherwise, i.e. that $\pi_1(M) \longrightarrow^* U$ for some I-term U. As U is a I-term, the reduction $\pi_1(M) \longrightarrow^* U$ must have been of the

form

$$\pi_1(M) \longrightarrow^* \pi_1(\langle U', V' \rangle) \longrightarrow U' \longrightarrow^* U$$

with $M \longrightarrow^* \langle U', V' \rangle$: otherwise the outer $\pi_1(-)$ would have persisted. But M is simple and $M \longrightarrow^* \langle U', V' \rangle$, so—by our assumption—$\langle U', V' \rangle \in [\![A \times B]\!]$, hence $\pi_1(\langle U', V' \rangle) \in [\![A]\!]$ by definition. By multiple uses of (R2) of the IH, this yields that $U \in [\![A]\!]$.

For (2): if $M \in P_{A \times B}$ is stubborn, we argue as above: M is simple, and it never reduces to a I-term, so by (P3)(b) we have $\pi_1(M) \in P_A$ and $\pi_2(M) \in P_B$ respectively. These terms are in turn stubborn, so by the IH they are in $[\![A]\!]$ and $[\![B]\!]$ respectively, hence $M \in [\![A \times B]\!]$ by definition.

3. Case$(A \to B)$. For (1):

   (R0) We only show (a) for the 'otherwise' case, the T and S4 case being very similar. Let $\Delta\,;\Gamma \vdash M \in [\![A \to B]\!]$, and $\Gamma \sqsubseteq \Gamma'$. We need to show that, given $\Gamma'' \sqsupseteq \Gamma'$, $\Delta'' \sqsupseteq \Delta$ and any $\Delta''\,;\Gamma'' \vdash N \in [\![A]\!]$ we have $\Delta''\,;\Gamma'' \vdash MN \in [\![B]\!]$. But, as $\Gamma \sqsubseteq \Gamma'$ and $\sqsubseteq$ is transitive, this follows from the definition of $[\![A \to B]\!]$. The reasoning is similar for (b).

   For (c): let $\Delta\,;\Gamma, \Gamma' \vdash M \in [\![A \to B]\!]$. We need to show that for all splittings $\Gamma' \equiv \Gamma'_a, \Gamma'_b$ and $\Delta' \sqsupseteq \Delta, \Gamma'_a$ and $\Gamma' \sqsupseteq \Gamma'_b$ we have that $\Delta'\,;\Gamma' \vdash N \in [\![A]\!]$ implies that $\Delta'\,;\Gamma' \vdash MN \in [\![B]\!]$. Pick $\Gamma_1 \stackrel{\text{def}}{=} \Gamma, \Gamma'_a$ and $\Gamma_2 \stackrel{\text{def}}{=} \Gamma'_b$; the definition of $[\![A \to B]\!]$ then ensures that, again by transitivity of $\sqsubseteq$.

   (R1) Trivially $[\![A \to B]\!] \subseteq P_{A \times B}$.

   (R2) Let $\Delta\,;\Gamma \vdash M \in [\![A \to B]\!]$ and suppose $M \longrightarrow N$. By (P2) we have $N \in P_{A \to B}$. It remains to show that, for all $P \in [\![A]\!]$, $NP \in [\![B]\!]$. But we have—by definition—that $MP \in [\![B]\!]$, and as $MP \longrightarrow NP$, we have by (R2) of the IH that $NP \in [\![B]\!]$.

   (R3) For the sake of clarity we omit the contexts in this case, for they are just annotations to the essence of the argument.

   Suppose that $M \in P_{A \to B}$ is a simple term, and whenever $M \longrightarrow^* \lambda x{:}A.\ P$ then $\lambda x{:}A.\ P \in [\![A \to B]\!]$. That is, for any $Q \in [\![A]\!]$, we have $(\lambda x{:}A.\ P)Q \in [\![B]\!]$. We need to show that, for any $N \in [\![A]\!]$ we have $MN \in [\![B]\!]$.

First, we show that for any $N \in [\![A]\!]$ we have $MN \in P_B$. We know by the assumption that whenever $M \longrightarrow^* \lambda x{:}A.\ P$ then $(\lambda x{:}A.\ P)N \in [\![B]\!] \subseteq P_B$. By (P3)(a), it follows that $MN \in P_B$.

There are two cases.

CASE(M stubborn). Then $MN \in P_B$ is also stubborn, as no top-level redexes can ever be created. It follows by the IH for B that $MN \in [\![B]\!]$.

CASE(M not stubborn). We distinguish on whether B is a base type or not.

CASE($B \equiv p_i$). Then $MN \in P_B = [\![B]\!]$.

CASE($B \not\equiv p_i$). The term $MN \in P_B$ is simple. Thus, it suffices—by (R3) of the IH for B—to show the following: if $MN \longrightarrow^* Q$ with Q a I-term, then $Q \in [\![B]\!]$.

If MN is stubborn, then it never reduces to a I-term, so the desideratum holds vacuously.

If MN is not stubborn, we have that $MN \longrightarrow^* U$ for some I-term U. As U is a I-term, that reduction must be of the form

$$MN \longrightarrow^* (\lambda x{:}A.\ P)N' \longrightarrow P[N'/x] \longrightarrow^* U$$

with $M \longrightarrow^* \lambda x{:}A.P$ and $N \longrightarrow^* N'$: otherwise the outer application would have persisted. But M is simple and $M \longrightarrow^* \lambda x{:}A.\ P$, so by the assumption $\lambda x{:}A.\ P \in [\![A \to B]\!]$. As $N \longrightarrow^* N'$, repeated applications of the (R2) of the IH yield $N' \in [\![B]\!]$. Thus, $(\lambda x{:}A.\ P)N' \in [\![B]\!]$, and again by repeated applications of (R2) of the IH, $U \in [\![B]\!]$.

For (2): if $M \in P_{A\to B}$ is stubborn, we argue as above: M is simple, and it never reduces to a I-term. Take any $N \in [\![A]\!] \subseteq P_A$. By (P3)(a) $MN \in P_B$. This MN is in turn stubborn—as M never reduces to a λ-abstraction and the outermost application persists—so, by the IH, $MN \in [\![B]\!]$. Hence $M \in [\![A \to B]\!]$.

4. CASE($\Box A$). For (1):

(R0) (a) trivially holds, for none of the judgments for Q in the definition of $[\![\Box A]\!]$ depend on the context Γ.

(b) and (c) follow from the assumption $\Delta\,;\Gamma \vdash M : \Box A$ and—depending on the logic—the statements (a), (b), or both, of (R0) of the IH for A.

(R1) Trivially $[\![\Box A]\!] \subseteq P_{\Box A}$.

(R2) We only show the case for K, the others being entirely analogous.

Let $\Delta\,;\Gamma \vdash M \in [\![\Box A]\!]$ and suppose $M \longrightarrow N$. By ($\mathsf{P2}$) we have $\Delta\,;\Gamma \vdash N \in P_{\Box A}$. It remains to show that, whenever $N \longrightarrow^* \mathsf{box}\, Q$, then $\cdot\,;\Delta \vdash Q \in [\![A]\!]$. But when that sequence of reductions happens, we have

$$M \longrightarrow N \longrightarrow^* \mathsf{box}\, Q$$

thus, by the definition of $[\![\Box A]\!]$, we have that $\cdot\,;\Delta \vdash Q \in [\![A]\!]$.

(R3) We only show the case for $\mathsf{S4}$, all the others being similar.

Suppose that $\Delta\,;\Gamma \vdash M \in P_{\Box A}$ is a simple term, and whenever $M \longrightarrow^* \mathsf{box}\, Q$ then that term is in $[\![\Box A]\!]$: this is to say that whenever $\mathsf{box}\, Q \longrightarrow^* \mathsf{box}\, Q'$, then $\Delta\,;\cdot \vdash Q' \in [\![A]\!]$. We need to show that, if $M \longrightarrow^* \mathsf{box}\, Q$, then $\Delta;\cdot \vdash Q \in [\![A]\!]$. But, by reflexivity, $\mathsf{box}\, Q \longrightarrow^* \mathsf{box}\, Q$, so this already follows by our assumption.

For (2): if $M \in P_{\Box A}$ is stubborn, then it never reduces to a I-term of shape $\mathsf{box}\, Q$, so it is—by definition—in $[\![\Box A]\!]$. Likewise for GL.

□

6.2 Closure under formation: the latter two properties

We now introduce two further properties. Property ($\mathsf{P4}$) is essentially closure of $\mathcal{P}$ under introduction rules. Property ($\mathsf{P5}$) ensures that, if a term is in $\mathcal{P}$ is after 'eliminating a detour,' then it is also in $\mathcal{P}$ before the detour is eliminated.

Definition 11 (Properties $\mathsf{P4}$-$\mathsf{P5}$)**.**

($\mathsf{P4}$) (a) If $\Delta\,;\Gamma, x{:}A \vdash M \in P_B$ then $\Delta\,;\Gamma \vdash \lambda x{:}A.\, M \in P_{A\to B}$.

(b) $\Delta\,;\Gamma \vdash M \in P_A$ and $\Delta\,;\Gamma \vdash N \in P_B$ imply $\Delta\,;\Gamma \vdash \langle M, N\rangle \in P_{A\times B}$.

(c)

i. (for K and T) $\cdot\,;\Delta \vdash M \in P_A$ implies $\Delta\,;\Gamma \vdash \mathsf{box}\, M \in P_{\Box A}$

ii. (for $\mathsf{K4}$) $\Delta\,;\Delta^\perp \vdash M^\perp \in P_A$ implies $\Delta\,;\Gamma \vdash \mathsf{box}\, M \in P_{\Box A}$

iii. (for GL) $\Delta\,;\Delta^\perp, z^\perp : \Box A \vdash M^\perp \in P_A$ implies $\Delta\,;\Gamma \vdash \mathsf{fix}\, z\, \mathsf{in}\, \mathsf{box}\, M \in P_{\Box A}$

iv. (for S4) $\Delta\,;\cdot \vdash M \in P_A$ implies $\Delta\,;\Gamma \vdash \mathsf{box}\, M \in P_{\Box A}$

(P5) (a) If $\Delta' \sqsupseteq \Delta$ and $\Gamma' \sqsupseteq \Gamma$ satisfy $\Delta'\,;\Gamma' \vdash N \in P_A$ and $\Delta'\,;\Gamma' \vdash M[N/x] \in P_B$, then $\Delta'\,;\Gamma' \vdash (\lambda x{:}A.\ M)N \in P_B$.

(b) $\Delta\,;\Gamma \vdash M \in P_A$ and $\Delta\,;\Gamma \vdash N \in P_B$ imply $\Delta\,;\Gamma \vdash \pi_1(\langle M, N\rangle) \in P_A$ and $\Delta\,;\Gamma \vdash \pi_2(\langle M, N\rangle) \in P_B$.

(c) i. (for non-GL) If we have $\Delta\,;\Gamma \vdash M \in P_{\Box A}$ and $\Delta, u{:}A\,;\Gamma \vdash N \in P_C$, and whenever $M \longrightarrow^* \mathsf{box}\, Q$ then $\Delta\,;\Gamma \vdash N[Q/u] \in P_C$, then we have that $\Delta\,;\Gamma \vdash \mathsf{let\ box}\, u \Leftarrow M\ \mathsf{in}\ N \in P_C$.

ii. (for GL only) If we have $\Delta;\Gamma \vdash M \in P_{\Box A}$ and $\Delta, u{:}A;\Gamma \vdash N \in P_C$, and whenever $M \longrightarrow^* \mathsf{fix}\ z\ \mathsf{in\ box}\, Q$ then $\Delta;\Gamma \vdash N\,[Q[\mathsf{fix}\ z\ \mathsf{in\ box}\, Q/z]/u] \in P_C$, then we have that $\Delta\,;\Gamma \vdash \mathsf{let\ box}\, u \Leftarrow M\ \mathsf{in}\ N \in P_C$.

The next theorem shows that properties (P4) and (P5) carry over to the candidates of reducible judgments $[\![A]\!]$.

Theorem 22. *If $\mathcal{P} = \{P_A\}$ satisfies properties (P1)-(P5), then*

1. *If whenever $\Gamma' \sqsupseteq \Gamma$, $\Delta' \sqsupseteq \Delta$ and $\Delta'\,;\Gamma' \vdash N \in [\![A]\!]$ we have $\Delta'\,;\Gamma' \vdash M[N/x] \in [\![B]\!]$, then*
$$\Delta\,;\Gamma \vdash \lambda x{:}A.\ M \in [\![A \to B]\!]$$

2. *If $\Delta\,;\Gamma \vdash M \in [\![A]\!]$ and $\Delta\,;\Gamma \vdash N \in [\![B]\!]$ then*
$$\Delta\,;\Gamma \vdash \langle M, N\rangle \in [\![A \times B]\!]$$

3. (a) *(for K and T) If $\Delta\,;\Gamma \vdash M \in [\![\Box A]\!]$, and whenever $\Delta' \sqsupseteq \Delta$ and $\cdot\,;\Delta' \vdash Q \in [\![A]\!]$ then we have $\Delta'\,;\Gamma \vdash N[Q/u] \in [\![C]\!]$ then*
$$\Delta\,;\Gamma \vdash \mathsf{let\ box}\, u \Leftarrow M\ \mathsf{in}\ N \in [\![C]\!]$$

(b) *(for K4 only) If $\Delta\,;\Gamma \vdash M \in [\![\Box A]\!]$, and whenever $\Delta' \sqsupseteq \Delta$ and $\Delta'\,;\Delta'^{\perp} \vdash Q^{\perp} \in [\![A]\!]$ then we have $\Delta'\,;\Gamma \vdash N[Q/u] \in [\![C]\!]$, then*
$$\Delta\,;\Gamma \vdash \mathsf{let\ box}\, u \Leftarrow M\ \mathsf{in}\ N \in [\![C]\!]$$

(c) *(for GL only) If $\Delta;\Gamma \vdash M \in [\![\Box A]\!]$, and whenever $\Delta' \sqsupseteq \Delta$ and $\Delta';\Delta'^{\perp}, z^{\perp} : \Box A \vdash Q^{\perp} \in [\![A]\!]$ then $\Delta'\,;\Gamma \vdash N\,[Q[\mathsf{fix}\ z\ \mathsf{in\ box}\, Q/z]/u] \in [\![C]\!]$, then*
$$\Delta\,;\Gamma \vdash \mathsf{let\ box}\, u \Leftarrow M\ \mathsf{in}\ N \in [\![C]\!]$$

(d) *(for S4 only) If* $\Delta\,;\Gamma \vdash M \in [\![\Box A]\!]$*, and whenever* $\Delta' \sqsupseteq \Delta$ *and* $\Delta'\,;\cdot \vdash Q \in [\![A]\!]$ *then we have* $\Delta'\,;\Gamma \vdash N[Q/u] \in [\![C]\!]$*, then*

$$\Delta\,;\Gamma \vdash \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N \in [\![C]\!]$$

Proof.

1. First, we show that $\Delta\,;\Gamma \vdash \lambda x{:}A.\ M \in P_{A\to B}$. By Lemma 5 and Theorem 21, it is the case that $\Delta\,;\Gamma, x{:}A \vdash x \in [\![A]\!]$. Hence, by taking $\Gamma' \stackrel{\text{def}}{=} \Gamma, x{:}A$ and $\Delta' \stackrel{\text{def}}{=} \Delta$ in the assumption, we have $\Delta\,;\Gamma, x{:}A \vdash M[x/x] \in [\![B]\!] \subseteq P_B$. Thus, as $M[x/x] \equiv M$, we have by (P4)(a) that $\Delta\,;\Gamma \vdash \lambda x{:}A.\ M \in P_{A\to B}$.

   It remains to show that, for $\Delta' \sqsupseteq \Delta$, $\Gamma' \sqsupseteq \Gamma$ and $\Delta'\,;\Gamma' \vdash N \in [\![A]\!]$, we have $\Delta'\,;\Gamma' \vdash (\lambda x{:}A.\ M)N \in [\![B]\!]$. First we need to show that $(\lambda x{:}A.\ M)N \in P_B$. But, by the assumption, $M[N/x] \in [\![B]\!] \subseteq P_B$. By invoking (P5)(a) we have that $(\lambda x{:}A.\ M)N \in P_B$. There are now two cases.

   Case$(B \equiv p_i)$. Then $P_B = [\![B]\!]$ and the result follows.

   Case$(B \not\equiv p_i)$. We have that $(\lambda x{:}A.\ M)N$ is simple, so we use (R3): it suffices to show that whenever $(\lambda x{:}A.\ M)N \longrightarrow^* Q$ and Q is a I-term, then $Q \in [\![B]\!]$.

   If $(\lambda x{:}A.\ M)N$ is stubborn, then the desideratum is trivial.

   Otherwise, if $(\lambda x{:}A.\ M)N \longrightarrow^* Q$ where Q is a I-term, then the reduction must be of the form

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

   where $M \longrightarrow^* M'$ and $N \longrightarrow^* N'$: otherwise the outermost application would persist. But, by the assumption, $M[N/x] \in [\![B]\!]$, and

   $$M[N/x] \longrightarrow^* M'[N'/x] \longrightarrow^* Q$$

   so, by applying (R2) repeatedly, $Q \in [\![B]\!]$.

2. First, we show that $\langle M, N\rangle \in P_{A\times B}$. We have $M \in [\![A]\!] \subseteq P_A$ and $N \in [\![B]\!] \subseteq P_B$, so what we want follows simply by (P4)(b).

   It remains to show that $\pi_1(\langle M, N\rangle) \in [\![A]\!]$ and $\pi_2(\langle M, N\rangle) \in [\![B]\!]$. That each is already in P_A and P_B respectively follows by (P5)(2) and the fact M and N are already in P_A and P_B respectively.

   There are now two cases: we show each for A, the one for B being analogous.

Case($A \equiv p_i$). Then $\pi_1(\langle M, N\rangle) \in P_A = [\![A]\!]$.

Case($A \not\equiv p_i$). Then $\pi_1(\langle M, N\rangle)$ is simple, so we use (R3): it suffices to show that whenever $\pi_1\langle M, N\rangle \longrightarrow^* Q$ and Q is a I-term, then $Q \in [\![A]\!]$.

If $\pi_1(\langle M, N\rangle)$ is stubborn, then the desideratum is trivial.

Otherwise, if $\pi_1(\langle M, N\rangle) \longrightarrow^* Q$ where Q is a I-term, then the reduction must be of the form

$$\pi_1(\langle M, N\rangle) \longrightarrow^* \pi_1(\langle M', N'\rangle) \longrightarrow M' \longrightarrow^* Q$$

where $M \longrightarrow^* M'$ and $N \longrightarrow^* N'$: otherwise, the outermost projection construct would persist. But, by assumption, $M \in [\![A]\!]$, and

$$M \longrightarrow^* M' \longrightarrow^* Q$$

so by multiple applications of (R2) we get that $Q \in [\![A]\!]$.

3. We only show the case for K and T, with the other cases being analogous (e.g. using (P5)(c)(ii) for GL).

   First, we show that $\mathsf{let\ box}\, u \Leftarrow M\ \mathsf{in}\ N \in P_C$, and we invoke (P5)(c)(i) to do so. It suffices to show that $\Delta\,;\Gamma \vdash M \in P_{\Box A}$, that $\Delta, u{:}A\,;\Gamma \vdash N \in P_C$, and whenever $M \longrightarrow^* \mathsf{box}\, Q$ then $\Delta\,;\Gamma \vdash N[Q/u] \in P_C$. The first of these is implied by the assumption that $\Delta\,;\Gamma \vdash M \in [\![A]\!] \subseteq P_A$. For the second, we infer that—by Lemma 5 and Theorem 21—we have that $\cdot\,;\Delta, u{:}A \vdash u \in [\![A]\!]$. Hence, as $\Delta \sqsubseteq \Delta, u{:}A$, we have by the assumption that

   $$\Delta, u{:}A\,;\Gamma \vdash N \equiv N[u/u] \in [\![C]\!]$$

   The final desideratum also follows: if $M \longrightarrow^* \mathsf{box}\, Q$ then, by the definition of $[\![\Box A]\!]$, we have that $\cdot\,;\Delta \vdash Q \in [\![A]\!]$ and hence—by the assumption—that $\Delta\,;\Gamma \vdash N[Q/u] \in [\![C]\!] \subseteq P_C$.

   For the rest, there are two cases.

   Case(M is stubborn). Then so is $\mathsf{let\ box}\, u \Leftarrow M\ \mathsf{in}\ N$, as the let construct persists. As it is a simple term, it never reduces to a I-term, and it is in P_C, it is also in $[\![C]\!]$, simply by invoking (R3).

   Case(M is not stubborn). We distinguish again on whether C is a base type or not.

   Case($C \equiv p_i$). Then $\mathsf{let\ box}\, u \Leftarrow M\ \mathsf{in}\ N \in P_C = [\![C]\!]$.

CASE($C \not\equiv p_i$). Then $\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N$ is simple, so we use (R3): it suffices to show that whenever $\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N \longrightarrow^* Q$ and Q is a I-term, then $Q \in [\![C]\!]$.
If $\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N$ is stubborn, then the desideratum is trivial.
Otherwise, if $\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N \longrightarrow^* Q$ where Q is a I-term, then the reduction must be of the form

$$\begin{aligned} & \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N \\ \longrightarrow^* & \mathsf{let\ box}\ u \Leftarrow \mathsf{box}\ U\ \mathsf{in}\ N' \\ \longrightarrow & N'[U/u] \\ \longrightarrow^* & Q \end{aligned}$$

where $M \longrightarrow^* \mathsf{box}\, U$ and $N \longrightarrow^* N'$: otherwise the let construct would persist. But, by assumption, $\Delta\,;\Gamma \vdash M \in [\![\Box A]\!]$, so by multiple applications of (R2) we infer that $\Delta\,;\Gamma \vdash \mathsf{box}\, U \in [\![\Box A]\!]$ and hence that $\cdot;\Delta \vdash U \in [\![A]\!]$. By the assumption, we get $\Delta;\Gamma \vdash N[U/u] \in [\![C]\!]$. But

$$N[U/u] \longrightarrow^* N'[U/u] \longrightarrow^* Q$$

so, by repeated applications of (R2), $Q \in [\![C]\!]$.

□

6.3 The main theorem

Definition 12. A *substitution* is a finite function $\sigma : \mathcal{V} \rightharpoonup \Lambda$ from the set of all variables $\mathcal{V}$ to the set of all possible terms Λ.

Definition 13. A substitution $\sigma : \mathcal{V} \rightharpoonup \Lambda$ is *type-preserving from* $\Delta'\,;\Gamma'$ *to* $\Delta\,;\Gamma$, written

$$\Delta'\,;\Gamma' \stackrel{\sigma}{\Longrightarrow}_{\mathsf{D}\mathcal{L}} \Delta\,;\Gamma$$

just if

1. $dom(\sigma) \subseteq \textsc{Vars}\,(\Delta) \cup \textsc{Vars}\,(\Gamma)$,
2. $(x : C) \in \Gamma$ implies $\Delta'\,;\Gamma' \vdash \sigma(x) : C$, and
3. either
   - $\mathcal{L} \in \{\mathsf{K}, \mathsf{T}\}$ and $(u : C) \in \Delta$ implies $\cdot\,;\Delta' \vdash \sigma(u) \in C$, or

- $\mathcal{L} = \mathsf{K4}$ and $(u : C) \in \Delta$ implies $\Delta' ; \Delta'^{\perp} \vdash (\sigma(u))^{\perp} \in C$, or
- $\mathcal{L} = \mathsf{GL}$ and there exists a variable z such that $(u : C) \in \Delta$ implies $\Delta' ; \Delta'^{\perp}, z^{\perp} : \Box C \vdash (\sigma(u))^{\perp} \in C$, or
- $\mathcal{L} = \mathsf{S4}$ and $(u : C) \in \Delta$ implies $\Delta' ; \cdot \vdash \sigma(u) \in C$.

We write if $\sigma : \mathcal{V} \rightharpoonup \Lambda$ is a substitution, we write $\sigma[x \mapsto N] : \mathcal{V} \rightharpoonup \Lambda$ to mean the substitution defined by

$$\sigma(y) \stackrel{\text{def}}{=} \begin{cases} \sigma(y) & \text{if } y \not\equiv x \\ N & \text{if } y \equiv x \end{cases}$$

One may weaken substitutions freely:

Lemma 6 (Substitution Weakening)**.** *If* $\Delta' ; \Gamma' \vdash \sigma : \Delta ; \Gamma$ *and* $\Delta' \sqsubseteq \Delta''$ *and* $\Gamma' \sqsubseteq \Gamma'$ *then* $\Delta'' ; \Gamma'' \vdash \sigma : \Delta ; \Gamma$.

Proof. Use weakening for individual terms. □

It is easy to show the following convenient technical result:

Lemma 7 (Modal Drop)**.** *Given a type-preserving substitution* $\sigma : \mathcal{V} \rightharpoonup \Lambda$*, such that* $\Delta' ; \Gamma' \stackrel{\sigma}{\Longrightarrow}_{\mathsf{D}\mathcal{L}} \Delta ; \Gamma$ *we also have that*

- *If* $\mathcal{L} \in \{\mathsf{K}, \mathsf{T}\}$*, then* $\cdot ; \Delta' \stackrel{\sigma}{\Longrightarrow}_{\mathsf{DK}} \cdot ; \Delta$
- *If* $\mathcal{L} = \mathsf{K4}$*, then* $\Delta' ; \Delta'^{\perp} \stackrel{\sigma}{\Longrightarrow}_{\mathsf{DK4}} \Delta ; \Delta^{\perp}$
- *If* $\mathcal{L} = \mathsf{GL}$*, then, for some variable* z *we have*

$$\Delta' ; \Delta'^{\perp}, z^{\perp} : \Box A \stackrel{\sigma}{\Longrightarrow}_{\mathsf{DGL}} \Delta ; \Delta^{\perp}, z^{\perp} : \Box A$$

- *If* $\mathcal{L} = \mathsf{S4}$*, then* $\Delta' ; \cdot \stackrel{\sigma}{\Longrightarrow}_{\mathsf{DS4}} \Delta ; \cdot$

Proof. Trivial. □

We extend the action of substitutions on terms, as follows:

$$\sigma(y) \stackrel{\text{def}}{=} \begin{cases} \sigma(y) & \text{if } y \in dom(\sigma) \\ y & \text{otherwise} \end{cases}$$
$$\sigma(\lambda x{:}A.\ M) \stackrel{\text{def}}{=} \lambda x{:}A.\ \sigma(M)$$
$$\sigma(MN) \stackrel{\text{def}}{=} \sigma(M)\sigma(N)$$
$$\sigma(\langle M, N\rangle) \stackrel{\text{def}}{=} \langle \sigma(M), \sigma(N)\rangle$$
$$\sigma(\pi_i(M)) \stackrel{\text{def}}{=} \pi_i(\sigma(M))$$
$$\sigma(\mathsf{box}\ M) \stackrel{\text{def}}{=} \mathsf{box}\ \sigma(M)$$
$$\sigma(\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N) \stackrel{\text{def}}{=} \mathsf{let\ box}\ u \Leftarrow \sigma(M)\ \mathsf{in}\ \sigma(N)$$
$$\sigma(\mathsf{fix}\ z\ \mathsf{in\ box}\ M) \stackrel{\text{def}}{=} \mathsf{fix}\ z\ \mathsf{in\ box}\ \sigma(M) \quad \text{(for GL only)}$$

where we silently α-rename bound variables in λ-abstractions, let bindings, or fixpoint terms, so as to avoid substituting for something bound, or having something free become bound after a substitution.

Lemma 8. *If* $\Delta' ; \Gamma' \stackrel{\sigma}{\Longrightarrow} \Delta ; \Gamma$ *and* $\Delta ; \Gamma \vdash M : C$ *then* $\Delta' ; \Gamma' \vdash \sigma(M) : C$.

Proof. By induction on M. We only show some cases: for the others the IH suffices.

> Case(x). Then $(x : C) \in \Gamma$, or—in the cases of T and $\mathsf{S4}$—$(x : C) \in \Delta$. If $(x : C) \in \Gamma$ then we have that $\Delta' ; \Gamma' \vdash \sigma(x) : C$. Otherwise, say in the case of T, we have that $\cdot ; \Delta' \vdash \sigma(x) : C$, so we use modal dereliction (Theorem 12) to conclude $\Delta' ; \cdot \vdash \sigma(x) : C$, and then weakening to obtain the result. The case of $\mathsf{S4}$ is similar.
>
> Case$(\lambda x{:}A.\ M)$. Then we have that $\Delta ; \Gamma, x{:}A \vdash M : B$ for some A and B such that $C \equiv A \to B$. Define
>
> $$\sigma' \stackrel{\text{def}}{=} \sigma[x \mapsto x]$$
>
> so that, by weakening and definition, $\Delta' ; \Gamma', x{:}A \stackrel{\sigma'}{\Longrightarrow} \Delta ; \Gamma, x{:}A$. By the IH, we have
>
> $$\Delta' ; \Gamma', x{:}A \vdash \sigma'(M) : B$$
>
> But $\sigma'(M) \equiv \sigma(M)$, so a single use of $(\to \mathcal{I})$ yields the result.
>
> Case$(\mathsf{box}\ M)$.

– (for K and T)

Then $\cdot\,;\Delta \vdash M : A$ for some A such that $C \equiv \Box A$. We have that

$$\cdot\,;\Delta' \stackrel{\sigma}{\Longrightarrow} \cdot\,;\Delta$$

by Lemma 7; thus, applying the IH yields $\cdot\,;\Delta' \vdash \sigma(M) : A$. But as $\sigma(\mathsf{box}\ M) \equiv \mathsf{box}\ \sigma(M)$, a single use of $(\Box\mathcal{I}_{\mathsf{K}})$ suffices.

– (others) Similar.

Case($\mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ M$). (for GL only) Similarly.

Case($\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N$). Similar to the case for λ-abstraction.

□

Theorem 23 (Candidats)**.** *Let $\mathcal{P} = \{P_A\}$ be a family satisfying properties (P1)–(P5). If $\Delta\,;\Gamma \vdash_{D\mathcal{L}} M : A$, and $\Delta'\,;\Gamma' \vdash \sigma : \Delta\,;\Gamma$ is a substitution such that*

$$(x : C) \in \Gamma \quad \Longrightarrow \quad \Delta'\,;\Gamma' \vdash \sigma(x) \in [\![C]\!]$$

and either

– $\mathcal{L} \in \{K, T\}$ *and* $(u : C) \in \Delta$ *implies* $\cdot\,;\Delta' \vdash \sigma(u) \in [\![C]\!]$*, or*

– $\mathcal{L} = K4$ *and* $(u : C) \in \Delta$ *implies* $\Delta'\,;\Delta'^{\perp} \vdash (\sigma(u))^{\perp} \in [\![C]\!]$*, or*

– $\mathcal{L} = GL$ *and there exists a variable z such that* $(u : C) \in \Delta$ *implies* $\Delta'\,;\Delta'^{\perp}, z^{\perp} : \Box C \vdash (\sigma(u))^{\perp} \in [\![C]\!]$*, or*

– $\mathcal{L} = S4$ *and* $(u : C) \in \Delta$ *implies* $\Delta'\,;\cdot \vdash \sigma(u) \in [\![C]\!]$

then

$$\Delta'\,;\Gamma' \vdash \sigma(M) \in [\![A]\!]$$

Proof. By induction on M.

Case(x).

Then $(x : C) \in \Gamma$, or—in the cases of T and $\mathsf{S4}$—$(x : C) \in \Delta$. In the case of the former, the assumption implies that $\Delta'\,;\Gamma' \vdash \sigma(x) \in [\![C]\!]$. In the case of the latter, we conclude that $\cdot\,;\Delta' \vdash \sigma(x) \in [\![C]\!]$. We use Theorem 21 and $(\mathsf{R0})$(c) to conclude that $\Delta'\,;\cdot \vdash \sigma(x) \in [\![C]\!]$, and then Theorem 21 again and $(\mathsf{R0})$(a) to weaken this to $\Delta'\,;\Gamma' \vdash \sigma(x) \in [\![C]\!]$.

Case($\lambda x{:}A.\ M$). Then $\Delta\,;\Gamma, x{:}A \vdash M : B$ for some B. We use Theorem 22(1): it suffices to show that for $\Delta'' \sqsupseteq \Delta'$ and $\Gamma'' \sqsupseteq \Gamma'$, and for every $\Delta'';\Gamma'' \vdash N \in [\![A]\!]$ we have $\Delta''\,;\Gamma'' \vdash \sigma(M)[N/x] \in [\![B]\!]$, for then Theorem 22(1) yields

$$\Delta'\,;\Gamma' \vdash \lambda x{:}A.\ \sigma(M) \in [\![A \to B]\!]$$

But then $\lambda x{:}A.\ \sigma(M) \equiv \sigma(\lambda x{:}A.\ M)$, hence the result. To this end, let

$$\sigma' \stackrel{\text{def}}{=} \sigma[x \mapsto N]$$

Then, by weakening both contexts in σ, we have that

$$\Delta''\,;\Gamma'' \stackrel{\sigma'}{\Longrightarrow} \Delta\,;\Gamma, x{:}A$$

and $\sigma(M)[N/x] \equiv \sigma'(M)$. But σ' satisfies the premises of the IH for M, hence

$$\Delta''\,;\Gamma'' \vdash \sigma'(M) \in [\![B]\!]$$

which is the desideratum.

Case(MN). Then $\Delta\,;\Gamma \vdash M : A \to B$ and $\Delta\,;\Gamma \vdash N : A$ for some A and B. We use the IH twice to conclude that $\Delta'\,;\Gamma' \vdash \sigma(M) \in [\![A \to B]\!]$ and $\Delta'\,;\Gamma' \vdash \sigma(N) \in [\![A]\!]$. By the definition of $[\![-]\!]$, this yields that

$$\Delta'\,;\Gamma' \vdash \sigma(MN) \equiv \sigma(M)\sigma(N) \in [\![B]\!]$$

Case($\langle M, N\rangle$). Then $\Delta\,;\Gamma \vdash M \in A$ and $\Delta\,;\Gamma \vdash N \in B$. We use Theorem 22(2): it suffices to show that $\Delta'\,;\Gamma' \vdash \sigma(M) \in [\![A]\!]$ and $\Delta'\,;\Gamma' \vdash \sigma(N) \in [\![B]\!]$, for then

$$\Delta'\,;\Gamma' \vdash \sigma(\langle M, N\rangle) \equiv \langle \sigma(M), \sigma(N)\rangle \in [\![A \times B]\!]$$

But the two desiderata follow from the IH.

Case($\pi_1(M)$). Then $\Delta\,;\Gamma \vdash M \in A \times B$ for some A and B. We use the IH to conclude that $\Delta'\,;\Gamma' \vdash \sigma(M) \in [\![A \times B]\!]$, and hence that

$$\Delta'\,;\Gamma' \vdash \sigma(\pi_1(M)) \equiv \pi_1(\sigma(M)) \in [\![A]\!]$$

which follows by the definition of $[\![A \times B]\!]$.

Case($\pi_2(M)$). Similar.

CASE($\mathsf{box}\ M$). We only show the case for K and T, the others being similar.

Then $\cdot;\Delta \vdash M : A$ for some A. By Lemma 7, we have that $\cdot;\Delta' \stackrel{\sigma}{\Longrightarrow} \cdot;\Delta$. Then, by the IH, we have that $\cdot\,;\Delta' \vdash \sigma(M) \in [\![A]\!]$. So, by ($\mathsf{P4}$)(c), $\mathsf{box}\,\sigma(M) \in P_{\Box A}$. It now suffices—by the definition of $[\![\Box A]\!]$—to show that

$$\mathsf{box}\,\sigma(M) \longrightarrow^* \mathsf{box}\,M'$$

implies $\cdot;\Delta' \vdash M' \in [\![A]\!]$. But then we must have $\sigma(M) \longrightarrow^* M'$, so by repeated applications of ($\mathsf{R2}$) we have $M' \in [\![A]\!]$.

CASE($\mathsf{fix}\ z\ \mathsf{in}\ \mathsf{box}\ M$). (for GL only) Similar.

CASE($\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N$).

We show the case for K. We have $\Delta\,;\Gamma \vdash M : A$ and $\Delta, u{:}A\,;\Gamma \vdash N : C$. We use Theorem 22(a): to show that

$$\Delta'\,;\Gamma' \vdash \sigma(\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N) \equiv \mathsf{let\ box}\ u \Leftarrow \sigma(M)\ \mathsf{in}\ \sigma(N) \in [\![C]\!]$$

It suffices to show that $\Delta'\,;\Gamma' \vdash \sigma(M) \in [\![\Box A]\!]$—which we have by the IH—and that whenever $\Delta'' \sqsupseteq \Delta'$ and $\cdot\,;\Delta'' \vdash Q \in [\![A]\!]$, then $\Delta''\,;\Gamma' \vdash \sigma(N)[Q/u] \in [\![C]\!]$.

Define

$$\sigma' \stackrel{\text{def}}{=} \sigma[u \mapsto Q]$$

Then, by weakening the modal context in σ, we have

$$\Delta'', u{:}A\,;\Gamma' \stackrel{\sigma'}{\Longrightarrow} \Delta, u{:}A\,;\Gamma$$

By the IH,

$$\Delta'', u{:}A\,;\Gamma' \vdash \sigma'(N) \in [\![C]\!]$$

But $\sigma'(N) \equiv \sigma(N)[Q/u]$.

□

Corollary 3. *If $\mathcal{P} = \{P_A\}$ is a family satisfying properties ($\mathsf{P1}$)–($\mathsf{P5}$), then*

$$P_A = \Lambda_A$$

Proof. By Theorem 23 we have that $M \in [\![A]\!]$ for every $\Delta\,;\Gamma \vdash M : A$. Hence $\Lambda_A \subseteq [\![A]\!] \subseteq P_A \subseteq \Lambda_A$. □

Chapter 7

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 the categorical semantics of simply-typed λ-calculus in cartesian closed categories, we refer to the classic books of Lambek and Scott (1988) and Crole (1993), as well as the detailed presentation of Abramsky and Tzevelekos (2011).

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.

In this chapter we introduce a modest amount of monoidal category theory that we will use in our modelling attempts. Further material on monoidal functors can be found in MacLane (Mac Lane, 1978, §XI.2). We draw a lot on a superbly lucid treatment by Melliès (Melliès, 2009, §5), which is specifically geared towards categorical logic.

7.1 Cartesian Closed Categories

Definition 14. A category $\mathcal{C}$ is *cartesian closed* just if it is cartesian (i.e. has a terminal object $\mathbf{1}$ and a binary products) and has *exponentials*, i.e. for each pair of objects $A, B \in \mathcal{C}$ there is an object $B^A \in \mathcal{C}$ and an arrow

$$\mathsf{ev}_{A,B} : B^A \times A \to B$$

such that for every $f : C \times A \to B$ there is a unique $\lambda(f) : C \to B^A$ such that the following diagram commutes:

$$\begin{array}{ccc} B^A \times A & \xrightarrow{\mathsf{ev}_{A,B}} & B \\ {\scriptstyle \lambda(f)\times id_A}\uparrow & \nearrow_{f} & \\ C \times A & & \end{array}$$

There are many equivalent definitions of cartesian closure, e.g. as a couniversal arrow from $- \times A$ to B for each pair of objects $A, B \in \mathcal{C}$, or as the existence of a right adjoint to the functor $- \times A$—see Crole (1993).

7.2 Lax and Strong Monoidal Functors

Let $\mathcal{C}$ and $\mathcal{D}$ be cartesian categories. We regard them as monoidal categories $(\mathcal{C}, \times, \mathbf{1})$ and $(\mathcal{D}, \times, \mathbf{1})$, respectively.

Definition 15. A functor $F : \mathcal{C} \longrightarrow \mathcal{D}$ between two cartesian categories is *lax monoidal* just if it is equipped with a natural transformation

$$m : F(-) \times F(-) \Rightarrow F(- \times -)$$

as well as an arrow $m_0 : \mathbf{1} \to F(\mathbf{1})$ such that the following diagrams commute:

$$\begin{array}{ccc} (FA \times FB) \times FC & \xrightarrow{\alpha} & FA \times (FB \times FC) \\ {\scriptstyle m_{A,B}\times id_{FC}}\downarrow & & \downarrow{\scriptstyle id_{FA}\times m_{B,C}} \\ F(A \times B) \times FC & & FA \times F(B \times C) \\ {\scriptstyle m_{A\times B,C}}\downarrow & & \downarrow{\scriptstyle m_{A,B\times C}} \\ F((A \times B) \times C) & \xrightarrow[F(\alpha)]{} & F(A \times (B \times C)) \end{array}$$

$$\begin{array}{ccc} FA \times \mathbf{1} & \xrightarrow{\rho_A} & FA \\ {\scriptstyle id_{FA}\times m_0}\downarrow & & \uparrow{\scriptstyle F(\rho_A)} \\ FA \times F\mathbf{1} & \xrightarrow[m_{A,\mathbf{1}}]{} & F(A \times \mathbf{1}) \end{array} \qquad \begin{array}{ccc} \mathbf{1} \times FB & \xrightarrow{\lambda_B} & FB \\ {\scriptstyle m_0\times id_{FB}}\downarrow & & \uparrow{\scriptstyle F(\lambda_B)} \\ F\mathbf{1} \times FB & \xrightarrow[m_{\mathbf{1},B}]{} & F(\mathbf{1} \times B) \end{array}$$

Definition 16. 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.

These 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:

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

Then the $m^{(n)}$'s are a natural transformation, so that

$$m^{(n)} \circ \prod_{i=1}^{n} Ff_i = F\left(\prod_{i=1}^{n} f_i\right) \circ m^{(n)}$$

We also note that if $F : \mathcal{C} \longrightarrow \mathcal{C}$ is a monoidal endofunctor, then so is $F^2 \stackrel{\text{def}}{=} F \circ F$, with components

$$n_{A,B} \stackrel{\text{def}}{=} F^2A \times F^2B \xrightarrow{m_{A,B}} F(FA \times FB) \xrightarrow{F(m_{A,B})} F^2(A \times B)$$

and $n_0 \stackrel{\text{def}}{=} Fm_0 \circ m_0$—see e.g. (Melliès, 2009, §5.9).

7.2.1 Product-Preserving Functors

The definition of lax and strong monoidal functors is widely used as notions of morphism between any two monoidal categories. However, in our setting, the monoidal product will always be the cartesian product. In the rest of this section we note some facts which are particular to the cartesian case.

To start, here is another notion of a functor between cartesian categories that 'plays well with products,' namely that of *product-preserving functors.* The definition seems to be much stronger than simple monoidality.

Definition 17. A *product-preserving functor* $F : \mathcal{C} \longrightarrow \mathcal{D}$ between two cartesian categories is one for which, the arrows

$$\begin{aligned} p_{A,B} &\stackrel{\text{def}}{=} \langle F\pi_1, F\pi_2 \rangle : F(A \times B) \xrightarrow{\cong} F(A) \times F(B) \\ p_0 &\stackrel{\text{def}}{=} !_{F(\mathbf{1})} : F(\mathbf{1}) \xrightarrow{\cong} \mathbf{1} \end{aligned}$$

are isomorphisms.

Product-preserving functors are—indeed—strong monoidal. To show that, all we need to consider is the inverse of the arrows required by the definition, namely

$$m_{A,B} \stackrel{\text{def}}{=} p_{A,B}^{-1} : F(A) \times F(B) \stackrel{\cong}{\to} F(A \times B)$$
$$m_0 \stackrel{\text{def}}{=} p_0^{-1} : \mathbf{1} \stackrel{\cong}{\to} F(\mathbf{1})$$

Before we show that, we first need to note that product-preserving functions satisfy two rather remarkable equations. The first one will often come in handy in calculations:

Proposition 1. *If F is product-preserving, then*

$$m_{A,B} \circ \langle Ff, Fg \rangle = F\langle f, g \rangle$$

for $f : C \to A$, and $g : D \to B$.

Proof. We may compute

$$p_{A,B} \circ F\langle f, g \rangle = \langle F\pi_1 \circ F\langle f, g \rangle, F\pi_2 \circ F\langle f, g \rangle \rangle = \langle Ff, Fg \rangle$$

and, since $p_{A,B}^{-1} = m_{A,B}$, the result follows. □

The second equation concerns the fact that the $m_{A,B}$'s may be used to relate the projections with their image under the functor.

Proposition 2. *Let $F : \mathcal{C} \longrightarrow \mathcal{D}$ be product-preserving, and let*

$$A \xleftarrow{\pi_1^{A,B}} A \times B \xrightarrow{\pi_2^{A,B}} B$$

and

$$FA \xleftarrow{\pi_1^{FA,FB}} FA \times FB \xrightarrow{\pi_2^{FA,FB}} FB$$

be product diagrams in $\mathcal{C}$ and $\mathcal{D}$ respectively. Then

$$F(\pi_i^{A,B}) \circ m_{A,B} = \pi_i^{FA,FB}$$

Proof. $\pi_i \circ m_{A,B}^{-1} = \pi_i \circ \langle F(\pi_1), F(\pi_2) \rangle = F(\pi_i)$ □

We will often write equations of this sort as $F(\pi_1) \circ m = \pi_1$ without further ado. Armed with these facts, it is now easy to see that

Theorem 24. *Any product-preserving functor is strong monoidal, with $m_{A,B}$ and m_0 defined as above.*

Proof. For $f : C \to A$ and $g : D \to B$, we calculate that

$$\begin{aligned}
& m_{A,B} \circ (Ff \times Fg) \\
= \; & \{ \text{definition} \} \\
& m_{A,B} \circ \langle Ff \circ \pi_1, Fg \circ \pi_2 \rangle \\
= \; & \{ \text{Proposition 2} \} \\
& m_{A,B} \circ \langle Ff \circ F(\pi_1) \circ m_{C,D}, Fg \circ F(\pi_2) \circ m_{C,D} \rangle \\
= \; & \{ \text{functoriality of F, naturality of product} \} \\
& m_{A,B} \circ \langle F(f \circ \pi_1), F(g \circ \pi_2) \rangle \circ m_{C,D} \\
= \; & \{ \text{Proposition 1, definition} \} \\
& F(f \times g) \circ m_{C,D}
\end{aligned}$$

so that

$$m : F(-) \times F(-) \Rightarrow F(- \times -)$$

is a natural transformation. The associativity diagram commutes: the proof is a lengthy but simple calculation involving the naturality of the product arrow, the definition $\alpha \stackrel{\text{def}}{=} \langle \pi_1 \pi_1, \langle \pi_2 \pi_1, \pi_2 \rangle \rangle$, and—more crucially—the invertibility of the $m_{A,B}$'s. Commutation of the other two diagrams follows from Proposition 2 and the observation that $\rho_A \stackrel{\text{def}}{=} \pi_1$ and $\lambda_B \stackrel{\text{def}}{=} \pi_2$. □

Rather strikingly, the converse holds as well: these two notions of functors between cartesian categories coincide.

Theorem 25. *Any strong monoidal functor between two cartesian categories is product-preserving.*

Proof. Note that we have that $m_0^{-1} : F(\mathbf{1}) \longrightarrow \mathbf{1}$ is necessarily equal to $!_{F(\mathbf{1})}$, as $\mathbf{1}$ is a terminal object. Hence, it suffices to show that, for any $A, B \in \mathcal{C}$, $m_{A,B}^{-1} = \langle F(\pi_1), F(\pi_2) \rangle$.

We will first show a particular case, *viz.* that

$$m_{A,\mathbf{1}}^{-1} = \langle F\pi_1, F\pi_2 \rangle$$

from which the general case will follow. We compute that

$$(id_{FA} \times m_0)^{-1} = id_{FA}^{-1} \times m_0^{-1} = id_{FA} \times !_{F(\mathbf{1})}$$

Hence, reversing the direction of that arrow as well as that of $m_{A,\mathbf{1}}$ in the second diagram of the definition of lax monoidality yields

$$F(\pi_1) = \pi_1 \circ (id_{FA} \times !_{F(\mathbf{1})}) \circ m^{-1}_{A,\mathbf{1}} = \pi_1 \circ m_{A,\mathbf{1}}$$

once we recall that $\rho_A \stackrel{\text{def}}{=} \pi_1$. Also, as $m_0 : \mathbf{1} \xrightarrow{\cong} F\mathbf{1}$, $F\mathbf{1}$ is also a terminal object, and any arrow into it is of the form $m_0 \circ !_A : A \to F\mathbf{1}$. Hence,

$$\pi_2 \circ m^{-1}_{A,\mathbf{1}} = m_0 \circ !_{F(A\times\mathbf{1})}$$

But $F\pi_2 : F(A \times \mathbf{1}) \to F\mathbf{1}$, so it is also equal to $m_0 \circ !_{F(A\times\mathbf{1})}$. Thus

$$m^{-1}_{A,\mathbf{1}} = \langle F\pi_1, F\pi_2 \rangle$$

Now for the general case. As $m_{A,B}$ is a natural isomorphism, its inverse is a natural transformation with components $m^{-1}_{A,B}$. The naturality square for $(id_A, !_B)$ is

$$\begin{array}{ccc} F(A \times B) & \xrightarrow{m^{-1}_{A,B}} & FA \times FB \\ {\scriptstyle F(id_A\times !_B)}\downarrow & & \downarrow{\scriptstyle id_{FA}\times F(!_B)} \\ F(A \times \mathbf{1}) & \xrightarrow[m^{A,\mathbf{1}}]{} & FA \times F\mathbf{1} \end{array}$$

Calculating down and across gives

$$m^{-1}_{A,\mathbf{1}} \circ F(id_A \times !_B) = \langle F\pi_1, !_{\mathbf{1}} \rangle \circ F(id_A \times !_B) = \langle F\pi_1, !_{F(A\times B)} \rangle$$

whereas across and down gives

$$(id_{FA} \times F(!_B)) \circ m^{-1}_{A,B} = \langle \pi_1 \circ m^{-1}_{A,B}, F(!_B) \circ \pi_2 \circ m^{-1}_{A,B} \rangle$$

The first two components of these should be equal, therefore $\pi_1 \circ m^{-1}_{A,B} = F\pi_1$. Similarly, $\pi_2 \circ m^{-1}_{A,B} = F\pi_2$, and hence $m^{-1}_{A,B} = \langle F\pi_1, F\pi_2 \rangle$. □

7.2.2 Monoidal Natural Transformations

Definition 18. Let $F, G : \mathcal{C} \longrightarrow \mathcal{D}$ be two lax monoidal functors between two cartesian categories $\mathcal{C}, \mathcal{D}$. A *monoidal natural transformation* between F and G is a natural transformation $t : F \Rightarrow G$ such that the following coherence conditions hold:

$$\begin{array}{ccc} FA \times FB & \xrightarrow{t_A\times t_B} & GA \times GB \\ {\scriptstyle m_{A,B}}\downarrow & & \downarrow{\scriptstyle n_{A,B}} \\ F(A \times B) & \xrightarrow[t_{A\times B}]{} & G(A \times B) \end{array} \qquad \begin{array}{ccc} & & \mathbf{1} \\ & {\scriptstyle m_0}\swarrow & \\ F\mathbf{1} & \xrightarrow[t_{\mathbf{1}}]{} & G\mathbf{1} \end{array} \quad {\scriptstyle n_0}\searrow$$

7.3 Categorical Models of Modal Logic

In this section we introduce the main definitions of the structures needed to produce categories that can interpret modal logics. We begin with the basic two examples of Kripke categories (K), and Bierman–de Paiva categories (S4). These are the best behaved, and most commonly encountered in category theory. We then discuss the slightly more obscure cases of Kripke-4 categories (K4), Kripke-T categories (T), and finally Gödel-Löb categories (GL).

7.3.1 Kripke categories

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

Definition 19. 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 model Scott's rule (see §2.5.2), by defining an operation

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

as follows:

$$\frac{f : \prod_{i=1}^{n} A_i \to B}{f^\bullet \stackrel{\text{def}}{=} \prod_{i=1}^{n} FA_i \xrightarrow{m^{(n)}} F\left(\prod_{i=1}^{n} A_i\right) \xrightarrow{Ff} FB}$$

The operation $(-)^\bullet$ 'distributes' over composition with a product arrow. If that arrow is made of projections, the resulting expression is even simpler.

Proposition 3.

1. *Let* $f : \prod_{i=1}^{n} B_i \to C$ *and* $g_i : \prod_{j=1}^{k} A_j \to B_i$ *for* $i = 1, \ldots, n$. *Then*

$$(f \circ \langle \overrightarrow{g_i} \rangle)^\bullet = f^\bullet \circ \left\langle \overrightarrow{g_i^\bullet} \right\rangle$$

2. *For* $f : \prod_{i=1}^{n} A_i \to B$ *and* $\langle \vec{\pi_j} \rangle : \prod_{i=1}^{n} FA_i \to \prod_{j \in J} FA_j$ *for* J *a list with elements from* $\{1, \ldots, n\}$,

$$(f \circ \langle \vec{\pi_j} \rangle)^\bullet = f^\bullet \circ \langle \vec{\pi_j} \rangle$$

Proof. For (1):

$$\begin{aligned}
& (f \circ \langle \overrightarrow{g_i} \rangle)^\bullet \\
= \; & \{ \text{ definition, functoriality } \} \\
& Ff \circ F\langle \overrightarrow{g_i} \rangle \circ m^{(k)} \\
= \; & \{ F \text{ strong monoidal } \} \\
& Ff \circ m^{(n)} \circ \langle \overrightarrow{Fg_i} \rangle \circ m^{(k)} \\
= \; & \{ \text{ naturality of product morphism, definitions } \} \\
& f^\bullet \circ \left\langle \overrightarrow{g_i^\bullet} \right\rangle
\end{aligned}$$

For (2), it suffices notice that $\pi_j^\bullet \stackrel{\text{def}}{=} F\pi_j \circ m^{(n)} = \pi_j$. □

7.3.2 Bierman-de Paiva categories

In addition to a Kripke category, the central gadget in the semantics of S4 is a *monoidal comonad*.

Definition 20. A comonad (F, ϵ, δ) consists of an endofunctor $F : \mathcal{C} \longrightarrow \mathcal{C}$, and two natural transformations

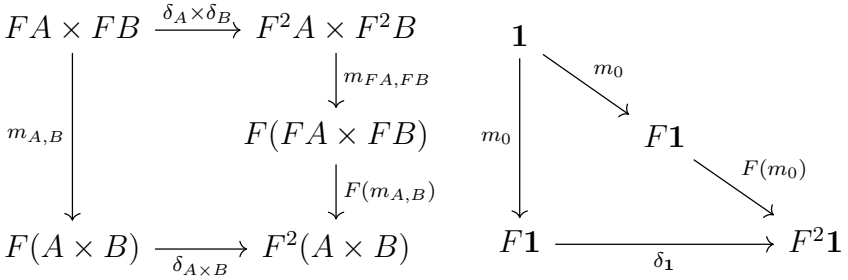
$$\epsilon : F \Rightarrow \mathsf{Id}, \qquad \delta : F \Rightarrow F^2$$

such that the following diagrams commute:

$$\begin{array}{ccc} FA & \xrightarrow{\delta_A} & F^2A \\ {\scriptstyle \delta_A}\downarrow & & \downarrow{\scriptstyle \delta_{F(A)}} \\ F^2A & \xrightarrow[F(\delta_A)]{} & F^3A \end{array} \qquad \begin{array}{ccc} FA & \xrightarrow{\delta_A} & F^2A \\ {\scriptstyle \delta_A}\downarrow & \searrow^{id_{FA}} & \downarrow{\scriptstyle \epsilon_{FA}} \\ F^2A & \xrightarrow[F(\epsilon_A)]{} & FA \end{array}$$

Definition 21. A *monoidal comonad* on a cartesian category $\mathcal{C}$ is a comonad (F, ϵ, δ) such that $F : \mathcal{C} \longrightarrow \mathcal{C}$ is a monoidal functor, and $\epsilon : F \Rightarrow \mathsf{Id}$ and $\delta : F \Rightarrow F^2$ are monoidal natural transformations. Concretely, ϵ and δ being monoidal means that the following diagrams commute:

$$\begin{array}{ccc} FA \times FB & \xrightarrow{\epsilon_A \times \epsilon_B} & A \times B \\ {\scriptstyle m_{A,B}}\downarrow & & \| \\ F(A \times B) & \xrightarrow[\epsilon_{A\times B}]{} & A \times B \end{array} \qquad \begin{array}{ccc} \mathbf{1} & & \\ {\scriptstyle m_0}\downarrow & \searrow & \| \\ F\mathbf{1} & \xrightarrow[\epsilon_{\mathbf{1}}]{} & \mathbf{1} \end{array}$$



Definition 22. A *Bierman-de Paiva category (BdP category)* $(\mathcal{C}, \times, \mathbf{1}, F, \epsilon, \delta)$ is a Kripke category $(\mathcal{C}, \times, \mathbf{1}, F)$ whose functor $F : \mathcal{C} \longrightarrow \mathcal{C}$ is part of a monoidal comonad (F, ϵ, δ).

Bierman-de Paiva categories are the minimal setting in which both the Four and T rules can be modelled. The T rule is modelled directly by the monoidal natural transformation ϵ. On the other hand, the Four rule is modelled by (a generalisation of) something already well-known in category theory, namely the *co-Kleisli lifting*:

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

which is defined as follows:

$$\frac{f : \prod_{i=1}^{n} FA_i \to B}{f^* \stackrel{\text{def}}{=} \prod_{i=1}^{n} FA_i \xrightarrow{\prod_{i=1}^{n} \delta_{A_i}} \prod_{i=1}^{n} F^2 A_i \xrightarrow{m^{(n)}} F\left(\prod_{i=1}^{n} FA_i\right) \xrightarrow{Ff} FB}$$

This operation interacts in the expected way with the transformations δ and ϵ.

Proposition 4.

1. *Let* $f : \prod_{i=1}^{n} FA_i \to B$. *Then* $\delta_B \circ f^* = (f^*)^*$.
2. *Let* $f : \prod_{i=1}^{n} FA_i \to B$. *Then* $\epsilon_B \circ f^* = f$.

Proof.

1. Let $E \stackrel{\text{def}}{=} \prod_{i=1}^{n} FA_i$. Then

$$\begin{aligned}
& \delta_B \circ f^* \\
= \quad & \{ \text{ definition } \} \\
& \delta_B \circ Ff \circ m^{(n)} \circ \prod_{i=1}^{n} \delta_{A_i} \\
= \quad & \{ \, \delta \text{ natural } \} \\
& F^2 f \circ \delta_E \circ m^{(n)} \circ \prod_{i=1}^{n} \delta_{A_i} \\
= \quad & \{ \text{ monoidal equation for } \delta \, \} \\
& F^2 f \circ F(m^{(n)}) \circ m^{(n)} \circ \prod_{i=1}^{n} \delta_{FA_i} \circ \prod_{i=1}^{n} \delta_{A_i} \\
= \quad & \{ \text{ product is functorial } \} \\
& F^2 f \circ F(m^{(n)}) \circ m^{(n)} \circ \prod_{i=1}^{n} \delta_{FA_i} \delta_{A_i} \\
= \quad & \{ \text{ equation of comonads } \} \\
& F^2 f \circ F(m^{(n)}) \circ m^{(n)} \circ \prod_{i=1}^{n} F(\delta_{A_i}) \delta_{A_i} \\
= \quad & \{ \text{ product functorial, } F \text{ product-preserving } \} \\
& F^2 f \circ F(m^{(n)}) \circ F\left(\prod_{i=1}^{n} \delta_{A_i} \right) \circ m^{(n)} \circ \prod_{i=1}^{n} \delta_{A_i} \\
= \quad & \{ \, F \text{ functor, definitions } \} \\
& (f^*)^*
\end{aligned}$$

2. Straightforward calculation involving—amongst other things—the naturality and monoidality of ϵ.

□

The co-Kleisli extension also has a few more properties, and also distributes appropriately over compositions where the first arrow is already 'modalised.'

Proposition 5.

1. $id^*_{FA} = \delta_{FA}$

2. $\epsilon^*_A = id_{FA}$

3. *For* $k : \prod_{i=1}^{n} FA_i \to B$ *and* $l : FB \to C$,

$$(l \circ k^*)^* = l^* \circ k^*$$

4. *For* $k : \prod_{i=1}^{n} A_i \to B$ *and* $l : FB \to C$,

$$(l \circ k^\bullet)^* = l^* \circ k^\bullet$$

5. *Let* $f : \prod_{i=1}^{n} B_i \to C$ *and* $g_i : \prod_{j=1}^{k} FA_j \to B_i$ *for* $i = 1, \ldots, n$. *Then*

$$(f \circ \langle \overrightarrow{g_i} \rangle)^* = f^\bullet \circ \left\langle \overrightarrow{g_i^*} \right\rangle$$

6. *For* $f : \prod_{i=1}^{n} FA_i \to B$ *and* $\langle \vec{\pi_j} \rangle : \prod_{i=1}^{n} FA_i \to \prod_{j \in J} FA_j$ *for* J *a list with elements from* $\{1, \ldots, n\}$,

$$(f \circ \langle \vec{\pi_j} \rangle)^* = f^* \circ \langle \vec{\pi_j} \rangle$$

Proof. Straightforward calculations involving the comonadic equations. (1) and (2) are standard from the theory of comonads and functional programming. (3) and (4) are easy calculations; e.g. for (4):

$$\begin{aligned}
& (l \circ k^\bullet)^* \\
= \; & \{ \text{ definitions } \} \\
& Fl \circ F^2 k \circ F(m^{(n)}) \circ m^{(n)} \circ \prod_{i=1}^{n} \delta_{A_i} \\
= \; & \{ \, \delta \text{ monoidal } \} \\
& Fl \circ F^2 k \circ \delta \circ m^{(n)} \\
= \; & \{ \, \delta \text{ natural } \} \\
& Fl \circ \delta \circ Fk \circ m^{(n)} \\
= \; & \{ \text{ definitions } \} \\
& l^* \circ k^\bullet
\end{aligned}$$

(5) is a straightforward calculation, similar to Proposition 3. (6) is a corollary of (5), once we notice that $\pi_i^* = \delta_{A_i} \circ \pi_i$, and use the definition of $f^* \stackrel{\text{def}}{=} f^\bullet \circ \prod \delta$. □

7.3.3 Kripke-4 categories

Kripke-4 categories model $\mathsf{K4}$; they are essentially 'half a comonad,' namely the half that consists of the comultiplication δ. We still require that one of the comonadic equations, viz. the one that only refers to δ, holds.

Definition 23. A *Kripke-4* category $(\mathcal{C}, \times, \mathbf{1}, F, \delta)$ is a Kripke category $(\mathcal{C}, \times, \mathbf{1}, F)$ along with a monoidal natural transformation

$$\delta : F \Rightarrow F^2$$

such that the following diagram commutes:

$$\begin{array}{ccc} FA & \xrightarrow{\delta_A} & F^2A \\ {\scriptstyle \delta_A}\downarrow & & \downarrow{\scriptstyle \delta_{F(A)}} \\ F^2A & \xrightarrow[F(\delta_A)]{} & F^3A \end{array}$$

Concretely, $\delta : F \Rightarrow F^2$ being monoidal means that the following diagrams commute:

$$\begin{array}{ccc} FA \times FB & \xrightarrow{\delta_A \times \delta_B} & F^2A \times F^2B \\ {\scriptstyle m_{A,B}}\downarrow & & \downarrow{\scriptstyle m_{FA,FB}} \\ & & F(FA \times FB) \\ & & \downarrow{\scriptstyle F(m_{A,B})} \\ F(A \times B) & \xrightarrow[\delta_{A\times B}]{} & F^2(A \times B) \end{array} \qquad \begin{array}{ccc} \mathbf{1} & & \\ {\scriptstyle m_0}\downarrow & \searrow^{m_0} & \\ F\mathbf{1} & & F\mathbf{1} \\ & \searrow^{F(m_0)} & \\ F\mathbf{1} & \xrightarrow[\delta_{\mathbf{1}}]{} & F^2\mathbf{1} \end{array}$$

We can also model the Four rule in Kripke-4 categories, but in a way that is slightly more involved than the simple co-Kleisli lifting of Bierman–de Paiva categories. They are the minimal setting in which this can happen; see §2.5.2. To see this, let $(\mathcal{C}, \times, \mathbf{1}, F, \delta)$ be a Kripke-4 category, and write

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

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

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

as follows:

$$\frac{f : \prod_{i=1}^{n} FA_i \times_l \prod_{i=1}^{n} A_i \to B}{f^{\#} \stackrel{\text{def}}{=} \prod_{i=1}^{n} FA_i \xrightarrow{\langle \overrightarrow{\delta_{A_i} \pi_i}, \overrightarrow{\pi_i} \rangle} \left(\prod_{i=1}^{n} F^2 A_i \right) \times_l \left(\prod_{i=1}^{n} FA_i \right) \xrightarrow{m^{(2n)}} F \left(\prod_{i=1}^{n} FA_i \times_l \prod_{i=1}^{n} A_i \right) \xrightarrow{Ff} B}$$

Even though it might seem slightly unnatural at first sight, we can show that the $(-)^{\#}$ operation satisfies very natural distribution laws. For example, composition works if we take care to substitute *the same thing* for all the assumptions.

Proposition 6.

1. *Let* $f : \prod_{i=1}^{n} B_i \to C$ *and* $g_i : \prod_{j=1}^{k} FA_j \times \prod_{j=1}^{k} A_j \to B_i$ *for* $i = 1, \ldots, n$. *Then*

$$(f \circ \langle \overrightarrow{g_i} \rangle)^{\#} = f^{\bullet} \circ \left\langle \overrightarrow{g_i^{\#}} \right\rangle$$

2. *For* $k : \prod_{i=1}^{n} FA_i \times \prod_{i=1}^{n} A_i \to B$ *and* $l : FB \to C$, *then*

$$(l \circ k^{\#})^{*} = l^{*} \circ k^{\#}$$

Proof. (1) and (2) are straightforward calculations, similar to Propositions 3 and 5 respectively. □

Even though this setting might seem a bit limited compared to a full monoidal comonad, quite a few results can be recovered. For example, it can be shown that $(-)^{\#}$ still does the expected thing is δ is post-composed to it; in fact, it leads us straight back to the 'co-Kleisli extension' (even though we should not speak of a co-Kleisli extension when we do not have a full comonad).

Proposition 7. *Let* $f : \prod_{i=1}^{n} FA_i \times_l \prod_{i=1}^{n} A_i \to B$. *Then*

$$\delta_B \circ f^{\#} = \left(f^{\#} \right)^{*}$$

Proof. Let $E \stackrel{\text{def}}{=} \prod_{i=1}^{n} FA_i \times_l \prod_{i=1}^{n} A_i$. Then

$$
\begin{aligned}
& \delta_B \circ f^{\#} \\
= \quad & \{ \text{ definition } \} \\
& \delta_B \circ Ff \circ m^{(2n)} \circ \langle \overrightarrow{\delta_{A_i} \pi_i}, \overrightarrow{\pi_i} \rangle \\
= \quad & \{ \, \delta \text{ natural } \} \\
& F^2 f \circ \delta_E \circ m^{(2n)} \circ \langle \overrightarrow{\delta_{A_i} \pi_i}, \overrightarrow{\pi_i} \rangle \\
= \quad & \{ \, \delta \text{ monoidal } \} \\
& F^2 f \circ F(m^{(2n)}) \circ m^{(2n)} \circ \left(\prod_{i=1}^{n} \delta_{FA_i} \times_l \prod_{i=1}^{n} \delta_{A_i} \right) \circ \langle \overrightarrow{\delta_{A_i} \pi_i}, \overrightarrow{\pi_i} \rangle \\
= \quad & \{ \text{ product after bracket law } \} \\
& F^2 f \circ F(m^{(2n)}) \circ m^{(2n)} \circ \left\langle \overrightarrow{\delta_{FA_i} \delta_{A_i} \pi_i}, \overrightarrow{\delta_{A_i} \pi_i} \right\rangle \\
= \quad & \{ \text{ law pertaining to } \delta \, \} \\
& F^2 f \circ F(m^{(2n)}) \circ m^{(2n)} \circ \left\langle \overrightarrow{F(\delta_{A_i}) \delta_{A_i} \pi_i}, \overrightarrow{\delta_{A_i} \pi_i} \right\rangle \\
= \quad & \{ \text{ naturality of product morphisms, projections } \} \\
& F^2 f \circ F(m^{(2n)}) \circ m^{(2n)} \circ \left\langle \overrightarrow{F(\delta_{A_i}) \pi_i}, \overrightarrow{\pi_i} \right\rangle \circ \left\langle \overrightarrow{\delta_{A_i} \pi_i} \right\rangle \\
= \quad & \{ \text{ Proposition 2 } \} \\
& F^2 f \circ F(m^{(2n)}) \circ m^{(2n)} \circ \left\langle \overrightarrow{F(\delta_{A_i}) F(\pi_i) \circ m^{(n)}}, \overrightarrow{F(\pi_i) \circ m^{(n)}} \right\rangle \circ \left\langle \overrightarrow{\delta_{A_i} \pi_i} \right\rangle \\
= \quad & \{ \text{ naturality of product morphism, } F \text{ strong monoidal } \} \\
& F^2 f \circ F(m^{(2n)}) \circ F\left(\left\langle \overrightarrow{\delta_{A_i} \pi_i}, \overrightarrow{\pi_i} \right\rangle \right) \circ m^{(n)} \circ \left\langle \overrightarrow{\delta_{A_i} \pi_i} \right\rangle \\
= \quad & \{ \text{ definitions } \} \\
& F(f^{\#}) \circ m^{(n)} \circ \prod_{i=1}^{n} \delta_{A_i}
\end{aligned}
$$

□

Finally, when the morphism of type $\prod_{i=1}^{n} FA_i \times_l \prod_{i=1}^{n} A_i \to B$ does not depend on the A_i, then the operation $(-)^{\#}$ reduces to a simpler expression, which—were F and δ components of a comonad—would coincide with the co-Kleisli extension of the arrow.

Proposition 8. *Let* $f : \prod_{i=1}^{n} FA_i \to B$. *Then*

$$(f \circ \langle \overrightarrow{\pi_{FA_i}} \rangle)^{\#} = f^*$$

Proof. We calculate:

$$\begin{aligned}
& (f \circ \langle \overrightarrow{\pi_{FA_i}} \rangle)^{\#} \\
= & \quad \{ \text{ definition } \} \\
& F\,(f \circ \langle \overrightarrow{\pi_{FA_i}} \rangle) \circ m^{(2n)} \circ \langle \overrightarrow{\delta_{A_i} \pi_i}, \overrightarrow{\pi_i} \rangle \\
= & \quad \{ \text{ functoriality, and Proposition 1 } \} \\
& Ff \circ m^{(n)} \circ \langle \overrightarrow{F(\pi_{FA_i})} \rangle \circ m^{(2n)} \circ \langle \overrightarrow{\delta_{A_i} \pi_i}, \overrightarrow{\pi_i} \rangle \\
= & \quad \{ \text{ naturality of product morphism, and Proposition 2 } \} \\
& Ff \circ m^{(n)} \circ \langle \overrightarrow{\pi_{F^2 A_i}} \rangle \circ \langle \overrightarrow{\delta_{A_i} \pi_i}, \overrightarrow{\pi_i} \rangle \\
= & \quad \{ \text{ naturality of product morphisms, projections } \} \\
& Ff \circ m^{(n)} \circ \langle \overrightarrow{\delta_{A_i} \pi_i} \rangle
\end{aligned}$$

□

And, finally, we prove another crucial distribution property of $(-)^{\#}$. Namely, if we substitute 'the same thing' at appropriate types, the hash distributes in the following way:

Proposition 9. *Let* $f : \prod_{i=1}^{n} FB_i \times \prod_{i=1}^{n} B_i \to B$, *and* $g_i : \prod_{i=1}^{n} FA_i \times \prod_{i=1}^{n} A_i \to B$. *Then*

$$\left(f \circ \langle \overrightarrow{g_i^{\#} \circ \langle \overrightarrow{\pi_{FA_i}} \rangle}, \overrightarrow{g_i} \rangle \right)^{\#} = f^{\#} \circ \langle \overrightarrow{g_i^{\#}} \rangle$$

Proof.

$$\begin{aligned}
& \left(f \circ \left\langle \overrightarrow{g_i^{\#} \circ \langle \overrightarrow{\pi_{FA_i}} \rangle}, \overrightarrow{g_i} \right\rangle \right)^{\#} \\
= & \quad \{ \text{ Proposition 6(1) } \} \\
& f^{\bullet} \circ \left\langle \overrightarrow{\left(g_i^{\#} \circ \langle \overrightarrow{\pi_{FA_i}} \rangle \right)^{\#}}, \overrightarrow{g_i^{\#}} \right\rangle \\
= & \quad \{ \text{ Proposition 8 } \} \\
& f^{\bullet} \circ \left\langle \overrightarrow{\left(g_i^{\#} \right)^{*}}, \overrightarrow{g_i^{\#}} \right\rangle \\
= & \quad \{ \text{ Proposition 7 } \} \\
& f^{\bullet} \circ \left\langle \overrightarrow{\delta \circ g_i^{\#}}, \overrightarrow{g_i^{\#}} \right\rangle \\
= & \quad \{ \text{ definitions } \} \\
& f^{\#} \circ \langle \overrightarrow{g_i^{\#}} \rangle
\end{aligned}$$

□

7.3.4 Kripke-T categories

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

Definition 24. A *Kripke-T* category $(\mathcal{C}, \times, \mathbf{1}, F, \delta)$ is a Kripke category $(\mathcal{C}, \times, \mathbf{1}, F)$ along with a monoidal natural transformation

$$\epsilon : F \Rightarrow \mathsf{Id}$$

Modelling the T rule from §2.5.2 amounts to precomposition with a product of a bunch of components of $\epsilon : F \Rightarrow \mathsf{Id}$. This operation interacts nicely with Scott's rule:

Proposition 10. *Let* $f : \prod_{i=1}^{n} A_i \to B$. *Then*

$$f \circ \prod_{i=1}^{n} \epsilon_{A_i} = \epsilon_B \circ f^\bullet$$

Proof. Let $E \stackrel{\text{def}}{=} \prod_{i=1}^{n} A_i$. Then

$$\epsilon_B \circ f^\bullet = f \circ \epsilon_E \circ m^{(n)} = f \circ \prod_{i=1}^{n} \epsilon_{A_i}$$

by the definition of $(-)^\bullet$, the naturality of ϵ, and its being a monoidal transformation. □

7.3.5 Gödel-Löb categories

Gödel-Löb are the setting where Löb's rule can be modelled. This requires a notion of *modal fixed point*.

Definition 25. Let $(\mathcal{C}, \times, \mathbf{1}, F, \delta)$ be a Kripke-4 category. A *modal fixed point* of $f : \prod_{i=1}^{n} FB_i \times \prod_{i=1}^{n} B_i \times FA \to A$ is an arrow

$$f^\dagger : \prod_{i=1}^{n} FB_i \to FA$$

such that the following diagram commutes:

$$\begin{array}{ccc} \prod_{i=1}^{n} FB_i & \xrightarrow{\langle id^\#, (f^\dagger)^* \rangle} & F\left(\prod_{i=1}^{n} FB_i \times \prod_{i=1}^{n} B_i\right) \times F^2 A \\ {\scriptstyle f^\dagger}\downarrow & \swarrow_{f^\bullet} & \\ FA & & \end{array}$$

Definition 26. Given Kripke-4 category $(\mathcal{C}, \times, \mathbf{1}, F, \delta)$, an object $A \in \mathcal{C}$ *has modal fixed points* just if for each $B \in \mathcal{C}$ there is a hom-set map

$$(-)^{\dagger}_{B} : \mathcal{C}\left(\prod_{i=1}^{n} FB_i \times \prod_{i=1}^{n} B_i \times FA, A\right) \to \mathcal{C}\left(\prod_{i=1}^{n} FB_i, FA\right)$$

such that, for each $f : \prod_{i=1}^{n} FB_i \times \prod_{i=1}^{n} B_i \times FA \to A$, $f^{\dagger}$ is a modal fixed point of f.

This is an *external* specification of modal fixed points, in the sense that they are given as a map on the hom-sets of the Kripke-4 category. We might instead consider an *internal* specification, i.e. through an appropriate notion of a *modal fixed point combinator*. This will—unsurprisingly—be an arrow

$$\mathbb{Y} : F(A^{FA}) \to FA$$

which is the type of the Gödel-Löb axiom $\Box(\Box A \to A) \to \Box A$ of provability logic.

Definition 27. Let $(\mathcal{C}, \times, \mathbf{1}, F, \delta)$ be a Kripke-4 category. A *modal fixed point combinator at* $A \in \mathcal{C}$ is an arrow

$$\mathbb{Y}_A : F(A^{FA}) \to FA$$

such that for each B and $f : \prod_{i=1}^{n} FB_i \times \prod_{i=1}^{n} B_i \times FA \to A$,

$$\prod_{i=1}^{n} FB_i \xrightarrow{(\lambda(f))^{\#}} F(A^{FA}) \xrightarrow{\mathbb{Y}_A} FA$$

is a modal fixed point of f.

We can prove that having a modal fixed point combinator as above is equivalent to having modal fixed points at A. But for that, we will need a lemma.

Lemma 9. *If* $f : \prod_{i=1}^{n} FA_i \times \prod_{i=1}^{n} A_i \times FB \to B$ *and* $a : \prod_{i=1}^{n} FA_i \to F^2A$, *then*

$$ev^{\bullet} \circ \langle (\lambda f)^{\#}, a \rangle = f^{\bullet} \circ \langle id^{\#}, a \rangle$$

Proof. Calculation:

$$\begin{aligned}
& \mathsf{ev}^\bullet \circ \langle (\lambda f)^\# , a \rangle \\
= \; & \{ \text{definitions} \} \\
& F\mathsf{ev} \circ m \circ \left\langle F(\lambda f) \circ m \circ \langle \overrightarrow{\delta \pi_i}, \overrightarrow{\pi_i} \rangle, a \right\rangle \\
= \; & \{ \text{product equation, definition of } (-)^* \} \\
& F\mathsf{ev} \circ m \circ (F(\lambda f) \times id) \circ \left\langle m \circ \langle \overrightarrow{\delta \pi_i}, \overrightarrow{\pi_i} \rangle, a \right\rangle \\
= \; & \{ m \text{ natural} \} \\
& F\mathsf{ev} \circ F\left(\lambda f \times id\right) \circ m \circ \left\langle m \circ \langle \overrightarrow{\delta \pi_i}, \overrightarrow{\pi_i} \rangle, a \right\rangle \\
= \; & \{ \text{cartesian closure, definition of } (-)^\bullet \text{ and } (-)^\# \} \\
& f^\bullet \circ \left\langle id^\#, a \right\rangle
\end{aligned}$$

□

Theorem 26. *Let there be a Kripke-Ⅎ category $(\mathcal{C}, \times, \mathbf{1}, F, \delta)$. An object $A \in \mathcal{C}$ has modal fixed points if and only if it has a modal fixed point combinator at A.*

Proof. For the backwards direction, we define $(-)^\dagger_B$ by mapping $f : FB \times B \times FA \to A$ to its modal fixed point $\mathbb{Y}_A \circ (\lambda(f))^\#$.

For the forwards direction, let

$$g \stackrel{\text{def}}{=} F(A^{FA}) \times A^{FA} \times FA \xrightarrow{\langle \pi_2, \pi_3 \rangle} A^{FA} \times FA \xrightarrow{\mathsf{ev}} A$$

We will show that $g^\dagger : F(A^{FA}) \to FA$ is a modal fixed point combinator at A. For this, it suffices to show that, for any $f : FB \times B \times FA \to A$, the arrow $g^\dagger \circ (\lambda(f))^\#$ is a modal fixed point of f.

It is easy to calculate that

$$g^\dagger = \mathsf{ev}^\bullet \circ \langle id, \left(g^\dagger\right)^* \rangle$$

Then, it follows that

$$\begin{aligned}
& g^\dagger \circ (\lambda f)^\# \\
= \; & \{ \text{above, plus naturality of angled brackets} \} \\
& \mathsf{ev}^\bullet \circ \langle (\lambda f)^\# , \left(g^\dagger\right)^* \circ (\lambda f)^\# \rangle \\
= \; & \{ \text{Proposition 6} \} \\
& \mathsf{ev}^\bullet \circ \langle (\lambda f)^\# , \left(g^\dagger \circ (\lambda f)^\#\right)^* \rangle \\
= \; & \{ \text{Lemma 9} \} \\
& f^\bullet \circ \langle id^\#, \left(g^\dagger \circ (\lambda f)^\#\right)^* \rangle
\end{aligned}$$

□

Finally,

Proposition 11. *If in a Kripke-4 category we have a modal fixed point map* $(-)^\dagger$ *that derived by a modal fixed point combinator* $\mathbb{Y}_A$*, then this map is natural, in the sense that*

$$\left(f \circ (\langle g^\# \circ \langle \overrightarrow{\pi_{FA_i}} \rangle, g \rangle \times id)\right)^\dagger = f^\dagger \circ g^\#$$

Proof. Use the preceding theorem (Theorem 26) along with naturality of $\lambda(-)$ and Proposition 9. □

Chapter 8

Categorical semantics

In this chapter we use the modal category theory developed in §7 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
CGL	$\longleftrightarrow$	DGL	$\longleftrightarrow$	Gödel-Löb 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. The case for GL remains incomplete in the present document.

We begin by endowing our calculi with an equational theory, and then proceed to show soundness and completeness for this equational theory.

8.1 Equational Theory

To state the full set of equatios, we will need the notion of *term contexts*, i.e. terms with a single *hole*.

Definition 28 (Term Contexts)**.**

1. Term contexts $C[-]$ are defined by the following grammar:

$$\begin{aligned} C[-] \quad ::= \quad & [-] \mid \lambda x{:}A.\, C[-] \mid C[-]\ M \mid M\ C[-] \\ & \mid \langle C[-], M\rangle \mid \langle M, C[-]\rangle \mid \pi_i(C[-]) \\ & \mid \mathsf{box}\ C[-] \\ & \mid \mathsf{let\ box}\ u \Leftarrow C[-]\ \mathsf{in}\ M \\ & \mid \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ C[-] \end{aligned}$$

2. $C[-]$ is *non-modal* just if it is generated without the clause $\mathsf{box}\, C[-]$.

3. $C[-]$ does not bind u just if it is generated without the clause $\mathsf{let\ box}\, u \Leftarrow C[-]\ \mathsf{in}\ C[-]$.

We write $C[M]$ for the term that results from (capture-insensitive) substitution of the term M for the hole $[-]$ of the term context $C[-]$.

The equational rules that pertain to all our systems can be found in Figure 8.1, whereas the equations for the various modalities can be found in Figure 8.2. To obtain the complete set, one should also add congruences for function types, and rules to make equality an equivalence relation. We need not include substitution rules, as the next theorem shows that they are derivable.

Theorem 27. *Structural rules of weakening, exchange and contraction for contexts are admissible in the equational theory. Furthermore, the following rules are derivable in the equational theory:*

1. *(Substitution)*

$$\frac{\Delta\,;\Gamma, x{:}A \vdash M = N : C \qquad \Delta\,;\Gamma \vdash P = Q : A}{\Delta\,;\Gamma \vdash M[P/x] = N[Q/x] : C}$$

2. *(Modal Substitution)*

$$\frac{\Delta, u{:}A\,;\Gamma \vdash M = N : C \qquad \cdot\,;\Delta \vdash P = Q : \Box A}{\Delta\,;\Gamma \vdash M[P/u] = N[Q/u] : C}$$

8.1.1 Commuting Conversions

The most interesting rules are the unavoidable commuting conversions that arise from the study of the categorical semantics of our systems.

The rule (commweak) is a 'weakening' rule that disposes of an explicit substitution which binds a non-occuring variable. This rule has never been considered in the study of dual-context systems, for DILL (Barber, 1996) was a linear system, and Davies and Pfenning (Pfenning and Davies, 2001) did not study neither reduction nor equality. However, a similar rule was proposed by Goubault-Larrecq (1996) in his study of Bierman and de Paiva's calculus for S4. This rule was later included in (Bierman and de Paiva, 2000).

The rule (commlet), read in one direction, allows one to 'pull' an explicit substitution that is buried in a subterm to an outermost position—as long as that would

Figure 8.1: Equations for all systems

Function Spaces

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

Modality

$$\frac{\Delta\,;\Gamma \vdash M : \Box A}{\Delta\,;\Gamma \vdash \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in\ box}\ u = M : \Box A}\,(\Box\eta)$$

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

Commuting Conversions

(commlet)

$$\frac{\Delta\,;\Gamma \vdash C[\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N] : C \qquad C[-] \text{ is non-modal, does not bind } u}{\Delta\,;\Gamma \vdash \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ C[N] = C[\mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in}\ N] : C}$$

(commweak)

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

(commcontr)

$$\frac{\Delta\,;\Gamma \vdash M : \Box A \qquad \Delta, u{:}A, v{:}A\,;\Gamma \vdash N : C \qquad u, v \notin \mathrm{fv}(M)}{\Delta\,;\Gamma \vdash \mathsf{let\ box}\ u \Leftarrow M\ \mathsf{in\ let\ box}\ v \Leftarrow M\ \mathsf{in}\ N = \mathsf{let\ box}\ w \Leftarrow M\ \mathsf{in}\ N[w, w/u, v] = N : C}$$

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.

Figure 8.2: Equations for the modalities

For DK and DT:

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

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

For DK4:

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

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

For DGL:

$$\frac{\Delta\,;\Delta^{\perp}, z^{\perp} : \Box A \vdash M^{\perp} : A \qquad \Delta, u{:}A\,;\Gamma \vdash N : C}{\Delta\,;\Gamma \vdash \mathsf{let\ box}\ u \Leftarrow \mathsf{fix}\ z\ \mathsf{in\ box}\ M\ \mathsf{in}\ N = N\left[M\left[\mathsf{fix}\ z\ \mathsf{in\ box}\ M/z\right]/u\right] : C}\ (\Box\beta_{\mathsf{GL}})$$

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

For DS4:

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

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

not imply that it binds something in the process. A variant of it was considered in the study of DILL by Barber (1996), and is also mentioned by Kakutani (2007). It is worth noting that, as a special case, (commlet) includes a form of 'exchange,' namely swapping of the order of non-interacting explicit substitutions; this special case is thoroughly studied by Goubault-Larrecq (1996).

Finally, (commcontr) is a 'contraction' rule. This is also unfamiliar in dual-context calculi—essentially for the same reasons as (commweak)—but is well-known as a 'garbage collecton' rule in Bierman–de Paiva type calculi: see (Goubault-Larrecq, 1996), Bierman and de Paiva (2000) and Kakutani (2007).

8.2 Categorical Interpretation

We are now fully equipped to define the categorical semantics of our dual-context systems. For background on the categorical semantics of simply-typed λ-calculus in cartesian closed categories, we refer to the classics by Lambek and Scott (1988) and Crole (1993), as well as the detailed presentation of Abramsky and Tzevelekos (2011).

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:

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

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 all logics, but we use each of the maps defined in §7 to interpret the different introduction rules for the modality. To do that we need more than just a Kripke category: for K4 we need a Kripke-4 category; for T a Kripke-T category, for GL a Gödel-Löb category, and for S4 a Bierman-de Paiva category.

Figure 8.3: Categorical Semantics

Definitions for all calculi

$$[\![\Delta\,;\Gamma, x{:}A, \Gamma' \vdash x : A]\!] \stackrel{\text{def}}{=} \pi : [\![\Delta\,;\Gamma, x{:}A, \Gamma']\!] \longrightarrow [\![A]\!]$$

$$[\![\Delta\,;\Gamma \vdash \langle M, N\rangle : A \to B]\!] \stackrel{\text{def}}{=} \langle [\![\Delta\,;\Gamma \vdash M : A]\!]\,, [\![\Delta\,;\Gamma \vdash N : B]\!]\rangle$$

$$[\![\Delta\,;\Gamma \vdash \pi_i(M) : A_i]\!] \stackrel{\text{def}}{=} \pi_i \circ [\![\Delta\,;\Gamma \vdash M : A_1 \times A_2]\!]$$

$$[\![\Delta\,;\Gamma \vdash \lambda x{:}A.M : A \to B]\!] \stackrel{\text{def}}{=} \lambda\,([\![\Delta\,;\Gamma, x : A \vdash M : B]\!]) : [\![\Delta\,;\Gamma]\!] \longrightarrow [\![B]\!]^{[\![A]\!]}$$

$$[\![\Delta\,;\Gamma \vdash MN : B]\!] \stackrel{\text{def}}{=} \mathsf{ev} \circ \langle [\![\Delta\,;\Gamma \vdash M : A \to B]\!]\,, [\![\Delta\,;\Gamma \vdash N : A]\!]\rangle$$

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

Definitions for various modalities

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

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

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

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

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

The full definition is given in Figure 8.3. 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

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

8.3 Soundness

The main tools in proving soundness of our interpretation are (a) lemmas giving the categorical interpretation of various admissible rules, and (b) a fundamental lemma relating substitution of terms to composition in the category. In the sequel we often use informal vector notation for contexts: for example, we write $\vec{u} : \vec{B}$ for the context $u_1 : B_1, \ldots, u_n : B_m$. We also write $[\vec{N}/\vec{u}]$ for the simultaneous, capture-avoiding substitution $[N_1/u_1, \ldots, N_m/u_n]$.

First, we interpret weakening and exchange.

Lemma 10 (Semantics of Weakening)**.**

1. *Let* $\Delta \,;\, \Gamma, x{:}C, \Gamma' \vdash M : A$ *with* $x \notin \mathrm{FV}(M)$*. Then*

$$[\![\Delta \,;\, \Gamma, x{:}C, \Gamma' \vdash M : A]\!] = [\![\Delta \,;\, \Gamma, \Gamma' \vdash M : A]\!] \circ \pi$$

   where $\pi : [\![\Delta \,;\, \Gamma, x{:}C, \Gamma']\!] \to [\![\Delta \,;\, \Gamma, \Gamma']\!]$ *is the obvious projection.*

2. *Let* $\Delta, u{:}B, \Delta' \,;\, \Gamma \vdash M : A$ *with* $u \notin \mathrm{FV}(M)$*. Then*

$$[\![\Delta, u{:}B, \Delta' \,;\, \Gamma \vdash M : A]\!] = [\![\Delta, \Delta' \,;\, \Gamma \vdash M : A]\!] \circ \pi$$

   where $\pi : [\![\Delta, u{:}B, \Delta' \,;\, \Gamma]\!] \to [\![\Delta, \Delta' \,;\, \Gamma]\!]$ *is the obvious projection.*

Proof. By induction on the two derivations. All cases are straightforward. □

Lemma 11 (Semantics of Exchange)**.**

1. *Let* $\Delta \,;\, \Gamma, x{:}C, y{:}D, \Gamma' \vdash M : A$*. Then*

$$[\![\Delta \,;\, \Gamma, x{:}C, y{:}D, \Gamma' \vdash M : A]\!] = [\![\Delta \,;\, \Gamma, y{:}D, x{:}C, \Gamma' \vdash M : A]\!] \circ (\cong)$$

   where $(\cong) : [\![\Delta \,;\, \Gamma, x{:}C, y{:}D, \Gamma']\!] \stackrel{\cong}{\to} [\![\Delta \,;\, \Gamma, y{:}D, x{:}C, \Gamma']\!]$ *is the obvious isomorphism.*

2. *Let* $\Delta, u{:}C, v{:}D, \Delta' \,;\, \Gamma \vdash M : A$. *Then*

$$[\![\Delta, u{:}C, v{:}D, \Delta' \,;\, \Gamma \vdash M : A]\!] = [\![\Delta, v{:}D, u{:}C, \Delta' \,;\, \Gamma \vdash M : A]\!] \circ (\cong)$$

where $(\cong) : [\![\Delta, u{:}C, v{:}D \,;\, \Gamma]\!] \xrightarrow{\cong} [\![\Delta, v{:}D, u{:}C \,;\, \Gamma]\!]$ *is the obvious isomorphism.*

Proof. By induction on the two derivations. All cases are straightforward. □

Then, we move on to something particular to the cases of T and $\mathsf{S4}$, namely the interpretation of the Modal Dereliction rule—see §12.

Lemma 12 (Semantics of Dereliction)**.** *Let* $\Delta \,;\, \Gamma, \Gamma' \vdash_{D\mathcal{L}} M : A$ *where* $\mathcal{L} \in \{\mathsf{T}, \mathsf{S4}\}$ *and* $\Gamma = \vec{z} : \vec{C}$. *Then*

$$[\![\Delta, \Gamma \,;\, \Gamma' \vdash M : A]\!]_{\mathcal{L}} = [\![\Delta \,;\, \Gamma, \Gamma' \vdash M : A]\!]_{\mathcal{L}} \circ \left(\overrightarrow{id_\Delta} \times \overrightarrow{\epsilon_{C_i}} \times \overrightarrow{id'_\Gamma}\right)$$

Proof. By induction on the derivation of $\Delta \,;\, \Gamma, \Gamma' \vdash_{\mathsf{D}\mathcal{L}} M : A$. All cases are straightforward. The case for $(\Box\mathcal{E})$ depends on the semantics of exchange lemma. □

Only one thing remains to show, namely that the components of the various models interact in the expected way with the semantics of terms of the calculus.

Lemma 13 (Double box)**.**

1. *If* $\Delta \,;\, \Delta^\perp \vdash_{DK4} M : A$, *then*

$$[\![\Delta \,;\, \Gamma \vdash \mathsf{box}\,(\mathsf{box}\,M) : \Box\Box A]\!] = \delta_A \circ [\![\Delta \,;\, \Gamma \vdash \mathsf{box}\,M : \Box A]\!]$$

2. *If* $\Delta \,;\, \cdot \vdash_{DS4} M : A$, *then*

$$[\![\Delta \,;\, \Gamma \vdash \mathsf{box}\,(\mathsf{box}\,M) : \Box\Box A]\!] = \delta_A \circ [\![\Delta \,;\, \Gamma \vdash \mathsf{box}\,M : \Box A]\!]$$

Proof.

1. Let $f \stackrel{\text{def}}{=} [\![\Delta \,;\, \Delta^\perp \vdash M : A]\!]$. Then

$$\begin{aligned}
& [\![\Delta \,;\, \Gamma \vdash \mathsf{box}\,(\mathsf{box}\,M) : \Box\Box A]\!] \\
= \;& \{\,\text{definitions}\,\} \\
& (f^\# \circ \pi_\Delta^{\Delta;\Delta^\perp})^\# \circ \pi_\Delta^{\Delta;\Gamma} \\
= \;& \{\,\text{Proposition 8}\,\} \\
& \left(f^\#\right)^* \circ \pi_\Delta^{\Delta;\Gamma} \\
= \;& \{\,\text{Proposition 7}\,\} \\
& \delta_A \circ f^\# \circ \pi_\Delta^{\Delta;\Gamma} \\
= \;& \{\,\text{definitions}\,\} \\
& \delta_A \circ [\![\Delta \,;\, \Gamma \vdash \mathsf{box}\,M : \Box A]\!]
\end{aligned}$$

2. Let $f \stackrel{\text{def}}{=} [\![\Delta\,;\cdot \vdash M : A]\!]$. Then

$$\begin{aligned}
& [\![\Delta\,;\Gamma \vdash \mathsf{box}\,(\mathsf{box}\,M) : \Box\Box A]\!] \\
= \;& \{\,\text{definitions}\,\} \\
& (f^*)^* \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \;& \{\,\text{Proposition 4}\,\} \\
& \delta_A \circ f^* \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \;& \{\,\text{definitions}\,\} \\
& \delta_A \circ [\![\Delta\,;\Gamma \vdash \mathsf{box}\,M : \Box A]\!]
\end{aligned}$$

□

Lemma 14 (Identity Lemma)**.** *For* $(u_i : B_i) \in \Delta$*, and* $\mathcal{L} \in \{\mathsf{K}, \mathsf{K4}, \mathsf{T}, \mathsf{S4}\}$*,*

$$[\![\Delta\,;\Gamma \vdash \mathsf{box}\,u_i : \Box B_i]\!]_{\mathcal{L}} = \pi_{\Box B_i}^{\Delta;\Gamma}$$

Proof.

Case(K, T).

$$\begin{aligned}
& [\![\Delta\,;\Gamma \vdash \mathsf{box}\,u_i : \Box B_i]\!] \\
= \;& \{\,\text{definition}\,\} \\
& [\![\cdot\,;\Delta \vdash u_i : B_i]\!]^{\bullet} \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \;& \{\,\text{definition}\,\} \\
& \left(\pi_{B_i}^{\cdot;\Delta}\right)^{\bullet} \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \;& \{\,\text{Proposition 2}\,\} \\
& \pi_{\Box B_i}^{\Delta;\cdot} \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \;& \{\,\text{projections}\,\} \\
& \pi_{\Box B_i}^{\Delta;\Gamma}
\end{aligned}$$

Case(K4).

$$
\begin{aligned}
& [\![\Delta\,;\Gamma \vdash \mathsf{box}\ u_i : \Box B_i]\!] \\
= \;& \{\,\text{definition}\,\} \\
& [\![\Delta\,;\Delta^{\perp} \vdash u_i^{\perp} : B_i]\!]^{\#} \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \;& \{\,\text{definition}\,\} \\
& \left(\pi_{B_i}^{\Delta;\Delta^{\perp}}\right)^{\#} \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \;& \{\,\text{definition}\,\} \\
& F\pi_{B_i}^{\Delta;\Delta^{\perp}} \circ m^{(2n)} \circ \langle \overrightarrow{\delta_{B_i}\pi_i}, \overrightarrow{\pi_i} \rangle \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \;& \{\,\text{Proposition 2}\,\} \\
& \pi_{\Box B_i}^{\Box\Delta;\Box\Delta^{\perp}} \circ \langle \overrightarrow{\delta_{B_i}\pi_i}, \overrightarrow{\pi_i} \rangle \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \;& \{\,\text{projections}\,\} \\
& \pi_{\Box B_i}^{\Delta;\Gamma}
\end{aligned}
$$

Case(S4).

$$
\begin{aligned}
& [\![\Delta\,;\Gamma \vdash \mathsf{box}\ u_i : \Box B_i]\!] \\
= \;& \{\,\text{definition}\,\} \\
& [\![\Delta\,;\cdot \vdash u_i : B_i]\!]^{*} \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \;& \{\,\text{definition}\,\} \\
& \left(\epsilon_{B_i} \circ \pi_{\Box B_i}^{\Delta;\cdot}\right)^{*} \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \;& \{\,\text{Proposition 5}\,\} \\
& \epsilon_{B_i}^{*} \circ \pi_{\Box B_i}^{\Delta;\cdot} \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \;& \{\,\text{Proposition 5}\,\} \\
& \pi_{\Box B_i}^{\Delta;\cdot} \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \;& \{\,\text{projections}\,\} \\
& \pi_{\Box B_i}^{\Delta;\Gamma}
\end{aligned}
$$

□

Lemma 15 (Semantics of Substitution)**.** *Suppose that* $\vec{u} : \vec{B}\,;\vec{x} : \vec{A} \vdash_{\mathsf{DL}} P : C$*. Let* $\Delta\,;\Gamma \vdash_{\mathsf{DL}} M_i : A_i$ *for* $i = 1, \ldots, n$*, and let*

$$\alpha_i \stackrel{def}{=} [\![\Delta\,;\Gamma \vdash M_i : A_i]\!]_{\mathcal{L}}$$

If either

1. $\mathcal{L} \in \{\mathsf{K}, \mathsf{T}\}$ *and* $\cdot\,;\Delta \vdash N_j : B_j$ *for* $j = 1, \ldots, m$, *or*

2. $\mathcal{L} = \mathsf{K4}$ *and* $\Delta\,;\Delta^{\perp} \vdash N_j^{\perp} : B_j$ *for* $j = 1, \ldots, m$, *or*

3. $\mathcal{L} = \mathsf{S4}$ *and* $\Delta\,;\cdot \vdash N_j : B_j$ *for* $j = 1, \ldots, m$,

then, letting for $j = 1, \ldots, m$

$$\beta_j \stackrel{def}{=} [\![\Delta\,;\Gamma \vdash \mathsf{box}\ N_j : \Box B_j]\!]$$

we have that

$$\Big[\!\Big[\Delta\,;\Gamma \vdash P[\vec{N}/\vec{u}, \vec{M}/\vec{x}] : C\Big]\!\Big] = \Big[\!\Big[\vec{u} : \vec{B}\,;\vec{x} : \vec{A} \vdash P : C\Big]\!\Big] \circ \langle \beta_1, \ldots, \beta_m, \alpha_1, \ldots, \alpha_n \rangle$$

Proof. By induction on the derivation of $\vec{u} : \vec{B}\,;\vec{x} : \vec{A} \vdash P : C$. Most cases are straightforward, and use a combination of standard equations that hold in cartesian closed categories—see §7.1 or (Crole, 1993, §2)—in order to perform calculations very close the ones detailed in (Abramsky and Tzevelekos, 2011, §1.6.5). Because of the precise definitions we have used, we also need to make use of Lemma 10 to interpret weakening whenever variables in the context do not occur freely in the term. We only cover the modal cases.

CASE($\Box$var). We do the case T only. The case for $\mathsf{S4}$ is similar, but uses Proposition 4 instead of Proposition 10. Then $P \equiv u_i$ for some u_i amongst the $\vec{u}$. Hence, the LHS is $\Delta\,;\Gamma \vdash N_i : B_i$, whereas we calculate that the RHS is

$$\begin{aligned}
& \Big[\!\Big[\vec{u} : \vec{B}\,;\vec{x} : \vec{A} \vdash P : C\Big]\!\Big] \circ \langle \vec{\beta}, \vec{\alpha} \rangle \\
= \;& \{\,\text{definition}\,\} \\
& \epsilon_{B_i} \circ \pi^{\vec{u}:\vec{B};\vec{x}:\vec{A}}_{u_i:B_i} \circ \langle \vec{\beta}, \vec{\alpha} \rangle \\
= \;& \{\,\text{projection}\,\} \\
& \epsilon_{B_i} \circ [\![\Delta\,;\Gamma \vdash \mathsf{box}\ N_i : \Box B_i]\!] \\
= \;& \{\,\text{definition}\,\} \\
& \epsilon_{B_i} \circ ([\![\cdot\,;\Delta \vdash N_i : B_i]\!])^{\bullet} \circ \pi^{\Delta;\Gamma}_{\Delta} \\
= \;& \{\,\text{Proposition 10}\,\} \\
& [\![\cdot\,;\Delta \vdash N_i : B_i]\!] \circ \prod_{i=1}^{l} \epsilon_{C_i} \circ \pi^{\Delta;\Gamma}_{\Delta} \\
= \;& \{\,\text{Semantics of Dereliction (Lemma 12)}\,\} \\
& [\![\Delta\,;\cdot \vdash N_i : B_i]\!] \circ \pi^{\Delta;\Gamma}_{\Delta} \\
= \;& \{\,\text{Semantics of Weakening (Lemma 10)}\,\} \\
& [\![\Delta\,;\Gamma \vdash N_i : B_i]\!]
\end{aligned}$$

Case($\Box\mathcal{I}_{\mathsf{K}}$). We have that $\vec{u} : \vec{B} \,;\, \vec{x} : \vec{A} \vdash \mathsf{box}\ P : \Box C$, so that $\cdot \,;\, \vec{u} : \vec{B} \vdash P : C$, with the result that none of the variables $\vec{x}$ occurs free in P. We use this fact and the definition of substitution to calculate:

$$
\begin{array}{ll}
 & \Big[\!\Big[\Delta \,;\, \Gamma \vdash \mathsf{box}\ (P[\vec{N}/\vec{u}, \vec{M}/\vec{x}]) : \Box C \Big]\!\Big] \\
= & \{\, \text{definition, and non-occurence of the } \vec{x} \,\} \\
 & \Big(\Big[\!\Big[\cdot \,;\, \Delta \vdash P[\vec{N}/\vec{u}] : C \Big]\!\Big] \Big)^{\bullet} \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= & \{\, \text{IH} \,\} \\
 & \Big(\Big[\!\Big[\cdot \,;\, \vec{u} : \vec{B} \vdash P : C \Big]\!\Big] \circ \Big\langle \overrightarrow{\big[\!\big[\cdot \,;\, \Delta \vdash N_i : B_i \big]\!\big]} \Big\rangle \Big)^{\bullet} \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= & \{\, \text{Proposition 3} \,\} \\
 & \Big(\Big[\!\Big[\cdot \,;\, \vec{u} : \vec{B} \vdash P : C \Big]\!\Big] \Big)^{\bullet} \circ \Big\langle \overrightarrow{\big[\!\big[\cdot \,;\, \Delta \vdash N_i : B_i \big]\!\big]^{\bullet}} \Big\rangle \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= & \{\, \text{naturality of product morphism, definition} \,\} \\
 & \Big(\Big[\!\Big[\cdot \,;\, \vec{u} : \vec{B} \vdash P : C \Big]\!\Big] \Big)^{\bullet} \circ \pi_{\vec{u}:\vec{B}}^{\vec{u}:\vec{B};\vec{x}:\vec{A}} \circ \Big\langle \overrightarrow{\beta}, \overrightarrow{\alpha} \Big\rangle \\
= & \{\, \text{definition} \,\} \\
 & \Big[\!\Big[\vec{u} : \vec{B} \,;\, \vec{x} : \vec{A} \vdash \mathsf{box}\ P : \Box C \Big]\!\Big] \circ \Big\langle \overrightarrow{\beta}, \overrightarrow{\alpha} \Big\rangle
\end{array}
$$

Case($\Box\mathcal{I}_{\mathsf{K4}}$). We have that $\vec{u} : \vec{B} \,;\, \vec{x} : \vec{A} \vdash \mathsf{box}\ P : \Box C$, so that $\vec{u} : \vec{B} \,;\, \overrightarrow{u^{\perp}} : \vec{B} \vdash P : C$, with the result that none of the variables $\vec{x}$ or $\overrightarrow{x^{\perp}}$ occur free in P. Hence,

$$\Big(P[\vec{N}/\vec{u}, \vec{M}/\vec{x}] \Big)^{\perp} \equiv P[\vec{N}/\vec{u}, \overrightarrow{N^{\perp}}/\overrightarrow{u^{\perp}}]$$

by Theorem 7. Now we calculate:

$$
\begin{array}{ll}
& \left[\!\left[\Delta\,;\Gamma \vdash \mathsf{box}\,(P[\vec{N}/\vec{u},\vec{M}/\vec{x}]) : \Box C\right]\!\right] \\
= & \{\,\text{definition, and non-occurence of the } \vec{x} \text{ and } \overrightarrow{x^{\perp}}\,\} \\
& \left(\left[\!\left[\Delta\,;\Delta^{\perp} \vdash P[\vec{N}/\vec{u},\overrightarrow{N^{\perp}}/\overrightarrow{u^{\perp}}] : C\right]\!\right]\right)^{\#} \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= & \{\,\text{IH}\,\} \\
& \left(\left[\!\left[\vec{u} : \vec{B}\,;\vec{u^{\perp}} : \vec{B} \vdash P : C\right]\!\right] \circ \left\langle \overrightarrow{\left[\!\left[\Delta\,;\Delta^{\perp} \vdash \mathsf{box}\,N_i : \Box B_i\right]\!\right]}, \overrightarrow{\left[\!\left[\Delta\,;\Delta^{\perp} \vdash N_i : B_i\right]\!\right]} \right\rangle\right)^{\#} \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= & \{\,\text{Proposition } \mathbf{??}\,\} \\
& \left[\!\left[\vec{u} : \vec{B}\,;\vec{u^{\perp}} : \vec{B} \vdash P : C\right]\!\right]^{\bullet} \circ \left\langle \overrightarrow{\left[\!\left[\Delta\,;\Delta^{\perp} \vdash \mathsf{box}\,N_i : \Box B_i\right]\!\right]^{\#}}, \overrightarrow{\left[\!\left[\Delta\,;\Delta^{\perp} \vdash N_i : B_i\right]\!\right]^{\#}} \right\rangle \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= & \{\,\text{naturality of product morphism, definition}\,\} \\
& \left[\!\left[\vec{u} : \vec{B}\,;\vec{u^{\perp}} : \vec{B} \vdash P : C\right]\!\right]^{\bullet} \circ \left\langle \overrightarrow{\left[\!\left[\Delta\,;\Gamma \vdash \mathsf{box}\,(\mathsf{box}\,N_i) : \Box\Box B_i\right]\!\right]}, \overrightarrow{\left[\!\left[\Delta\,;\Gamma \vdash \mathsf{box}\,N_i : \Box B_i\right]\!\right]} \right\rangle \\
= & \{\,\text{Double box (Theorem 13)}\,\} \\
& \left[\!\left[\vec{u} : \vec{B}\,;\vec{u^{\perp}} : \vec{B} \vdash P : C\right]\!\right]^{\bullet} \circ \left\langle \overrightarrow{\delta_{B_i} \circ \left[\!\left[\Delta\,;\Gamma \vdash \mathsf{box}\,N_i : \Box B_i\right]\!\right]}, \overrightarrow{\left[\!\left[\Delta\,;\Gamma \vdash \mathsf{box}\,N_i : \Box B_i\right]\!\right]} \right\rangle \\
= & \{\,\text{naturality and projections}\,\} \\
& \left[\!\left[\vec{u} : \vec{B}\,;\vec{u^{\perp}} : \vec{B} \vdash P : C\right]\!\right]^{\bullet} \circ \left\langle \overrightarrow{\delta_{B_i}\pi_i}, \overrightarrow{\pi_i} \right\rangle \circ \left\langle \overrightarrow{\left[\!\left[\Delta\,;\Gamma \vdash \mathsf{box}\,N_i : \Box B_i\right]\!\right]} \right\rangle \\
= & \{\,\text{some projections and definition}\,\} \\
& \left[\!\left[\vec{u} : \vec{B}\,;\vec{x} : \vec{A} \vdash \mathsf{box}\,P : \Box C\right]\!\right] \circ \left\langle \overrightarrow{\beta}, \overrightarrow{\alpha} \right\rangle
\end{array}
$$

Case($\Box\mathcal{I}_{\mathsf{S4}}$). We have that $\overrightarrow{u} : \overrightarrow{B}\,;\overrightarrow{x} : \overrightarrow{A} \vdash \mathsf{box}\,P : \Box C$, so that $\overrightarrow{u} : \overrightarrow{B}\,;\cdot \vdash P : C$, with the result that none of the variables $\overrightarrow{x}$ occur in P. Hence

$P[\vec{N}/\vec{u}, \vec{M}/\vec{x}] \equiv P[\vec{N}/\vec{u}]$, and we calculate:

$$
\begin{aligned}
& \left[\!\!\left[\Delta \,;\, \Gamma \vdash \mathsf{box}\ (P[\vec{N}/\vec{u}, \vec{M}/\vec{x}]) : \Box C \right]\!\!\right] \\
= \ & \{ \text{definition, and non-occurence of the } \vec{x} \text{ in } P \} \\
& \left[\!\!\left[\Delta \,;\, \cdot \vdash P[\vec{N}/\vec{u}] : C \right]\!\!\right]^{*} \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \ & \{ \text{IH} \} \\
& \left(\left[\!\!\left[\vec{u} : \vec{B} \,;\, \cdot \vdash P : C \right]\!\!\right] \circ \left\langle \overrightarrow{\left[\!\!\left[\Delta \,;\, \cdot \vdash \mathsf{box}\ N_i : \Box B_i \right]\!\!\right]} \right\rangle \right)^{*} \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \ & \{ \text{Proposition } \textbf{??} \} \\
& \left[\!\!\left[\vec{u} : \vec{B} \,;\, \cdot \vdash P : C \right]\!\!\right]^{\bullet} \circ \left\langle \overrightarrow{\left[\!\!\left[\Delta \,;\, \cdot \vdash \mathsf{box}\ N_i : \Box B_i \right]\!\!\right]^{*}} \right\rangle \circ \pi_{\Delta}^{\Delta;\Gamma} \\
= \ & \{ \text{naturality of product morphism, definition} \} \\
& \left[\!\!\left[\vec{u} : \vec{B} \,;\, \cdot \vdash P : C \right]\!\!\right]^{\bullet} \circ \left\langle \overrightarrow{\left[\!\!\left[\Delta \,;\, \Gamma \vdash \mathsf{box}\ (\mathsf{box}\ N_i) : \Box\Box B_i \right]\!\!\right]} \right\rangle \\
= \ & \{ \text{Double box (Theorem 13} \} \\
& \left[\!\!\left[\vec{u} : \vec{B} \,;\, \cdot \vdash P : C \right]\!\!\right]^{\bullet} \circ \left\langle \overrightarrow{\delta_{B_i} \circ \left[\!\!\left[\Delta \,;\, \Gamma \vdash \mathsf{box}\ N_i : \Box B_i \right]\!\!\right]} \right\rangle \\
= \ & \{ \text{product after angled brackets} \} \\
& \left[\!\!\left[\vec{u} : \vec{B} \,;\, \cdot \vdash P : C \right]\!\!\right]^{\bullet} \circ \prod_{i=1}^{n} \delta_{B_i} \circ \left\langle \overrightarrow{\left[\!\!\left[\Delta \,;\, \Gamma \vdash \mathsf{box}\ N_i : \Box B_i \right]\!\!\right]} \right\rangle \\
= \ & \{ \text{some projections and definition of } (-)^{*} \text{ and } [\!\![-]\!\!] \} \\
& \left[\!\!\left[\vec{u} : \vec{B} \,;\, \vec{x} : \vec{A} \vdash \mathsf{box}\ P : \Box C \right]\!\!\right] \circ \left\langle \overrightarrow{\beta}, \overrightarrow{\alpha} \right\rangle
\end{aligned}
$$

□

Theorem 28 (Soundness)**.** *If* $\Delta \,;\, \Gamma \vdash_{\mathsf{D}\mathcal{L}} M = N : A$*, then we have that*

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

Proof. By induction on the derivation of $\Delta \,;\, \Gamma \vdash_{\mathsf{D}\mathcal{L}} M = N : A$. The congruence cases are clear, as is the majority of the ordinary clauses—see Crole (1993) and Abramsky and Tzevelekos (2011). The rules that remain are $(\Box\eta)$, the many variants of $(\Box\beta)$, and the commuting conversions.

First, we prove the modal β (except GL) and η cases by direct calculation. At this point we ought to remark that it is of paramount importance that the monoidal functor be strong: perhaps unexpectedly, this is not only used in proving $(\Box\eta)$ sound, but it is necessary in the cases of $(\Box\beta)$ as well—in particular when obtaining Lemma 14.

Let $\Delta = \vec{u} : \vec{B}$ and $\Gamma = \vec{x} : \vec{A}$. We then calculate:

$$
\begin{aligned}
& [\![\Delta \,;\, \Gamma \vdash \mathsf{let\ box}\ u \Leftarrow \mathsf{box}\ M\ \mathsf{in}\ N : C]\!] \\
= \;& \{\, \text{definition} \,\} \\
& [\![\Delta, u{:}A \,;\, \Gamma \vdash N : C]\!] \circ \langle \overrightarrow{\pi_\Delta}, [\![\Delta \,;\, \Gamma \vdash \mathsf{box}\ M : \Box A]\!] \,, \overrightarrow{\pi_\Gamma} \rangle \\
= \;& \{\, \text{Lemma 14} \,\} \\
& [\![\Delta, u{:}A \,;\, \Gamma \vdash N : C]\!] \circ \langle \overrightarrow{[\![\Delta \,;\, \Gamma \vdash \mathsf{box}\ u_i : \Box B_i]\!]}, [\![\Delta \,;\, \Gamma \vdash \mathsf{box}\ M : \Box A]\!] \,, \overrightarrow{[\![\Delta \,;\, \Gamma \vdash x_i : A_i]\!]} \rangle \\
= \;& \{\, \text{Lemma 15} \,\} \\
& [\![\Delta \,;\, \Gamma \vdash N[\vec{u_i}/\vec{u_i}, M/u, \vec{x_i}/\vec{x_i}] : C]\!]
\end{aligned}
$$

The case of $(\Box\eta)$ is even simpler, and follows immediately from Lemma 14.

The commuting conversions for weakening and contraction are straightforward and follow from the associated lemmas we have proved above. The (commlet) requires a subsidiary induction on contexts $C[-]$, which follows easily from naturality of the various operations of the CCC. □

8.4 Completeness

In this section, we prove that our categorical semantics is complete; that is:

Theorem 29 (Completeness)**.**

1. *If* $[\![\Delta \,;\, \Gamma \vdash_{DK} M : A]\!] = [\![\Delta \,;\, \Gamma \vdash_{DK} N : A]\!]$ *in every Kripke category, then the judgment* $\Delta \,;\, \Gamma \vdash_{DK} M = N : A$ *is derivable.*

2. *If* $[\![\Delta \,;\, \Gamma \vdash_{DK4} M : A]\!] = [\![\Delta \,;\, \Gamma \vdash_{DK4} N : A]\!]$ *in every Kripke-4 category, then the judgment* $\Delta \,;\, \Gamma \vdash_{DK4} M = N : A$ *is derivable.*

3. *If* $[\![\Delta \,;\, \Gamma \vdash_{DT} M : A]\!] = [\![\Delta \,;\, \Gamma \vdash_{DT} N : A]\!]$ *in every Kripke-T category, then the judgment* $\Delta \,;\, \Gamma \vdash_{DT} M = N : A$ *is derivable.*

4. *If* $[\![\Delta \,;\, \Gamma \vdash_{DS4} M : A]\!] = [\![\Delta \,;\, \Gamma \vdash_{DS4} N : A]\!]$ *in every Bierman-de Paiva category, then the judgment* $\Delta \,;\, \Gamma \vdash_{DS4} M = N : A$ *is derivable.*

By the method of Lindenbaum and Tarski, to prove this theorem it suffices to construct a suitable category of each sort from the bare syntax of each calculus. Thus, we construct a Kripke category $\mathbb{C}_{\mathsf{K}}$ based on the syntax of DK, a Bierman-de Paiva category $\mathbb{C}_{\mathsf{S4}}$ based on the syntax of DS4, and so on. The reasoning then proceeds as follows: if an equation holds in all categories of this sort, then it holds

in the one made of syntax, which—and we must also show this—yields the required equality.

To perform the aforementioned syntactic construction, we follow a pattern that we learned from Čubrić et al. (1998). The objects of all our categories will be *two-zoned lists of types*,

$$\langle \vec{B} | \vec{A} \rangle$$

and the morphisms $\langle \vec{B} | \vec{A} \rangle \longrightarrow \langle \vec{D} | \vec{C} \rangle$ shall be two-zoned lists of terms, quotiented *up to provable renaming and equality.*

In the first zone, the typing will have a form that will be readily substitutable for a modal variable. For $\mathbb{C}_{\mathsf{K}}$ and $\mathbb{C}_{\mathsf{T}}$, the morphisms will be

$$\langle \cdot \,;\, \vec{u} : \vec{B} \vdash N_1 : D_1, \ldots, \cdot \,;\, \vec{u} : \vec{B} \vdash N_l : D_l \mid \\ \vec{u} : \vec{B} \,;\, \vec{x} : \vec{A} \vdash M_1 : C_1, \ldots, \vec{u} : \vec{B} \,;\, \vec{x} : \vec{A} \vdash M_k : C_k \rangle$$

whereas for $\mathbb{C}_{\mathsf{S4}}$ they will be

$$\langle \vec{u} : \vec{B} \,;\, \cdot \vdash N_1 : D_1, \ldots, \vec{u} : \vec{B} \,;\, \cdot \vdash N_l : D_l \mid \\ \vec{u} : \vec{B} \,;\, \vec{x} : \vec{A} \vdash M_1 : C_1, \ldots, \vec{u} : \vec{B} \,;\, \vec{x} : \vec{A} \vdash M_k : C_k \rangle$$

Finally, in $\mathbb{C}_{\mathsf{K4}}$ morphisms will respect the structure of complementary variables and their relationship to substitution, and so take the form

$$\langle \vec{u} : \vec{B} \,;\, \vec{u^{\perp}} : \vec{B} \vdash N_1^{\perp} : D_1, \ldots, \vec{u} : \vec{B} \,;\, \vec{u^{\perp}} : \vec{B} \vdash N_l^{\perp} : D_l \mid \\ \vec{u} : \vec{B} \,;\, \vec{x} : \vec{A} \vdash M_1 : C_1, \ldots, \vec{u} : \vec{B} \,;\, \vec{x} : \vec{A} \vdash M_k : C_k \rangle$$

Composition is then defined by substitution, and the identity morphisms will be simply occurences of variables; e.g. in $\mathbb{C}_{\mathsf{K}}$ and $\mathbb{C}_{\mathsf{T}}$ they will be

$$\langle \cdot \,;\, \vec{u} : \vec{B} \vdash u_1 : B_1, \ldots, \cdot \,;\, \vec{u} : \vec{B} \vdash u_m : B_m \mid \\ \vec{u} : \vec{B} \,;\, \vec{x} : \vec{A} \vdash x_1 : A_1, \ldots, \vec{u} : \vec{B} \,;\, \vec{x} : \vec{A} \vdash x_n : A_n \rangle$$

It is easy to verify that composition is associative and that the proposed arrows are identities: associativity corresponds to the so-called *substitution lemma*, and identities vanish up to renaming.

This constitutes a cartesian closed category, on which there is an easy-to-define *strict* monoidal functor. To complete the argument, one shows by induction on M that

$$\left[\!\!\left[\vec{u} : \vec{B} \,;\, \vec{x} : \vec{A} \vdash M : A \right]\!\!\right] = \left\langle - \middle| \cdot \,;\, \vec{v} : \Box\vec{B}, \vec{x} : \vec{A} \vdash \mathsf{let\ box}\ \vec{u} \Leftarrow \vec{v}\ \mathsf{in}\ M : A \right\rangle$$

Chapter 9

Coda

We have thus 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).

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 8), 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 Nielson and Nielson (1992). The distinction between compile-time vs. run-time—or even code vs. value—is known to be expressible in terms of modalities: this result is is due to Davies and Pfenning Davies and Pfenning (2001), who embed two-level λ-calucli in a 'full and faithful' manner in their modal programming language. Even though their system is $\mathsf{DS4}$ 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*. Suppose we pick a cartesian closed category $\mathcal{C}$; we can turn $\mathcal{C}$ into a Kripke category, by defining a strong monoidal functor by $F(A) \stackrel{\text{def}}{=} \mathbf{1}$. This should prime us towards the following fact: 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. Gentry (2010)). Indeed, the term $\mathsf{ax_K}$ that is the proof-relevant version of axiom K can be understood as the server-side routine that applies an *encrypted* function to an *encrypted* datum. Previous work of this sort has appeared before: e.g. Mitchell et al. Mitchell et al. (2012) embed domain-specific λ-calculus for structuring homomorphically encrypted computation in Haskell. But their results to be based on monads, and hence the monadic metalanguage (Moggi, 1991), whose modality satisfies $(A \to B) \to (TA \to TB)$ A term of this type intuitively allows the server to apply any function $A \to B$ to an encrypted datum of type TA, to obtain an encrypted datum of type TB. Arguably, the server should not be allowed to do that, unless the client has encrypted the function to obtain a term of type $T(A \to B)$ beforehand. This is a requirement that our calculus already enforces.

Bibliography

Abadi, M., Banerjee, A., Heintze, N., and Riecke, J. G. (1999). A core calculus of dependency. In *Proceedings of the 26th ACM SIGPLAN-SIGACT symposium on Principles of programming languages - POPL '99*, pages 147–160, New York, New York, USA. ACM Press.

Abramsky, S. and Tzevelekos, N. (2011). Introduction to Categories and Categorical Logic. In Coecke, B., editor, *New Structures for Physics*, pages 3–94. Springer-Verlag.

Andreoli, J.-M. (1992). Logic Programming with Focusing Proofs in Linear Logic. *Journal of Logic and Computation*, 2(3):297–347.

Barber, A. G. (1996). Dual Intuitionistic Linear Logic. Technical report, ECS-LFCS-96-347, Laboratory for Foundations of Computer Science, University of Edinburgh.

Barendregt, H. (1984). *Lambda Calculus: Its Syntax and Semantics*. North-Holland, Amsterdam.

Bellin, G. (1985). A system of natural deduction for GL. *Theoria*, 51(2):89–114.

Bellin, G., de Paiva, V., and Ritter, E. (2001). Extended Curry-Howard correspondence for a basic constructive modal logic. In *Proceedings of Methods for Modalities*.

Benton, N., Bierman, G., de Paiva, V., and Hyland, M. (1993). A term calculus for Intuitionistic Linear Logic. In *Typed Lambda Calculi and Applications, International Conference on Typed Lambda Calculi and Applications, TLCA '93, Utrecht, The Netherlands, March 16-18, 1993, Proceedings*, pages 75–90.

Bierman, G. M. and de Paiva, V. (1992). Intuitionistic Necessity Revisited. In *Proceedings of the Logic at Work Conference, Amsterdam, Holland.*

Bierman, G. M. and de Paiva, V. (1996). Intuitionistic Necessity Revisited. Technical report, University of Birmingham.

Bierman, G. M. and de Paiva, V. (2000). On an Intuitionistic Modal Logic. *Studia Logica*, 65(3):383–416.

Boolos, G. S. (1994). *The Logic of Provability*. Cambridge University Press, Cambridge.

Crole, R. L. (1993). *Categories for Types*. Cambridge University Press.

Čubrić, D., Dybjer, P., and Scott, P. J. (1998). Normalization and the Yoneda embedding. *Mathematical Structures in Computer Science*, 8(2):153–192.

Curry, H. B. (1952). The elimination theorem when modality is present. *The Journal of Symbolic Logic*, 17(04):249–265.

Danos, V. and Joinet, J. B. (2003). Linear logic and elementary time. *Information and Computation*, 183(1):123–137.

Davies, R. and Pfenning, F. (1996). A modal analysis of staged computation. In *Proceedings of the 23rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'96)*, pages 258–270.

Davies, R. and Pfenning, F. (2001). A modal analysis of staged computation. *Journal of the ACM*, 48(3):555–604.

de Paiva, V., Goré, R., and Mendler, M. (2004). Editorial: Modalities in Constructive Logics and Type Theories. *Journal of Logic and Computation*, 14(4):439–446.

Gallier, J. (1990). On Girard's "Candidats de Reductibilite". In Odifreddi, P., editor, *Logic and Computer Science*, pages 123–203. Academic Press.

Gallier, J. (1993). Constructive logics Part I: A tutorial on proof systems and typed λ-calculi. *Theoretical Computer Science*, 110(2):249–339.

Gallier, J. (1995). On the Correspondence Between Proofs and Lambda Terms. In de Groote, P., editor, *The Curry-Howard Isomorphism*, pages 55–138. Academia, Louvain-la-Neuve.

Gentry, C. (2010). Computing arbitrary functions of encrypted data. *Communications of the ACM*, 53(3):97.

Gentzen, G. (1935a). Untersuchungen über das logische Schließen. I. *Mathematische Zeitschrift*, 39(1):176–210.

Gentzen, G. (1935b). Untersuchungen über das logische Schließen. II. *Mathematische Zeitschrift*, 39(1):405–431.

Girard, J.-Y. (1972). *Interprétation fonctionelle et élimination des coupures de l'arithmétique d'ordre supérieur*. PhD thesis, Université Paris VII.

Girard, J.-Y. (1993). On the unity of logic. *Annals of Pure and Applied Logic*, 59(3):201–217.

Girard, J.-Y., Lafont, Y., and Taylor, P. (1989). *Proofs and Types*. Cambridge University Press.

Goré, R. and Ramanayke, R. (2012). Valentini's Cut-Elimination for Provability Logic Resolved. *The Review of Symbolic Logic*, 5(02):212–238.

Goubault-Larrecq, J. (1996). On Computational Interpretations of the Modal Logic S4 - I. Cut Elimination. Technical report, 1996-35. Institut für Logik, Komplexität und Deduktionssysteme, Universität Karlsruhe.

Hakli, R. and Negri, S. (2012). Does the deduction theorem fail for modal logic? *Synthese*, 187(3):849–867.

Howard, W. A. (1980). The formulae-as-types notion of construction. In Seldin, J. P. and Hindley, J. R., editors, *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, pages 479–490. Academic Press, Boston, MA.

Kakutani, Y. (2007). Call-by-Name and Call-by-Value in Normal Modal Logic. In Shao, Z., editor, *Programming Languages and Systems (5th Asian Symposium, APLAS 2007, Singapore, November 28-December 1, 2007, Proceedings)*, pages 399–414, Berlin, Heidelberg. Springer Berlin Heidelberg.

Kavvos, G. A. (2016). The Many Worlds of Modal λ-calculi: I. Curry-Howard for Necessity, Possibility and Time. *CoRR*.

Koletsos, G. (1985). Church-Rosser theorem for typed functional systems. *The Journal of Symbolic Logic*, 50(03):782–790.

Kripke, S. A. (1963). Semantical Analysis of Modal Logic I. Normal Modal Propositional Calculi. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 9(5-6):67–96.

Lambek, J. and Scott, P. J. (1988). *Introduction to Higher-Order Categorical Logic*. Cambridge University Press.

Leivant, D. (1981). On the proof theory of the modal logic for arithmetic provability. *The Journal of Symbolic Logic*, 46(03):531–538.

Mac Lane, S. (1978). *Categories for the Working Mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer New York, New York, NY.

Melliès, P.-A. (2009). Categorical Semantics of Linear Logic. In Curien, P.-L., Herbelin, H., Krivine, J.-L., and Melliès, P.-A., editors, *Panoramas et synthèses 27: Interactive models of computation and program behaviour*. Société Mathématique de France.

Mitchell, J. C. (1996). *Foundations for programming languages*. Foundations of Computing. The MIT Press.

Mitchell, J. C., Sharma, R., Stefan, D., and Zimmerman, J. (2012). Information-flow control for programming on encrypted data. *Proceedings of the Computer Security Foundations Workshop*, pages 45–60.

Moggi, E. (1991). Notions of computation and monads. *Information and Computation*, 93(1):55–92.

Murphy, T., Crary, K., Harper, R., and Pfenning, F. (2004). A symmetric modal lambda calculus for distributed computing. In *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science, 2004.*, pages 286–295. IEEE.

Negri, S. (2011). Proof Theory for Modal Logic. *Philosophy Compass*, 6(8):523–538.

Newman, M. H. A. (1942). On Theories with a Combinatorial Definition of "Equivalence". *The Annals of Mathematics*, 43(2):223.

Nielson, F. and Nielson, H. R. (1992). *Two-Level Functional Languages*. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press.

Ohnisi, M. and Matsumoto, K. (1957). Gentzen method in modal calculi. *Osaka Journal of Mathematics*, 11(2):113–130.

Ohnisi, M. and Matsumoto, K. (1959). Gentzen method in modal calculi. II. *Osaka Journal of Mathematics*, 11(2):115–120.

Ohta, Y. and Hasegawa, M. (2006). A Terminating and Confluent Linear Lambda Calculus. In *Lecture Notes in Computer Science*, volume 4098, pages 166–180.

Ono, H. (1998). Proof-theoretic methods in nonclassical logic–an introduction. In Takahashi, M., Okada, M., and Dezani-Ciancaglini, M., editors, *Theories of Types and Proofs*, MSJ Memoirs, pages 207–254. The Mathematical Society of Japan, Tokyo.

Pfenning, F. (2001). Intensionality, extensionality, and proof irrelevance in modal type theory. *Proceedings of the 16th Annual IEEE Symposium on Logic in Computer Science (LICS 2001)*.

Pfenning, F. (2015). Decomposing Modalities.

Pfenning, F. and Davies, R. (2001). A judgmental reconstruction of modal logic. *Mathematical Structures in Computer Science*, 11(4):511–540.

Plotkin, G. D. (1993). Type theory and recursion. In *Proceedings Eighth Annual IEEE Symposium on Logic in Computer Science*, page 374. IEEE Comput. Soc. Press.

Prawitz, D. (1965). *Natural Deduction: a proof-theoretical study.* Almquist and Wiksell.

Sambin, G. and Valentini, S. (1980). A modal sequent calculus for a fragment of arithmetic. *Studia Logica*, 39(2-3):245–256.

Sambin, G. and Valentini, S. (1982). The modal logic of provability. The sequential approach. *Journal of Philosophical Logic*, 11(3):311–342.

Schroeder-Heister, P. (1984). A natural extension of natural deduction. *The Journal of Symbolic Logic*, 49(04):1284–1300.

Simpson, A. K. (1994). *The Proof Theory and Semantics of Intuitionistic Modal Logic*. PhD thesis, The University of Edinburgh.

Sørensen, M. H. and Urzyczyn, P. (2006). *Lectures on the Curry-Howard Isomorphism*. Elsevier.

Taha, W. and Sheard, T. (2000). MetaML and multi-stage programming with explicit annotations. *Theoretical Computer Science*, 248(1-2):211–242.

Takahashi, M. (1995). Parallel Reductions in λ-Calculus. *Information and Computation*, 118(1):120–127.

Terese (2003). *Term Rewriting Systems*. Cambridge University Press.

Tsukada, T. and Igarashi, A. (2010). A logical foundation for environment classifiers. *Logical Methods in Computer Science*, 6(4):1–43.

Valentini, S. (1982). Cut-elimination in a modal sequent calculus for K. *Bolletino dell'Unione Mathematica Italiana*, 1B:119–130.

Valentini, S. (1983). The Modal Logic of Provability: Cut-Elimination. *Journal of Philosophical Logic*, 12(4):471–476.

Wadler, P. (1993). 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*, volume 711 of *LNCS*, pages 185–210.

Wadler, P. (1994). A syntax for linear logic. In Brookes, S., Main, M., Melton, A., Mislove, M., and Schmidt, D., editors, *Mathematical Foundations of Programming Semantics: 9th International Conference, New Orleans, LA, USA, April 7 - 10, 1993. Proceedings*, pages 513–529. Springer-Verlag Berlin Heidelberg.

Wansing, H. (2002). Sequent Systems for Modal Logics. In *Handbook of Philosophical Logic*, pages 61–145. Springer Netherlands, Dordrecht.

Wijesekera, D. (1990). Constructive modal logics I. *Annals of Pure and Applied Logic*, 50(3):271–301.