Under consideration for publication in Math. Struct. in Comp. Science

A Judgmental Reconstruction of Modal Logic

FRANK PFENNING[†] and ROWAN DAVIES

Department of Computer Science

Carnegie Mellon University

Received May 2000

We reconsider the foundations of modal logic, following Martin-Löf's methodology of distinguishing judgments from propositions. We give constructive meaning explanations for necessity and possibility which yields a simple and uniform system of natural deduction for intuitionistic modal logic which does not exhibit anomalies found in other proposals. We also give a new presentation of lax logic and find that the lax modality is already expressible using possibility and necessity. Through a computational interpretation of proofs in modal logic we further obtain a new formulation of Moggi's monadic metalanguage.

Contents

[†] This work was partly supported by the National Science Foundation under grant CCR-9619832.

1. Introduction

In this paper we reconsider the foundations of modal logic, following Martin-Löf's (1996) methodology of distinguishing judgments from propositions. We give constructive meaning explanations for necessity ($\Box$) and possibility ($\Diamond$). This exercise yields a simple and uniform system of natural deduction for intuitionistic modal logic which does not exhibit anomalies found in other proposals. We also give a new presentation of lax logic (Fairtlough and Mendler, 1997) and find that it is already contained in modal logic, using the decomposition of the lax modality $\bigcirc A$ as $\Diamond\Box A$ and lax implication $A \Rightarrow B$ as $(\Box A) \supset B$. Through a computational interpretation of proofs in modal logic we further obtain a new formulation of Moggi's monadic metalanguage (Moggi, 1998; 1989; 1991), combining and systematizing previous work by S. Kobayashi (1997) and Benton, Bierman, and de Paiva (1998).

At the level of judgments, the above development requires surprisingly few primitive notions. In particular, we only need hypothetical judgments to explain implication, and categorical judgments to explain the modalities. We have thus obtained a satisfactory foundation for the constructive understanding of modal logic and its computational interpretations.

2. Judgments and Propositions

In his Siena lectures from 1983 (finally published in 1996), Martin-Löf provides a foundation for logic based on a clear separation of the notions of judgment and proposition. He reasons that to judge is to know and that an evident judgment is an object of knowledge. A proof is what makes a judgment evident. In logic, we make particular judgments such as "*A is a proposition*" or "*A is true*", presupposing in the latter case that A is already known to be a proposition. To know that "*A is a proposition*" means to know what counts as a verification of A, whereas to know that "*A is true*" means to know how to verify A. In his words (Martin-Löf, 1996, Page 27):

> *The meaning of a proposition is determined by [...] what counts as a verification of it.*

This approach leads to a clear conceptual priority: we first need to understand the notions of judgment and evidence for judgments, then the notions of proposition and verifications of propositions to understand truth.

As an example, we consider the explanation of conjunction. We know that $A \wedge B$ is a proposition if both A and B are propositions. As a rule of inference (called conjunction formation):

$$\frac{A\ prop \qquad B\ prop}{A \wedge B\ prop}\wedge F$$

The meaning is given by stating what counts a verification of $A \wedge B$. We say that we have a verification of $A \wedge B$ if we have verifications for both A and B. As a rule of inference:

$$\frac{A\ \mathit{true} \qquad B\ \mathit{true}}{A \wedge B\ \mathit{true}} \wedge I$$

where we presuppose that A and B are already known to be propositions. This is known as an *introduction rule*, a term due to Gentzen (1935) who first formulated a system of natural deduction. Conversely, what do we know if we know that $A \wedge B$ is true? Since a verification of $A \wedge B$ consists of verifications for both A and B, we know that A must be true and B must be true. Formulated as rules of inference (called conjunction eliminations):

$$\frac{A \wedge B\ \mathit{true}}{A\ \mathit{true}} \wedge E_L \qquad \frac{A \wedge B\ \mathit{true}}{B\ \mathit{true}} \wedge E_R$$

From the explanation above it should be clear that the two elimination rules are *sound*: if we define the meaning of conjunction by its introduction rule then we are fully justified in concluding that A is true if $A \wedge B$ is true, and similarly for the second rule.

Soundness guarantees that the elimination rules are not too strong. We have sufficient evidence for the judgment in the conclusion if we have sufficient evidence for the judgment in the premise. This is witnessed by a *local reduction* which constructs evidence for the conclusion from evidence for the premise.

$$\frac{\dfrac{\begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array} \qquad \begin{array}{c}\mathcal{E}\\ B\ \mathit{true}\end{array}}{A \wedge B\ \mathit{true}} \wedge I}{A\ \mathit{true}} \wedge E_L \quad \Longrightarrow_R \quad \begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array}$$

A symmetric reduction exists for $\wedge E_R$. We only consider each elimination immediately preceded by an introduction for a connective. We therefore call the property that each such pattern can be reduced *local soundness*.

The dual question, namely if the elimination rules are sufficiently strong, has, as far as we know, not been discussed by Martin-Löf. Of course, we can never achieve "absolute" completeness of rules for inferring evident judgments. But in some situations, elimination rules may be obviously incomplete. For example, we might have overlooked the second elimination rule for conjunction, $\wedge E_R$. This would not contradict soundness, but we would not be able to exploit the knowledge that $A \wedge B$ is true to its fullest. In particular, we cannot recover the knowledge that B is true even if we know that $A \wedge B$ is true.

In general we say that the elimination rules for a connective are *locally complete* if we can apply the elimination rules to a judgment to recover enough knowledge to permit reconstruction of the original judgment. In the case of conjunction, this is only possible if we have both elimination rules.

$$\begin{array}{c} \mathcal{D} \\ A \wedge B \; \mathit{true} \end{array} \Longrightarrow_E \frac{\dfrac{\begin{array}{c}\mathcal{D} \\ A \wedge B \; \mathit{true}\end{array}}{A \; \mathit{true}} \wedge E_L \quad \dfrac{\begin{array}{c}\mathcal{D} \\ A \wedge B \; \mathit{true}\end{array}}{B \; \mathit{true}} \wedge E_R}{A \wedge B \; \mathit{true}} \wedge I$$

We call this pattern a *local expansion* since we obtain more complex evidence for the original judgment.

An alternative way to understand local completeness is to reconsider our meaning explanation of conjunction. We have said that a verification of $A \wedge B$ consists of a verification of A and a verification of B. Local completeness entails that it is always possible to bring the verification of $A \wedge B$ into this form by a local expansion.

To summarize, logic is based on the notion of judgment where an evident judgment is an object of knowledge. A judgment can be immediately evident or, more typically, mediately evident, in which case the evidence is provided by a proof. The meaning of a proposition is given by what counts as a verification of it. This is written out in the form of introduction rules for logical connectives which allow us to conclude when propositions are true. They are complemented by elimination rules which allow us to obtain further knowledge from the knowledge of compound propositions. The elimination rules for a connective should be locally sound and complete in order to have a satisfactory meaning explanation for the connective. Local soundness and completeness are witnessed by local reductions and expansions of proofs, respectively.

Note that there are other ways to define meaning. For example, we frequently expand our language by *notational definition*. In intuitionistic logic negation is often given as a derived concept, where $\neg A$ is considered a notation for $A \supset \bot$. This means that negation has a rather weak status, as its meaning relies entirely on the meaning of implication and falsehood rather than having an independent explanation. The two should not be mixed: introduction and elimination rules for a connective should rely solely on judgmental concepts and not on other connectives. Sometimes (as in the case of negation) a connective can be explained directly or as a notational definition and we can establish that the two meanings coincide.

3. Hypothetical Judgments and Implication

So far we have seen two forms of judgment: "*A is a proposition*" and "*A is true*". These are insufficient to explain implication, since we would like to say that $A \supset B$ is true if B is true whenever A is true. For this we need hypothetical judgments and hypothetical proofs, which are new primitive notions. We simplify the account of hypothetical judgments by Martin-Löf by presupposing that subjects A and B are known to be propositions without making this explicit.

We write the general form of a hypothetical judgment as

$$J_1, \ldots, J_n \vdash J$$

which expresses "*J assuming J_1 through J_n*" or "*J under hypotheses J_1 through J_n*".

We also refer to $J_1, \ldots, J_n$ as the *antecedents* and J as the *succedent* of the hypothetical judgment.

We explain the meaning by explaining what constitutes evidence for such a hypothetical judgment, namely a hypothetical proof. In a hypothetical proof of the judgment above we can use the hypotheses J_i as if we knew them. We can consequently substitute an arbitrary derivation of J_i for the uses of a hypothesis J_i to obtain a judgment which no longer depends on J_i. Thus, at the core, the meaning of hypothetical judgments relies upon substitution on the level of proofs, that is, supplanting the use of a hypothesis by evidence for it.

The first particular form of hypothetical judgment we need here is

$$A_1 \ \mathit{true}, \ldots, A_n \ \mathit{true} \vdash A \ \mathit{true}$$

where we presuppose that A_1 through A_n and A are all propositions. We write Γ for a collection of hypotheses of the form above. The special case of the substitution principle for such hypotheses has the form

Substitution Principle for Truth
If $\Gamma \vdash A \ \mathit{true}$ and $\Gamma, A \ \mathit{true} \vdash J$ then $\Gamma \vdash J$.

In particular, we will be interested in the cases where the judgment J is $C \ \mathit{true}$ or a hypothetical judgment $\Gamma' \vdash C \ \mathit{true}$. In the latter case, iterated hypothetical judgments are combined and the substitution principle postulates that if $\Gamma \vdash A \ \mathit{true}$ and $\Gamma, A \ \mathit{true}, \Gamma' \vdash C \ \mathit{true}$ then $\Gamma, \Gamma' \vdash C \ \mathit{true}$. We further have the general rule for the use of hypotheses.

$$\frac{}{\Gamma, A \ \mathit{true}, \Gamma' \vdash A \ \mathit{true}} \ \mathit{hyp}$$

We emphasize that the substitution principle should not be viewed as an inference rule, but a property defining hypothetical judgments which we use in the design of a formal system. Therefore it should hold for any system of connectives and inference rules we devise. The correctness of the hypothesis rule, for example, can be seen from the substitution principle by adjoining unused hypotheses to the first derivation. In this paper we will not discuss the details of structural properties of collections of hypotheses such as weakening, exchange, or contraction.

Now we can explain the meaning of implication at the level of propositions. First, the formation rule:

$$\frac{A \ \mathit{prop} \qquad B \ \mathit{prop}}{A \supset B \ \mathit{prop}} \supset\! F$$

We follow the usual convention that implication associates to the right, so $A \supset B \supset C$ stands for $A \supset (B \supset C)$. The meaning of $A \supset B$ is given by what counts as a verification of it. We say that $A \supset B$ is true if B is true under hypothesis A.

$$\frac{\Gamma, A \ \mathit{true} \vdash B \ \mathit{true}}{\Gamma \vdash A \supset B \ \mathit{true}} \supset\! I$$

If we know that $A \supset B$ is true we know that B is true under assumption A. If we have evidence for the truth of A we can discharge this assumption and obtain evidence for the truth of B.

$$\dfrac{\Gamma \vdash A \supset B\ \mathit{true} \qquad \Gamma \vdash A\ \mathit{true}}{\Gamma \vdash B\ \mathit{true}}\,{\supset}E$$

This elimination rule is locally sound and complete. Local soundness can be seen from the local reduction

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ \Gamma, A\ \mathit{true} \vdash B\ \mathit{true}\end{array}}{\Gamma \vdash A \supset B\ \mathit{true}}\,{\supset}I \qquad \begin{array}{c}\mathcal{E}\\ \Gamma \vdash A\ \mathit{true}\end{array}}{\Gamma \vdash B\ \mathit{true}}\,{\supset}E \quad \Longrightarrow_R \quad \begin{array}{c}\mathcal{D}'\\ \Gamma \vdash B\ \mathit{true}\end{array}$$

where $\mathcal{D}'$ is constructed from $\mathcal{D}$ by substituting $\mathcal{E}$ for uses of the hypothesis A *true*. This takes advantage of the meaning of hypothetical proofs which rests on the substitution principle.[†]

Local completeness can be seen from the local expansion

$$\begin{array}{c}\mathcal{D}\\ \Gamma \vdash A \supset B\ \mathit{true}\end{array} \quad \Longrightarrow_E \quad \dfrac{\dfrac{\begin{array}{c}\mathcal{D}'\\ \Gamma, A\ \mathit{true} \vdash A \supset B\ \mathit{true}\end{array} \qquad \dfrac{}{\Gamma, A\ \mathit{true} \vdash A\ \mathit{true}}\,\mathit{hyp}}{\Gamma, A\ \mathit{true} \vdash B\ \mathit{true}}\,{\supset}E}{\Gamma \vdash A \supset B\ \mathit{true}}\,{\supset}I$$

where $\mathcal{D}'$ is constructed from $\mathcal{D}$ by adjoining the unused hypothesis A *true* to every judgment.

3.1. *Axiomatic Characterization*

For the sake of completeness, we recall the axiomatic characterization of implication by means of Modus Ponens

$$\dfrac{\vdash A \supset B\ \mathit{true} \qquad \vdash A\ \mathit{true}}{\vdash B\ \mathit{true}}\,\mathit{mp}$$

and the axiom schemas S and K.

$$\begin{array}{l}\vdash (A \supset B \supset C) \supset (A \supset B) \supset A \supset C\ \mathit{true}\\ \vdash A \supset B \supset A\ \mathit{true}\end{array}$$

Deductions of these axioms in the form of proof terms can be found in Section 6.

4. Categorical Judgments and Validity

Now that we have introduced hypothetical judgments, we can single out *categorical judgments*, a term which goes back to Kant. In our situation they are judgments which do not

[†] There is a small ambiguity here which arises since we may not be able to identify particular uses of hypotheses if there are several identical hypotheses. This will be resolved through the introduction of proof terms in Section 6.

depend on hypotheses about the truth of propositions. We introduce the new judgment that A is valid (written A *valid*), presupposing that A is a proposition. Evidence for the validity of A is simply unconditional evidence for A. We use "$\cdot$" to indicate an empty collection of hypotheses.

Definition of Validity

1 If $\cdot \vdash A$ *true* then A *valid*.
2 If A *valid* then $\Gamma \vdash A$ *true*.

We allow Γ as hypotheses of the form A_i *true* in part (2) in order to avoid explicit structural rules such as weakening.

Validity is a judgment on propositions whose meaning has already been explained via the notion of truth. Therefore this new judgment form is not particularly interesting unless we take the next step to allow hypotheses of the form A *valid*. Since order is irrelevant, we separate hypotheses about truth and validity and consider the hypothetical judgment

$$B_1\ \textit{valid}, \ldots, B_m\ \textit{valid}; A_1\ \textit{true}, \ldots, A_n\ \textit{true} \vdash A\ \textit{true}.$$

We use the semi-colon for visual clarity, and write Δ for a collection of validity assumptions. In the rules, we restrict ourselves to proving judgments of the form A *true* (rather than A *valid*), which is possible since the latter is directly defined in terms of the former. The meaning of hypothetical judgments yields the general substitution principle:

If $\Delta \vdash B$ *valid* and Δ, B *valid* $\vdash J$ then $\Delta \vdash J$.

Rewriting the first part in terms of truth, and making additional assumptions on truth explicit rather than absorbing them into J, we obtain the following version used in the remainder of this paper.

Substitution Principle for Validity
If $\Delta; \cdot \vdash B$ *true* and Δ, B *valid*; $\Gamma \vdash J$ then $\Delta; \Gamma \vdash J$.

We also have a generalized hypothesis rule, again expressed in a form which establishes truth rather than validity, which can be justified from the definition of validity.

$$\frac{}{\Delta, B\ \textit{valid}, \Delta'; \Gamma \vdash B\ \textit{true}}\ \textit{hyp}^*$$

It is sound, since evidence for the validity of B consists of a proof of B *true* from no assumptions about truth, to which we can adjoin the hypotheses Δ' and Γ.

The next step is to internalize the categorical judgment as a proposition. We write $\Box A$ for the proposition expressing that A is valid.

$$\frac{A\ \textit{prop}}{\Box A\ \textit{prop}}\ \Box F$$

We follow the convention that $\Box$ binds more tightly than $\supset$, so that $\Box A \supset B$ stands for $(\Box A) \supset B$. The introduction rule just allows the step from the validity of A to the truth of $\Box A$, according to the definition of validity.

$$\frac{\Delta; \cdot \vdash A\ \textit{true}}{\Delta; \Gamma \vdash \Box A\ \textit{true}}\ \Box I$$

The elimination rule is considerably more difficult to construct. Clearly, the rule

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

is unsound, since the hypotheses Γ in the premise are unjustified. We can construct a sound elimination rule such as

$$\frac{\Delta; \Gamma \vdash \Box A\ \mathit{true}}{\Delta; \Gamma \vdash A\ \mathit{true}}$$

but this is too weak, that is, not locally complete. There is no local expansion since after the only possible elimination

$$\begin{array}{c} \mathcal{D} \\ \Delta; \Gamma \vdash \Box A\ \mathit{true} \end{array} \overset{?}{\Longrightarrow}_E \frac{\begin{array}{c} \mathcal{D} \\ \Delta; \Gamma \vdash \Box A\ \mathit{true} \end{array}}{\Delta; \Gamma \vdash A\ \mathit{true}}$$

we cannot prove $\Delta; \Gamma \vdash \Box A\ \mathit{true}$ from the conclusion. An elimination rule which is locally sound and complete follows the pattern of the usual rules for disjunction or existential quantification: the knowledge that $\Box A$ is true licenses us to *assume* that A is valid.

$$\frac{\Delta; \Gamma \vdash \Box A\ \mathit{true} \qquad \Delta, A\ \mathit{valid}; \Gamma \vdash C\ \mathit{true}}{\Delta; \Gamma \vdash C\ \mathit{true}}\ \Box E$$

Local soundness of this rule is easily verified by the following local reduction.

$$\frac{\dfrac{\begin{array}{c} \mathcal{D} \\ \Delta; \cdot \vdash A\ \mathit{true} \end{array}}{\Delta; \cdot \vdash \Box A\ \mathit{true}}\ \Box I \qquad \begin{array}{c} \mathcal{E} \\ \Delta, A\ \mathit{valid}; \Gamma \vdash C\ \mathit{true} \end{array}}{\Delta; \Gamma \vdash C\ \mathit{true}}\ \Box E \quad \Longrightarrow_R \quad \begin{array}{c} \mathcal{E}' \\ \Delta; \Gamma \vdash C\ \mathit{true} \end{array}$$

where $\mathcal{E}'$ is constructed from $\mathcal{E}$ by substitution of $\mathcal{D}$ for uses of the hypothesis that A is valid, following the derived substitution principle for validity.

Local completeness is also a simple property.

$$\begin{array}{c} \mathcal{D} \\ \Delta; \Gamma \vdash \Box A\ \mathit{true} \end{array} \Longrightarrow_E \frac{\begin{array}{c} \mathcal{D} \\ \Delta; \Gamma \vdash \Box A\ \mathit{true} \end{array} \qquad \dfrac{\overline{\Delta, A\ \mathit{valid}; \cdot \vdash A\ \mathit{true}}\ \mathit{hyp}^*}{\Delta, A\ \mathit{valid}; \Gamma \vdash \Box A\ \mathit{true}}\ \Box I}{\Delta; \Gamma \vdash \Box A\ \mathit{true}}\ \Box E$$

This concludes the treatment of validity and propositions of the form $\Box A$. In order to discuss the computational interpretations of $\Box A$, we reexamine the rules with a proof term assignment in Section 6.

4.1. *Summary of Formal System*

Since a number of applications of modal logic require only necessity, we summarize the formal system developed up to this point. We allow atomic propositions P without additional properties.

$$\begin{array}{lrcl} \text{Propositions} & A & ::= & P \mid A_1 \supset A_2 \mid \Box A \\ \text{True Hypotheses} & \Gamma & ::= & \cdot \mid \Gamma, A\ \mathit{true} \\ \text{Valid Hypotheses} & \Delta & ::= & \cdot \mid \Delta, A\ \mathit{valid} \end{array}$$

The basic judgments A *true* and A *valid* are combined in a hypothetical judgment

$$\Delta; \Gamma \vdash A\ \mathit{true}$$

subject to the inference rules below.

$$\frac{}{\Delta; \Gamma, A\ \mathit{true}, \Gamma' \vdash A\ \mathit{true}}\ \mathit{hyp}$$

$$\frac{\Delta; \Gamma, A\ \mathit{true} \vdash B\ \mathit{true}}{\Delta; \Gamma \vdash A \supset B\ \mathit{true}} \supset\! I \qquad \frac{\Delta; \Gamma \vdash A \supset B\ \mathit{true} \qquad \Delta; \Gamma \vdash A\ \mathit{true}}{\Delta; \Gamma \vdash B\ \mathit{true}} \supset\! E$$

$$\frac{}{\Delta, B\ \mathit{valid}, \Delta'; \Gamma \vdash B\ \mathit{true}}\ \mathit{hyp}^*$$

$$\frac{\Delta; \cdot \vdash A\ \mathit{true}}{\Delta; \Gamma \vdash \Box A\ \mathit{true}} \Box I \qquad \frac{\Delta; \Gamma \vdash \Box A\ \mathit{true} \qquad \Delta, A\ \mathit{valid}; \Gamma \vdash C\ \mathit{true}}{\Delta; \Gamma \vdash C\ \mathit{true}} \Box E$$

This inference system satisfies the usual structural laws of exchange, weakening, and contraction, both for true and valid hypotheses. This can be shown trivially by structural induction. The guiding substitution principle can be expressed as a property of this formal system and also proven by induction over the structure of derivations.

Theorem 1 (Substitution).
The inference system for modal logic with implication and necessity satisfies:

1 If $\Delta; \Gamma, A\ \mathit{true}, \Gamma' \vdash C\ \mathit{true}$ and $\Delta; \Gamma \vdash A\ \mathit{true}$ then $\Delta; \Gamma, \Gamma' \vdash C\ \mathit{true}$.
2 If $\Delta, B\ \mathit{valid}, \Delta'; \Gamma \vdash C\ \mathit{true}$ and $\Delta; \cdot \vdash A\ \mathit{true}$ then $\Delta, \Delta'; \Gamma \vdash C\ \mathit{true}$.

Proof. In each case by straightforward induction over the structure of the first given derivation, using weakening where necessary. □

4.2. *Alternative Formulations*

We conclude this section with some remarks on two of Prawitz's formulations of natural deduction for modal logic (Prawitz, 1965, Chapter VI). His first formulation, in our notation, allows contexts of the form $\Box A_1\ \mathit{true}, \ldots, \Box A_n\ \mathit{true}$ which we write as $\Box\Gamma$.

$$\frac{\Box\Gamma \vdash A\ \mathit{true}}{\Box\Gamma, \Gamma' \vdash \Box A\ \mathit{true}} \Box I_1 \qquad \frac{\Gamma \vdash \Box A\ \mathit{true}}{\Gamma \vdash A\ \mathit{true}} \Box E_1$$

This pair of rules is locally sound, but not complete. Moreover, it violates the interpretation of $\Gamma \vdash A\ \mathit{true}$ as a hypothetical judgment, since

$$\dfrac{\dfrac{}{P, P \supset \Box Q \vdash P \supset \Box Q}\,\mathit{hyp} \qquad \dfrac{}{P, P \supset \Box Q \vdash P}\,\mathit{hyp}}{P, P \supset \Box Q \vdash \Box Q}\supset\!E$$

and

$$\dfrac{\dfrac{}{\Box Q \vdash \Box Q}\,\mathit{hyp}}{\Box Q \vdash \Box\Box Q}\,\Box I_1$$

but after substitution of the first derivation for uses of $\Box Q$ in the second we obtain an invalid derivation:

$$\dfrac{\dfrac{\dfrac{}{P, P \supset \Box Q \vdash P \supset \Box Q}\,\mathit{hyp} \qquad \dfrac{}{P, P \supset \Box Q \vdash P}\,\mathit{hyp}}{P, P \supset \Box Q \vdash \Box Q}\supset\!E}{P, P \supset \Box Q \vdash \Box\Box Q}\,\Box I_1?$$

A related lack of normal forms was noted by Prawitz himself and he introduced two further systems. The third system is related to the one by Bierman and de Paiva (1996) in which the introduction rule has the form

$$\dfrac{\Gamma \vdash \Box A_1\ \mathit{true} \quad \ldots \quad \Gamma \vdash \Box A_n\ \mathit{true} \qquad \Box A_1\ \mathit{true}, \ldots, \Box A_n\ \mathit{true} \vdash A\ \mathit{true}}{\Gamma \vdash \Box A\ \mathit{true}}\,\Box I_2$$

Prawitz writes this rule as

$$\dfrac{\Gamma \vdash A\ \mathit{true}}{\Gamma \vdash \Box A\ \mathit{true}}\,\Box I_3$$

with a side condition enforcing that the derivation of the premise can be decomposed as in Bierman and de Paiva's formulation.

The failure of the substitution property in the first formulation can be traced to the restriction of the introduction rule to assumptions of the form $\Box A_i\ \mathit{true}$ when it should be $A_i\ \mathit{valid}$. The revised version is still less than satisfactory since it requires a simultaneous substitution, either in the syntax or in the side condition.

4.3. *Axiomatic Characterization*

Necessity can be characterized axiomatically by the inference rule of necessitation

$$\dfrac{\vdash A\ \mathit{true}}{\vdash \Box A\ \mathit{true}}\,\mathit{nec}$$

together with the following three axioms (see, for example, (Viganò, 1997; Kobayashi, 1997; Alechina et al., 1998)):

$$\begin{array}{l} \vdash \Box(A \supset B) \supset (\Box A \supset \Box B)\ \mathit{true} \\ \vdash \Box A \supset A\ \mathit{true} \\ \vdash \Box A \supset \Box\Box A\ \mathit{true} \end{array}$$

The derivations of these axioms in natural deduction is given in Section 6 in abbreviated form as proof terms.

5. Possibility

We may view hypotheses A_1 *true*, $\ldots$, A_n *true* as describing knowledge of a given *world*. The judgment that A is valid can then be interpreted as expressing that A is true in a world about which we know nothing. In other words, A is *necessarily true*. Note that by verifying the truth of A without presupposing any knowledge, we can speak of necessary truth without circumscribing the totality of all conceivable worlds. The reasoning remains purely logical.

A dual concept is that of *possible truth*. We say that A is *possibly true* if there is a world in which A is true. Unlike in classical logic, we have no reason to expect that possible truth would be definable propositionally in terms of necessary truth. It also appears difficult to analyze this concept judgmentally without reference to the existence of particular worlds. And yet it is possible to do so by employing a combination of hypothetical and categorical judgments. The critical insight for necessity came from considering how to establish that A is valid. Here we take the opposite approach and consider how to use the knowledge that A is possibly true. It means that there is a world in which A is true, but about which we know nothing else. Therefore, if we assume that A is true (but nothing else) and then conclude that C is possible, then C must be possible. If we write A *poss* for the judgment that A is possible we obtain:

If A *poss* and A *true* $\vdash C$ *poss* then C *poss*.

Note that we can only draw conclusions regarding the possibility of C, but not its truth. In the end, the only way we can establish that A is possible is to show that A is true.

If A *true* then A *poss*.

This reasoning may use hypotheses, so in the definition we write out the corresponding principles in a more explicit form.

Definition of Possibility

1 If $\Gamma \vdash A$ *true* then $\Gamma \vdash A$ *poss*.
2 If $\Gamma \vdash A$ *poss* and A *true* $\vdash C$ *poss* then $\Gamma \vdash C$ *poss*.

We are interested in considering both necessity and possibility together. They interact because they are both concerned with truth, relativized to worlds. If we decide that they both should refer to the same worlds, then the definition of possible truth is extended by allowing assumptions about validity.

Definition of Possibility with Necessity

1 If $\Delta; \Gamma \vdash A$ *true* then $\Delta; \Gamma \vdash A$ *poss*.
2 If $\Delta; \Gamma \vdash A$ *poss* and $\Delta; A$ *true* $\vdash C$ *poss* then $\Delta; \Gamma \vdash C$ *poss*.

In part (2), the validity assumptions Δ are available for deriving C *poss* from A *true*. This is because they are true in all worlds and therefore, in particular, in the one in which A is assumed to be true. Note that part (2) has the form of a substitution principle and will be used as such. This leads to the non-standard form of substitution introduced in Section 6.

For the consideration of validity we needed to introduce a new form of hypothesis, A *valid*, but no new judgment to be derived. Here, instead, we do *not* need to introduce a new form of antecedent, only a new form of succedent, A *poss*. Next we internalize possibility as a propositional operator $\Diamond$.

$$\frac{A \; prop}{\Diamond A \; prop}\,\Diamond F$$

We use the same syntactic conventions as for $\Box$. The introduction and elimination rules follow the ideas above at the level of judgments.

$$\frac{\Delta; \Gamma \vdash A \; poss}{\Delta; \Gamma \vdash \Diamond A \; true}\,\Diamond I \qquad \frac{\Delta; \Gamma \vdash \Diamond A \; true \qquad \Delta; A \; true \vdash C \; poss}{\Delta; \Gamma \vdash C \; poss}\,\Diamond E$$

Part (1) in the definition of possibility allows us to pass from A *true* to A *poss*. Instead of introducing an explicit inference rule, we make this step silently whenever appropriate in order to avoid excessive syntactic baggage. This is akin to the direct use of an assumption A *valid* to conclude that A *true* in the extended hypothesis rule *hyp**. We similarly decorate the $\Diamond I$ and $\Diamond E$ rules with an asterisk when such a passage occurred in one of its premises.

Local soundness can be seen from the local reduction

$$\frac{\dfrac{\begin{array}{c}\mathcal{D}\\ \Delta; \Gamma \vdash A \; poss\end{array}}{\Delta; \Gamma \vdash \Diamond A \; true}\,\Diamond I \qquad \begin{array}{c}\mathcal{E}\\ \Delta; A \; true \vdash C \; poss\end{array}}{\Delta; \Gamma \vdash C \; poss}\,\Diamond E \quad \Longrightarrow_R \quad \begin{array}{c}\mathcal{E}'\\ \Delta; \Gamma \vdash C \; poss\end{array}$$

where $\mathcal{E}'$ is justified by part (2) in the definition of possibility.

The elimination rule is also locally complete, as witnessed by the following expansion.

$$\begin{array}{c}\mathcal{D}\\ \Delta; \Gamma \vdash \Diamond A \; true\end{array} \quad \Longrightarrow_E \quad \dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ \Delta; \Gamma \vdash \Diamond A \; true\end{array} \qquad \dfrac{}{\Delta; A \; true \vdash A \; true}\,hyp}{\Delta; \Gamma \vdash A \; poss}\,\Diamond E^*}{\Delta; \Gamma \vdash \Diamond A \; true}\,\Diamond I$$

The substitution principle for validity, using the new judgment C *poss* as the succedent J, justifies a new variant of the necessity elimination rule.

$$\frac{\Delta; \Gamma \vdash \Box A \; true \qquad \Delta, A \; valid; \Gamma \vdash C \; poss}{\Delta; \Gamma \vdash C \; poss}\,\Box E_p$$

Without this rule the judgment $\cdot; \Box A \; true, \Diamond(A \supset B) \; true \vdash B \; poss$, while derivable, would not have a derivation satisfying a strict subformula property. We leave the verification of local soundness when $\Box I$ is followed by $\Box E_p$ to the reader. As before, it follows from the appropriate instance of the substitution principle for validity. This concludes our meaning explanation of possibility.

5.1. *Summary of Formal System*

We now summarize the formal system of modal logic with necessity and possibility.

$$\begin{array}{rrcl} \text{Propositions} & A & ::= & P \mid A_1 \supset A_2 \mid \Box A \mid \Diamond A \\ \text{True Hypotheses} & \Gamma & ::= & \cdot \mid \Gamma, A\ \mathit{true} \\ \text{Valid Hypotheses} & \Delta & ::= & \cdot \mid \Delta, A\ \mathit{valid} \end{array}$$

The basic judgments A *true*, A *valid*, and A *poss* are combined in two forms of hypothetical judgment

$$\begin{array}{c} \Delta; \Gamma \vdash A\ \mathit{true} \\ \Delta; \Gamma \vdash A\ \mathit{poss} \end{array}$$

subject to the inclusion of A *true* in A *poss* and the inference rules below.

$$\frac{}{\Delta; \Gamma, A\ \mathit{true}, \Gamma' \vdash A\ \mathit{true}}\ \mathit{hyp}$$

$$\frac{\Delta; \Gamma, A\ \mathit{true} \vdash B\ \mathit{true}}{\Delta; \Gamma \vdash A \supset B\ \mathit{true}} \supset I \qquad \frac{\Delta; \Gamma \vdash A \supset B\ \mathit{true} \qquad \Delta; \Gamma \vdash A\ \mathit{true}}{\Delta; \Gamma \vdash B\ \mathit{true}} \supset E$$

$$\frac{}{\Delta, B\ \mathit{valid}, \Delta'; \Gamma \vdash B\ \mathit{true}}\ \mathit{hyp}^*$$

$$\frac{\Delta; \cdot \vdash A\ \mathit{true}}{\Delta; \Gamma \vdash \Box A\ \mathit{true}} \Box I \qquad \frac{\Delta; \Gamma \vdash \Box A\ \mathit{true} \qquad \Delta, A\ \mathit{valid}; \Gamma \vdash C\ \mathit{true}}{\Delta; \Gamma \vdash C\ \mathit{true}} \Box E$$

$$\frac{\Delta; \Gamma \vdash \Box A\ \mathit{true} \qquad \Delta, A\ \mathit{valid}; \Gamma \vdash C\ \mathit{poss}}{\Delta; \Gamma \vdash C\ \mathit{poss}} \Box E_p$$

$$\frac{\Delta; \Gamma \vdash A\ \mathit{poss}}{\Delta; \Gamma \vdash \Diamond A\ \mathit{true}} \Diamond I \qquad \frac{\Delta; \Gamma \vdash \Diamond A\ \mathit{true} \qquad \Delta; A\ \mathit{true} \vdash C\ \mathit{poss}}{\Delta; \Gamma \vdash C\ \mathit{poss}} \Diamond E$$

Again, this inference system satisfies the usual structural laws of exchange, weakening, and contraction, both for true and valid hypotheses. The appropriate instances of the defining substitution principle can be expressed as a property of this formal system and proven by induction over the structure of derivations.

Theorem 2 (Substitution).
The inference system for modal logic with implication, necessity, and possibility satisfies:

1 If $\Delta; \Gamma, A\ \mathit{true}, \Gamma' \vdash C\ \mathit{true}$ and $\Delta; \Gamma \vdash A\ \mathit{true}$ then $\Delta; \Gamma, \Gamma' \vdash C\ \mathit{true}$.
2 If $\Delta; \Gamma, A\ \mathit{true}, \Gamma' \vdash C\ \mathit{poss}$ and $\Delta; \Gamma \vdash A\ \mathit{true}$ then $\Delta; \Gamma, \Gamma' \vdash C\ \mathit{poss}$.
3 If $\Delta, B\ \mathit{valid}, \Delta'; \Gamma \vdash C\ \mathit{true}$ and $\Delta; \cdot \vdash A\ \mathit{true}$ then $\Delta, \Delta'; \Gamma \vdash C\ \mathit{true}$.
4 If $\Delta, B\ \mathit{valid}, \Delta'; \Gamma \vdash C\ \mathit{poss}$ and $\Delta; \cdot \vdash A\ \mathit{true}$ then $\Delta, \Delta'; \Gamma \vdash C\ \mathit{poss}$.
5 If $\Delta; A\ \mathit{true} \vdash C\ \mathit{poss}$ and $\Delta; \Gamma \vdash A\ \mathit{poss}$ then $\Delta; \Gamma \vdash C\ \mathit{poss}$.

Proof. In parts (1–4) by straightforward induction over the structure of the first given derivation, using weakening and the inclusion of A *true* in A *poss* where needed. Part (5) follows by induction over the second given derivation. □

5.2. *Alternative Formulations*

We could avoid introducing two separate elimination rules for necessity ($\Box E$ and $\Box E_p$) with the single rule

$$\frac{\Delta;\Gamma \vdash \Box A\ \mathit{true} \qquad \Delta, A\ \mathit{valid};\Gamma \vdash J}{\Delta;\Gamma \vdash J}\,\Box E_J.$$

Unfortunately such a rule would be impredicative, quantifying over all judgments J. We prefer to avoid this by using only those instances of the general schema relevant to our development.

In our system propositional reasoning is explicit, while reasoning at the level of judgments is implicit. We can obtain another system by representing the definitions of the judgments as inference rules.

$$\frac{\Delta;\cdot \vdash A\ \mathit{true}}{\Delta \vdash A\ \mathit{valid}} \qquad \frac{\Delta \vdash A\ \mathit{valid}}{\Delta;\Gamma \vdash A\ \mathit{true}}$$

$$\frac{\Delta;\Gamma \vdash A\ \mathit{true}}{\Delta;\Gamma \vdash A\ \mathit{poss}} \qquad \frac{\Delta;\Gamma \vdash A\ \mathit{poss} \qquad \Delta; A\ \mathit{true} \vdash C\ \mathit{poss}}{\Delta;\Gamma \vdash C\ \mathit{poss}}$$

For consistency, we would modify the rules concerned with validity as follows.

$$\frac{}{\Delta, B\ \mathit{valid}, \Delta' \vdash B\ \mathit{valid}}\,\mathit{hyp}$$

$$\frac{\Delta \vdash A\ \mathit{valid}}{\Delta;\Gamma \vdash \Box A\ \mathit{true}}\,\Box I \qquad \frac{\Delta;\Gamma \vdash \Box A\ \mathit{true} \qquad \Delta, A\ \mathit{valid};\Gamma \vdash C\ \mathit{true}}{\Delta;\Gamma \vdash C\ \mathit{true}}\,\Box E$$

$$\frac{\Delta;\Gamma \vdash \Box A\ \mathit{true} \qquad \Delta, A\ \mathit{valid};\Gamma \vdash C\ \mathit{poss}}{\Delta;\Gamma \vdash C\ \mathit{poss}}\,\Box E_p$$

The difference appears to be primarily cosmetic. In practice it is more efficient to work with the compact rules of our original system.

Even though they are not needed to develop modal logic, we can also allow hypotheses of the form A *poss*. Assumptions of this form are quite weak and do not seem to interact with the other judgments and propositions in interesting ways.

5.3. *Axiomatic Characterization*

Possibility can be characterized axiomatically by the following axioms.

$$\begin{array}{l} \vdash A \supset \Diamond A\ \mathit{true} \\ \vdash \Diamond\Diamond A \supset \Diamond A\ \mathit{true} \\ \vdash \Box(A \supset B) \supset (\Diamond A \supset \Diamond B)\ \mathit{true} \end{array}$$

Natural deductions for these axioms are given in abbreviated form as proof terms in the next section.

6. Analytic and Synthetic Judgments

Martin-Löf (1994) reviews the notions of analytic and synthetic judgments as analyzed by Kant. He states:

> *[...] an analytic judgement is one which is evident in virtue of the meanings of the terms that occur in it.*

The judgment A *prop* is analytic in this sense since we can easily construct evidence for the knowledge that A is a proposition from A itself without additional insight. However, the judgment A *true* is not analytic, but *synthetic*: we need to look outside the judgment itself for evidence, typically by searching for a proof of A. Proofs are essential in our use of logic in computer science, since they contain constructions and algorithms with computational contents. Therefore Martin-Löf (1980) bases his type theory on several analytic judgments. Again, we simplify[‡] and consider "M *is a proof term for* A" (written $M : A$). It is important that M contain enough information to reconstruct the evidence for A *true* in the sense we have discussed so far. Consequently, the notions of local soundness and completeness, witnessed by local reductions and expansion, can now be rendered on the proof terms M.

We will not repeat the full construction of the rules above, but merely summarize them in their analytic form. First, conjunction.

$$\frac{M : A \qquad N : B}{\langle M, N\rangle : A \wedge B}\,\wedge I$$

$$\frac{M : A \wedge B}{\mathrm{fst}\, M : A}\,\wedge E_L \qquad\qquad \frac{M : A \wedge B}{\mathrm{snd}\, M : B}\,\wedge E_R$$

Local reduction and expansion should now be considered judgments on proof terms. We summarize them in a form typical of their use in computer science.

$$\begin{array}{rcl} \mathrm{fst}\,\langle M, N\rangle & \Longrightarrow_R & M \\ \mathrm{snd}\,\langle M, N\rangle & \Longrightarrow_R & N \\ \\ M : A \wedge B & \Longrightarrow_E & \langle \mathrm{fst}\, M, \mathrm{snd}\, M\rangle \end{array}$$

The local expansion only makes sense when M is the proof of a conjunction, which is indicated in the rule.

We will freely switch back and forth between the view of M as a proof and A as a proposition, or M as a term and A as its type. For the reductions we presuppose that each left-hand side is well-typed, which means the each corresponding right-hand side will also be well-typed and have the same type. This follows from the meaning explanation of conjunction given in its synthetic form.

‡ Martin-Löf wrote M : proof(A) reserving the colon for the relationship between and object and its type.

For hypothetical judgments we label the assumptions with variables and write $x{:}A$ for "x is a proof term for A". We continue to use Γ to stand for a collection of hypotheses, now labeled, and call it a *context*. We suppose that all variables x declared in a context are different. We tacitly employ renaming to guarantee this invariant. Note that a judgment $\Gamma \vdash A$ *true* is parametric in all variables declared in Γ and thus combines the parametric and hypothetical judgment forms (Martin-Löf, 1996). The use of hypotheses and the substitution property are now as follows, where we write $[N/x]M$ for the result of substituting N for x in M, renaming bound variables as necessary in order to avoid variable capture.

$$\frac{}{\Gamma, x{:}A, \Gamma' \vdash x : A}\ hyp \qquad \begin{array}{l}\text{If } \Gamma \vdash N : A \text{ and } \Gamma, x{:}A, \Gamma' \vdash M : C\\ \text{then } \Gamma, \Gamma' \vdash [N/x]M : C.\end{array}$$

The rules for implication are annotated in the well-known manner, using functions and applications to realize implication introduction and elimination, respectively.

$$\frac{\Gamma, x{:}A \vdash M : B}{\Gamma \vdash \lambda x{:}A.\ M : A \supset B}\supset\! I \qquad \frac{\Gamma \vdash M : A \supset B \qquad \Gamma \vdash N : A}{\Gamma \vdash M\, N : B}\supset\! E$$

The local reductions and expansions are just the familiar β-reduction and η-expansion.

$$\begin{array}{rcll}(\lambda x{:}A.\ M)\, N & \Longrightarrow_R & [N/x]M & \\ M : A \supset B & \Longrightarrow_E & \lambda x{:}A.\ M\, x & \quad \text{where } x \text{ not free in } M\end{array}$$

As in type theory (Martin-Löf, 1980), the reduction rules have computational content, while the expansion rules implement an extensionality principle.

To complete the proof term assignment, we need to label hypotheses of the form A *valid*. We write $u{::}A$ to express that the variable u labels the hypothesis that A is valid. We continue to use Δ for a context of such assumptions, again presupposing that all variables labeling hypotheses in a judgment are distinct. Note that the judgment form $u{::}A$ is never used as a succedent of a hypothetical judgment. We obtain the following hypothesis rule and substitution property.

$$\frac{}{\Delta, u{::}A, \Delta'; \Gamma \vdash u : A}\ hyp^* \qquad \begin{array}{l}\text{If } \Delta; \cdot \vdash N : A \text{ and } \Delta, u{::}A, \Delta'; \Gamma \vdash M : C\\ \text{then } \Delta, \Delta'; \Gamma \vdash [\![N/u]\!]M : C\end{array}$$

Here we use the notation $[\![N/u]\!]M$ for the result of substituting N for uses of u in M, again renaming bound variables as necessary to avoid variable capture. It is defined like ordinary substitution—we use a different notation since it is derived from a different substitution principle and replaces another kind of variable.

Next, we show the annotated forms of introduction and elimination rules and associated conversions.

$$\frac{\Delta; \cdot \vdash M : A}{\Delta; \Gamma \vdash \mathrm{box}\, M : \Box A}\Box I \qquad \frac{\Delta; \Gamma \vdash M : \Box A \qquad \Delta, u{::}A; \Gamma \vdash N : C}{\Delta; \Gamma \vdash \mathrm{let\ box}\, u = M \mathrm{\ in\ } N : C}\Box E$$

$$\begin{array}{rcl}\mathrm{let\ box}\, u = \mathrm{box}\, M \mathrm{\ in\ } N & \Longrightarrow_R & [\![M/u]\!]N \\ M : \Box A & \Longrightarrow_E & \mathrm{let\ box}\, u = M \mathrm{\ in\ box}\, u\end{array}$$

To represent possibility, we need to add a new syntactic class E of *proof expressions* and judgment $E \div A$ to express that E is a proof of A *poss*. We use E and F to stand for proof expressions. Since we know A *poss* whenever A *true*, every term M is also an expression E. The defining inclusion and substitution properties appear as follows:

$$\begin{array}{ll} \text{If } \Delta; \Gamma \vdash M : A & \qquad \text{If } \Delta; \Gamma \vdash E \div A \text{ and } \Delta; x{:}A \vdash F \div C \\ \text{then } \Delta; \Gamma \vdash M \div A & \qquad \text{then } \Delta; \Gamma \vdash \langle\!\langle E/x \rangle\!\rangle F \div C \end{array}$$

The first property tells us that every proof term M is also a proof expression. The substitution operation $\langle\!\langle E/x \rangle\!\rangle F$ needed for the second property is unusual in that it must analyze the structure of E rather than F. We give a definition below, after introducing appropriate proof terms and local conversions for $\Diamond A$. However, it should not come as a surprise that such an operation is needed, since it is merely a reflection of clause (2) in the definition of possibility.

$$\frac{\Delta; \Gamma \vdash E \div A}{\Delta; \Gamma \vdash \mathrm{dia}\, E : \Diamond A}\,\Diamond I \qquad \frac{\Delta; \Gamma \vdash M : \Diamond A \qquad \Delta; x{:}A \vdash E \div C}{\Delta; \Gamma \vdash \mathrm{let\ dia}\, x = M \,\mathrm{in}\, E \div C}\,\Diamond E$$

$$\begin{array}{rcl} \mathrm{let\ dia}\, x = \mathrm{dia}\, E \,\mathrm{in}\, F & \Longrightarrow_R & \langle\!\langle E/x \rangle\!\rangle F \\ M : \Diamond A & \Longrightarrow_E & \mathrm{dia}\,(\mathrm{let\ dia}\, x = M \,\mathrm{in}\, x) \end{array}$$

The substitution operation $\langle\!\langle E/x \rangle\!\rangle F$ must be defined in a non-standard way as hinted above.

$$\begin{array}{rcl} \langle\!\langle M/x \rangle\!\rangle F & = & [M/x]F \\ \langle\!\langle \mathrm{let\ dia}\, y = M \,\mathrm{in}\, E/x \rangle\!\rangle F & = & \mathrm{let\ dia}\, y = M \,\mathrm{in}\, \langle\!\langle E/x \rangle\!\rangle F \end{array}$$

Note that these two cases are mutually exclusive: the first applies when the proof expression is actually a proof term M, otherwise the second case must apply.

We further annotate the derived elimination rule $\Box E_p$

$$\frac{\Delta; \Gamma \vdash M : \Box A \qquad \Delta, u{::}A; \Gamma \vdash E \div C}{\Delta; \Gamma \vdash \mathrm{let\ box}\, u = M \ \mathrm{in}\ E \div C}\,\Box E_p$$

which yields one additional local reduction

$$\mathrm{let\ box}\, u = \mathrm{box}\, M \ \mathrm{in}\ E \quad \Longrightarrow_R \quad [\![M/u]\!] E$$

and a new case in the definition of substitution

$$\langle\!\langle \mathrm{let\ box}\, u = M \ \mathrm{in}\ E/x \rangle\!\rangle F \quad = \quad \mathrm{let\ box}\, u = M \ \mathrm{in}\ \langle\!\langle E/x \rangle\!\rangle F.$$

6.1. *Summary of Formal System*

We summarize the proof terms and rules for the analytic presentation of modal logic developed above. The reader should not forget that the methodology of type theory is open-ended by its very nature, and additional logical connectives can be added in an orthogonal manner.

$$
\begin{array}{rrcl}
\text{Propositions} & A & ::= & P \mid A_1 \supset A_2 \mid \Box A \mid \Diamond A \\
\text{Proof Terms} & M & ::= & x \mid \lambda x{:}A.\ M \mid M_1\, M_2 \\
& & & \mid u \mid \mathrm{box}\, M \mid \mathrm{let\ box}\, u = M_1 \mathrm{\ in\ } M_2 \\
& & & \mid \mathrm{dia}\, E \\
\text{Proof Expressions} & E & ::= & M \\
& & & \mid \mathrm{let\ dia}\, x = M \mathrm{\ in\ } E \\
& & & \mid \mathrm{let\ box}\, u = M \mathrm{\ in\ } E \\
\text{True Contexts} & \Gamma & ::= & \cdot \mid \Gamma, x{:}A \\
\text{Valid Contexts} & \Delta & ::= & \cdot \mid \Delta, u{::}A
\end{array}
$$

We have two judgments

$$
\begin{array}{ll}
\Delta; \Gamma \vdash M : A & M \text{ is a proof term for } A\ \textit{true} \\
\Delta; \Gamma \vdash E \div A & E \text{ is a proof expression for } A\ \textit{poss}
\end{array}
$$

where $\Delta; \Gamma \vdash M \div A$ whenever $\Delta; \Gamma \vdash M : A$.

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

$$
\frac{\Delta; \Gamma, x{:}A \vdash M : B}{\Delta; \Gamma \vdash \lambda x{:}A.\ M : A \supset B}\,{\supset}I
\qquad
\frac{\Delta; \Gamma \vdash M : A \supset B \qquad \Delta; \Gamma \vdash N : A}{\Delta; \Gamma \vdash M\, N : B}\,{\supset}E
$$

$$
\frac{}{\Delta, u{::}A, \Delta'; \Gamma \vdash u : A}\,\textit{hyp}^*
$$

$$
\frac{\Delta; \cdot \vdash M : A}{\Delta; \Gamma \vdash \mathrm{box}\, M : \Box A}\,\Box I
\qquad
\frac{\Delta; \Gamma \vdash M : \Box A \qquad \Delta, u{::}A; \Gamma \vdash N : C}{\Delta; \Gamma \vdash \mathrm{let\ box}\, u = M \mathrm{\ in\ } N : C}\,\Box E
$$

$$
\frac{\Delta; \Gamma \vdash M : \Box A \qquad \Delta, u{::}A; \Gamma \vdash E \div C}{\Delta; \Gamma \vdash \mathrm{let\ box}\, u = M \mathrm{\ in\ } E \div C}\,\Box E_p
$$

$$
\frac{\Delta; \Gamma \vdash E \div A}{\Delta; \Gamma \vdash \mathrm{dia}\, E : \Diamond A}\,\Diamond I
\qquad
\frac{\Delta; \Gamma \vdash M : \Diamond A \qquad \Delta; x{:}A \vdash E \div C}{\Delta; \Gamma \vdash \mathrm{let\ dia}\, x = M \mathrm{\ in\ } E \div C}\,\Diamond E
$$

We have three different forms of substitution:

1 $[M/x]N$ and $[M/x]F$ which replace a variable x by a proof term M,
2 $[\![M/u]\!]N$ and $[\![M/u]\!]F$ which replaces a variable u by a proof term M,
3 $\langle\!\langle E/x \rangle\!\rangle F$ which replaces a variable x by a proof expression E.

The first two are defined in a standard fashion, including tacit renaming of bound variables in order to avoid capture of variables free in M. The last is defined by three mutually exclusive clauses, one for each possible proof expression E.

$$
\begin{array}{rcl}
\langle\!\langle M/x \rangle\!\rangle F & = & [M/x]F \\
\langle\!\langle \mathrm{let\ dia}\, y = M \mathrm{\ in\ } E/x \rangle\!\rangle F & = & \mathrm{let\ dia}\, y = M \mathrm{\ in\ } \langle\!\langle E/x \rangle\!\rangle F \\
\langle\!\langle \mathrm{let\ box}\, u = M \mathrm{\ in\ } E/x \rangle\!\rangle F & = & \mathrm{let\ box}\, u = M \mathrm{\ in\ } \langle\!\langle E/x \rangle\!\rangle F
\end{array}
$$

The guiding substitution principles can be expressed as a property.

Theorem 3 (Substitution on Proof Terms and Expressions).
The analytic inference system for modal logic with implication, necessity, and possibility satisfies:

1 If $\Delta; \Gamma, x{:}A, \Gamma' \vdash N : C$ and $\Delta; \Gamma \vdash M : A$ then $\Delta; \Gamma, \Gamma' \vdash [M/x]N : C$.
2 If $\Delta; \Gamma, x{:}A, \Gamma' \vdash F \div C$ and $\Delta; \Gamma \vdash M : A$ then $\Delta; \Gamma, \Gamma' \vdash [M/x]F \div C$.
3 If $\Delta, u{::}B, \Delta'; \Gamma \vdash N : C$ and $\Delta; \cdot \vdash M : B$ then $\Delta, \Delta'; \Gamma \vdash [\![M/u]\!]N : C$.
4 If $\Delta, u{::}B, \Delta'; \Gamma \vdash F \div C$ and $\Delta; \cdot \vdash M : B$ then $\Delta, \Delta'; \Gamma \vdash [\![M/u]\!]F \div C$.
5 If $\Delta; x{:}A \vdash F \div C$ and $\Delta; \Gamma \vdash E \div A$ then $\Delta; \Gamma \vdash \langle\!\langle E/x \rangle\!\rangle F \div C$.

Proof. By straightforward induction over the structure of the first given derivation except in part (5), where the induction is on the second given derivation as in the proof of Theorem 2. □

Ordinary substitutions satisfy a distribution property of the form

$$[M_1/x_1][M_2/x_2]M_3 = [[M_1/x_1]M_2/x_2][M_1/x_1]M_3$$

under the assumption that x_2 is not free in M_1. This follows by a simple induction on the structure of M_3. Similar properties hold for substitutions of $[\![M_1/u_1]\!]$ and $[M_1/x_1]$ in various terms or expressions, because these are essentially capture-avoiding replacement operations. The new form of substitution $\langle\!\langle E/x \rangle\!\rangle$ satisfies a corresponding law which we need in the proof of Theorem 7.

Theorem 4 (Composition of Substitution).
If $\Delta; \Gamma \vdash E_1 \div A_1$, $\Delta; x_1{:}A_1 \vdash E_2 \div A_2$, and $\Delta; x_2{:}A_2 \vdash E_3 \div A_3$, then

$$\langle E_1/x_1 \rangle \langle E_2/x_2 \rangle E_3 = \langle \langle E_1/x_1 \rangle E_2/x_2 \rangle E_3$$

Proof. By induction on the structure of E_1 (not E_3!), taking advantage of the straightforward substitution properties mentioned above. Note that the typing preconditions do not impose any artificial restrictions; they just guarantee that both substitution operations are sensible according to Theorem 3(5). □

The subject reduction and expansion theorem now follows easily from the substitution properties. The core of the proof is already contained in the local reductions we showed in the meaning explanation of the inference rules. We define $M \Longrightarrow_R M'$, $E \Longrightarrow_R E'$, $M \Longrightarrow_E M'$, and $E \Longrightarrow_E E'$ by the following rules.

$$\begin{array}{rcl}
(\lambda x{:}A.\ N)\, M & \Longrightarrow_R & [M/x]N \\
\mathrm{let\ box}\, u = \mathrm{box}\, M \mathrm{\ in\ } N & \Longrightarrow_R & [\![M/u]\!]N \\
\mathrm{let\ dia}\, x = \mathrm{dia}\, E \mathrm{\ in\ } F & \Longrightarrow_R & \langle\!\langle E/x \rangle\!\rangle F \\
\mathrm{let\ box}\, u = \mathrm{box}\, M \mathrm{\ in\ } F & \Longrightarrow_R & [\![M/u]\!]F
\end{array}$$

$$\begin{array}{rcll}
M : A \supset B & \Longrightarrow_E & \lambda x{:}A.\ M\, x & \quad \text{where } x \text{ not free in } M \\
M : \Box A & \Longrightarrow_E & \mathrm{let\ box}\, u = M \mathrm{\ in\ box}\, u & \\
M : \Diamond A & \Longrightarrow_E & \mathrm{dia}\, (\mathrm{let\ dia}\, x = M \mathrm{\ in\ } x) &
\end{array}$$

Theorem 5 (Subject Reduction and Expansion).
The modal λ-calculus with implication, necessity, and possibility satisfies:

1 If $\Delta; \Gamma \vdash M : A$ and $M \Longrightarrow_R N$ then $\Delta; \Gamma \vdash N : A$.
2 If $\Delta; \Gamma \vdash E \div A$ and $E \Longrightarrow_R F$ then $\Delta; \Gamma \vdash F \div A$.
3 If $\Delta; \Gamma \vdash M : A$ and $M : A \Longrightarrow_E N$ then $\Delta; \Gamma \vdash N : A$.

Proof. Parts (1) and (2) follow by simply inductions on the definition of $\Longrightarrow_R$: for congruence rules, we apply to the induction hypothesis; for actual reductions we use the substitution properties 3.

Part (3) follows similarly by induction, but no appeal to substitution is necessary. Instead we construct the needed derivation directly from the given one as in the local expansion on derivations. □

It is easy to see that the subject reduction property is preserved if we allow reductions to be applied at arbitrary subterms. For subject expansion this also holds if the subterm has the appropriate type.

6.2. *Some Examples*

We now revisit the axiomatic characterization of modal logic and give a proof term for each axiom.

$$\begin{array}{ll} \vdash & \lambda x{:}A \supset B \supset C.\ \lambda y{:}A \supset B.\ \lambda z{:}A.\ (x\,z)\,(y\,z) \\ : & (A \supset B \supset C) \supset (A \supset B) \supset A \supset C \end{array}$$

$$\begin{array}{ll} \vdash & \lambda x{:}A.\ \lambda y{:}B.\ x \\ : & A \supset B \supset A \end{array}$$

$$\begin{array}{ll} \vdash & \lambda x{:}\Box(A \supset B).\ \lambda y{:}\Box A.\ \mathrm{let\ box}\,u = x \mathrm{\ in\ let\ box}\,w = y \mathrm{\ in\ box}\,(u\,w) \\ : & \Box(A \supset B) \supset (\Box A \supset \Box B) \end{array}$$

$$\begin{array}{ll} \vdash & \lambda x{:}\Box A.\ \mathrm{let\ box}\,u = x \mathrm{\ in\ } u \\ : & \Box A \supset A \end{array}$$

$$\begin{array}{ll} \vdash & \lambda x{:}\Box A.\ \mathrm{let\ box}\,u = x \mathrm{\ in\ box\,box}\,u \\ : & \Box A \supset \Box\Box A \end{array}$$

$$\begin{array}{ll} \vdash & \lambda x{:}A.\ \mathrm{dia}\,x \\ : & A \supset \Diamond A \end{array}$$

$$\begin{array}{ll} \vdash & \lambda x{:}\Diamond\Diamond A.\ \mathrm{dia}\,(\mathrm{let\ dia}\,y = x \mathrm{\,in\ let\ dia}\,z = y \mathrm{\,in\ } z) \\ : & \Diamond\Diamond A \supset \Diamond A \end{array}$$

$$\begin{array}{ll} \vdash & \lambda x{:}\Box(A \supset B).\ \lambda y{:}\Diamond A.\ \mathrm{let\ box}\,u = x \mathrm{\ in\ dia}\,(\mathrm{let\ dia}\,z = y \mathrm{\,in\ } u\,z) \\ : & \Box(A \supset B) \supset (\Diamond A \supset \Diamond B) \end{array}$$

The inference rules of the axiomatic system are also easily realized.

$$\frac{\vdash M : A \supset B \qquad \vdash N : A}{\vdash M\,N : B}\,mp \qquad\qquad \frac{\vdash M : A}{\vdash \mathrm{box}\,M : \Box A}\,nec$$

7. Lax Logic

Lax logic (Fairtlough and Mendler, 1997) is an intuitionistic logic with a single modal operator $\bigcirc$. It was motivated by hardware verification (Fairtlough and Mendler, 1994) and has found applications in the foundations of constraint logic programming (Fairtlough et al., 1997). It has also been related to the monadic metalanguage (Benton et al., 1998), which we will examine in the next section, and to higher-order definitions of logical connectives (Aczel, 1999).

We develop here the fragment of lax logic containing implication $A \Rightarrow B$ and the *lax modality* $\bigcirc A$. We use a different notation for implication than in modal logic, so we may later give the connective a different interpretation as *lax implication*. We will give two different explanations of lax logic. The first characterizes lax truth via judgments in the manner of the preceding sections. Our starting points are just the concepts of truth and hypothetical judgments. In particular, the presentation is independent of modal logic and categorical judgments. The second explanation uses necessity and possibility to show that lax truth is a derived notion, already available in modal logic. The fact that our formulation is equivalent to the standard formulation is proven in Section 8, where we also exhibit translations between proof terms.

We begin with a judgmental definition of lax truth. We have a new judgment, A *lax* for a proposition A. We may think of A *lax* as stating that A is true subject to some constraints, without making explicit relative to which system of constraints.

Definition of Lax Truth

1 If $\Gamma \vdash A\ \mathit{true}$ then $\Gamma \vdash A\ \mathit{lax}$.
2 If $\Gamma \vdash A\ \mathit{lax}$ and $\Gamma, A\ \mathit{true} \vdash C\ \mathit{lax}$ then $\Gamma \vdash C\ \mathit{lax}$.

The first clause expresses that if A is true, then A is true under some constraint (namely: the constraint which is always satisfied). The second expresses that if A is true under some constraints, we may reason as if A were true. Any consequence we derive, however, will only be known as true under constraints. Internalizing this judgment as a propositional operator is simple.

$$\frac{\Gamma \vdash A\ \mathit{lax}}{\Gamma \vdash \bigcirc A\ \mathit{true}}\bigcirc I \qquad\qquad \frac{\Gamma \vdash \bigcirc A\ \mathit{true} \qquad \Gamma, A\ \mathit{true} \vdash C\ \mathit{lax}}{\Gamma \vdash C\ \mathit{lax}}\bigcirc E$$

As for possibility, we allow silent passage from A *true* to A *lax*, and write $\bigcirc I^*$ and $\bigcirc E^*$ when this inclusion is used the premises of these rules.

Local soundness is easily seen from the local reduction

$$\frac{\dfrac{\begin{array}{c}\mathcal{D}\\ \Gamma \vdash A\ \mathit{lax}\end{array}}{\Gamma \vdash \bigcirc A\ \mathit{true}}\bigcirc I \qquad \begin{array}{c}\mathcal{E}\\ \Gamma, A\ \mathit{true} \vdash C\ \mathit{lax}\end{array}}{\Gamma \vdash C\ \mathit{lax}}\bigcirc E \quad \Longrightarrow_R \quad \begin{array}{c}\mathcal{E}'\\ \Gamma \vdash C\ \mathit{lax}\end{array}$$

where $\mathcal{E}'$ is justified by part (2) in the definition of lax truth.

The elimination is also locally complete, as witnessed by the following expansion.

$$\begin{array}{c}\mathcal{D}\\ \Gamma \vdash \bigcirc A\ \mathit{true}\end{array} \quad \Longrightarrow_E \quad \dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ \Gamma \vdash \bigcirc A\ \mathit{true}\end{array} \qquad \dfrac{}{\Gamma, A\ \mathit{true} \vdash A\ \mathit{true}}\,\mathit{hyp}}{\Gamma \vdash A\ \mathit{lax}}\,\bigcirc E^*}{\Gamma \vdash \bigcirc A\ \mathit{true}}\,\bigcirc I$$

To provide more intuition, we return to the interpretation of A *lax* as A *is true under some constraint*. The following laws characterize lax logic axiomatically and have a simple interpretation in terms of constraints.

1 $\vdash A \Rightarrow \bigcirc A$ *true*: If A is true, the A is true under the trivial constraint.

2 $\vdash \bigcirc\bigcirc A \Rightarrow \bigcirc A$ *true*: If A is true under two constraints than A is true under their conjunction.

3 $\vdash (A \Rightarrow B) \Rightarrow (\bigcirc A \Rightarrow \bigcirc B)$ *true*: If A implies B, and A is true under some constraint, then B is true under the same constraint.

The lax modality is very similar to possibility, but it differs in the proposition $(A \Rightarrow B) \Rightarrow (\bigcirc A \Rightarrow \bigcirc B)$ which is not true for arbitrary A and B if we replace $\bigcirc$ by $\Diamond$. Instead, we only have $\vdash \Box(A \supset B) \supset (\Diamond A \supset \Diamond B)$. Similarly, in the elimination rule $\bigcirc E$ the hypotheses Γ are available in the second premise, while in $\Diamond E$ only the hypotheses Δ on the validity of propositions are available in the second premise.

This last observation provides a crucial insight for designing a direct interpretation of lax logic in intuitionistic modal logic. We use the embedding $()^+$ of propositions and hypotheses:

$$\begin{array}{rcl}(A \Rightarrow B)^+ &=& \Box A^+ \supset B^+\\ (\bigcirc A)^+ &=& \Diamond\Box A^+\\ P^+ &=& P \qquad \text{for atomic } P\\[4pt] (\cdot)^+ &=& \cdot\\ (\Gamma, A\ \mathit{true})^+ &=& \Gamma^+, A^+\ \mathit{valid}\end{array}$$

In order to state the correctness of this interpretation of lax logic in modal logic, we write $\overset{L}{\vdash}$ for judgments in lax logic and $\overset{M}{\vdash}$ for judgments in modal logic.

Theorem 6 (Lax Logic in Modal Logic).
$\Gamma \overset{L}{\vdash} A$ *true* iff $\Gamma^+; \cdot \overset{M}{\vdash} A^+$ *true*.

Proof. From left to right, we show

1 if $\Gamma \overset{L}{\vdash} A$ *true* then $\Gamma^+; \cdot \overset{M}{\vdash} A^+$ *true*, and
2 if $\Gamma \overset{L}{\vdash} A$ *lax* then $\Gamma^+; \cdot \overset{M}{\vdash} \Box A^+$ *poss*

by simultaneous induction on the structure of the given derivations. The inferences rules of lax logic become *derived* rules in modal logic, under the given translation on propositions.

For the opposite direction we define a reverse translation $()^{-}$:

$$\begin{array}{rcll}
(A \supset B)^{-} & = & A^{-} \Rightarrow B^{-} & \\
(\Box A)^{-} & = & A^{-} & \\
(\Diamond A)^{-} & = & \bigcirc A^{-} & \\
P^{-} & = & P & \text{for atomic } P \\
(\cdot)^{-} & = & \cdot & \\
(\Delta, A\ \mathit{valid})^{-} & = & \Delta^{-}, A^{-}\ \mathit{true} & \\
(\Gamma, A\ \mathit{true})^{-} & = & \Gamma^{-}, A^{-}\ \mathit{true} &
\end{array}$$

which satisfies $(A^{+})^{-} = A$. The two properties,

1 if $\Delta; \Gamma \overset{M}{\vdash} A\ \mathit{true}$ then $\Delta^{-}, \Gamma^{-} \overset{L}{\vdash} A^{-}\ \mathit{true}$, and
2 if $\Delta; \Gamma \overset{M}{\vdash} A\ \mathit{poss}$ then $\Delta^{-}, \Gamma^{-} \overset{L}{\vdash} A^{-}\ \mathit{lax}$,

then follow by simultaneous induction on the given derivations. In this direction we need weakening and the substitution principle. From the assumption $\Gamma^{+}; \cdot \overset{M}{\vdash} A^{+}\ \mathit{true}$ we then conclude $(\Gamma^{+})^{-} \overset{L}{\vdash} (A^{+})^{-}\ \mathit{true}$ and therefore $\Gamma \overset{L}{\vdash} A\ \mathit{true}$. □

The results above mean that we can define

$$\begin{array}{rcl}
A \Rightarrow B & = & \Box A \supset B \\
\bigcirc A & = & \Diamond \Box A
\end{array}$$

and then use modal logic for reasoning in lax logic. Since the rules of lax logic are derived (and not just admissible), we can retain the structure of proofs in the translation. We make this explicit in Section 8, where we revisit the above embedding, including proof terms.

It remains to see if we can characterize lax implication and the lax modality directly in modal logic via introduction and elimination rules which are locally sound and complete and equivalent to the definitions above.

For lax implication, this is easy to achieve and verify.

$$\frac{\Delta, A\ \mathit{valid}; \Gamma \vdash B\ \mathit{true}}{\Delta; \Gamma \vdash A \Rightarrow B\ \mathit{true}} \Rightarrow I \qquad \frac{\Delta; \Gamma \vdash A \Rightarrow B\ \mathit{true} \qquad \Delta; \cdot \vdash A\ \mathit{true}}{\Delta; \Gamma \vdash B\ \mathit{true}} \Rightarrow E$$

In the elimination rule we use $\Delta; \cdot \vdash A\ \mathit{true}$ to express that $\Delta \vdash A\ \mathit{valid}$, as in the introduction rule for necessity. Local soundness and completeness can be verified using the substitution principle for validity from Section 4. These rules are well-known from linear logic programming (Hodas and Miller, 1994), because in linear logic with a modal operator ! (which corresponds to $\Box$ in our setting), goal-directed search is incomplete. Replacing it by the analogue of lax implication avoids this problem and allows the use of intuitionistic linear logic as the basis of a logic programming language.

The lax modality is more difficult to characterize by introduction and elimination rules in the presence of necessity and possibility and seems to require a new judgment $A\ \mathit{lax}$ which we can also read as *A is possibly necessary*. This follows the blueprint of the definition of the lax modality, except that the interaction with the judgments of possibility and necessity requires laws relating them. In practice, it would seem preferable to either reason directly in lax logic as defined at the beginning of the section, or to reason in modal logic with the defined modality of $\bigcirc A = \Diamond\Box A$ and corresponding derived rules of inference.

8. Monadic Metalanguage

Moggi (1988; 1989; 1991) proposed the the monadic metalanguage λ_{ml} as a general foundation for the semantics of programming languages with functions and effects. He separates, in the type system, *values* from *computations*, where the latter may have effects. The monadic metalanguage abstracts from any particular notion of effect (such as update of mutable references, or raising of exceptions). In this way, it is similar to modal logic which reasons about necessity and possibility, but abstracts from any particular collection of worlds.

Benton, Biermann, and de Paiva (1998) showed that the monadic metalanguage is connected to lax logic via proof term assignment. We show the relevant fragment of the calculus here. We use the notation of lax logic, writing $\bigcirc A$ for the computations of type A, rather than TA or MA.

$$\frac{}{\Gamma, x{:}A, \Gamma' \vdash x : A}\,hyp$$

$$\frac{\Gamma, x{:}A \vdash e : B}{\Gamma \vdash \lambda x{:}A.\, e : A \Rightarrow B}\Rightarrow\!I \qquad \frac{\Gamma \vdash f : A \Rightarrow B \qquad \Gamma \vdash e : A}{\Gamma \vdash f\, e : B}\Rightarrow\!E$$

$$\frac{\Gamma \vdash e : A}{\Gamma \vdash \mathrm{val}\, e : \bigcirc A}\bigcirc I \qquad \frac{\Gamma \vdash e : \bigcirc A \qquad \Gamma, x{:}A \vdash f : \bigcirc C}{\Gamma \vdash \mathrm{let\,val}\, x = e \,\mathrm{in}\, f : \bigcirc C}\bigcirc E$$

We have the following two local reductions.

$$\begin{array}{rcl} (\lambda x{:}A.\ f)\ e & \Longrightarrow_R & [e/x]f \\ \mathrm{let\,val}\, x = \mathrm{val}\, e \,\mathrm{in}\, f & \Longrightarrow_R & [e/x]f \end{array}$$

However, these do not suffice as the basis for an operational semantics, because of the unusual elimination rule for the lax modality. We need the following additional rule, which does not fall into the class of local reductions but has the form of a *commuting reduction*.

$$\mathrm{let\,val}\, x_2 = (\mathrm{let\,val}\, x_1 = e_1 \,\mathrm{in}\, e_2) \,\mathrm{in}\, e \Longrightarrow_C \mathrm{let\,val}\, x_1 = e_1 \,\mathrm{in}\, (\mathrm{let\,val}\, x_2 = e_2 \,\mathrm{in}\, e)$$

The local expansions are not computationally relevant, but correspond to extensionality. They are less problematic.

$$\begin{array}{rcl} e : A \Rightarrow B & \Longrightarrow_E & \lambda x{:}A.\, e\, x \\ e : \bigcirc A & \Longrightarrow_E & \mathrm{let\,val}\, x = e \,\mathrm{in\,val}\, x \end{array}$$

We can fix the anomaly in the reduction relation through the judgmental reconstruction of lax logic in Section 7. We have two basic judgment forms $M : A$ (M is a proof term for A *true*) and $E \div A$ (E is a proof expression for A *lax*). The definition of the lax modality yields the following principles.

$$\begin{array}{ll} \text{If } \Gamma \vdash M : A & \text{If } \Gamma \vdash E \div A \text{ and } \Gamma, x{:}A \vdash F \div C \\ \text{then } \Gamma \vdash M \div A & \text{then } \Gamma \vdash \langle E/x \rangle F \div C \end{array}$$

The first one means that we view proof terms and proof expressions as separate syntactic classes, where every proof term is a proof expression, but not vice versa. The introduction and elimination rules:

$$\frac{\Gamma \vdash E \div A}{\Gamma \vdash \mathrm{val}\, E : \bigcirc A}\bigcirc I \qquad \frac{\Gamma \vdash M : \bigcirc A \qquad \Gamma, x{:}A \vdash E \div C}{\Gamma \vdash \mathrm{let\,val}\, x = M \,\mathrm{in}\, E \div C}\bigcirc E$$

Then the local reductions and expansions have the following form.

$$\begin{array}{rcl} (\lambda x{:}A.\ M)\, N & \Longrightarrow_R & [N/x]M \\ \mathrm{let\,val}\, x = \mathrm{val}\, E \,\mathrm{in}\, F & \Longrightarrow_R & \langle E/x\rangle F \\[1ex] M : A \Rightarrow B & \Longrightarrow_E & \lambda x{:}A.\ M\, x \\ M : \bigcirc A & \Longrightarrow_E & \mathrm{val}\,(\mathrm{let\,val}\, x = M \,\mathrm{in}\, x) \end{array}$$

Lax substitution $\langle E/x\rangle F$ is defined inductively on the structure of E.

$$\begin{array}{rcl} \langle M/x\rangle F & = & [M/x]F \\ \langle \mathrm{let\,val}\, y = M \,\mathrm{in}\, E/x\rangle F & = & \mathrm{let\,val}\, y = M \,\mathrm{in}\, \langle E/x\rangle F \end{array}$$

We now show the proof terms for the characteristic axioms of lax logic.

$$\begin{array}{ll} \vdash & \lambda x{:}A.\ \mathrm{val}\, A \\ : & A \Rightarrow \bigcirc A \\[1ex] \vdash & \lambda x{:}\bigcirc\bigcirc A.\ \mathrm{val}\,(\mathrm{let\,val}\, y = x \,\mathrm{in}\, \mathrm{let\,val}\, z = y \,\mathrm{in}\, z) \\ : & \bigcirc\bigcirc A \Rightarrow \bigcirc A \\[1ex] \vdash & \lambda x{:}A \Rightarrow B.\ \lambda y{:}\bigcirc A.\ \mathrm{val}\,(\mathrm{let\,val}\, z = y \,\mathrm{in}\, x\, z) \\ : & (A \Rightarrow B) \Rightarrow (\bigcirc A \Rightarrow \bigcirc B) \end{array}$$

The following two mutually recursive translations from terms in the monadic metalanguage to lax terms have several desirable properties, as we demonstrate below. $e^\sharp$ is defined for arbitrary well-typed terms e, while $e^\top$ is defined only for terms e whose type has the form $\bigcirc A$.

$$\begin{array}{rcl} x^\sharp & = & x \\ (\lambda x{:}A.\ e)^\sharp & = & \lambda x{:}A.\ e^\sharp \\ (e_1\, e_2)^\sharp & = & e_1^\sharp\, e_2^\sharp \\[1ex] (\mathrm{val}\, e)^\sharp & = & \mathrm{val}\, e^\sharp \\ (\mathrm{let\,val}\, x = e_1 \,\mathrm{in}\, e_2)^\sharp & = & \mathrm{val}\,(\mathrm{let\,val}\, x = e_1 \,\mathrm{in}\, e_2)^\top \\[1ex] (\mathrm{let\,val}\, x = e_1 \,\mathrm{in}\, e_2)^\top & = & \langle e_1^\top/x\rangle e_2^\top \\ (\mathrm{val}\, e)^\top & = & e^\sharp \\ x^\top & = & \mathrm{let\,val}\, x_0 = x^\sharp \,\mathrm{in}\, x_0 \\ (e_1\, e_2)^\top & = & \mathrm{let\,val}\, x_0 = (e_1\, e_2)^\sharp \,\mathrm{in}\, x_0 \end{array}$$

We write $\overset{L}{\Longleftrightarrow}{}^*_{RE}$ for the congruence relation generated by local reductions and expansions in the lax λ-calculus, and $\overset{C}{\Longleftrightarrow}{}^*_{C}$ and $\overset{C}{\Longleftrightarrow}{}^*_{REC}$ for the congruence relations generated by commuting conversion, and local reduction, expansion, and commuting conversion, respectively, in the monadic metalanguage. We also write $\overset{C}{\vdash}$ and $\overset{L}{\vdash}$ for hypothetical judgments in the monadic metalanguage and lax logic, respectively.

Theorem 7 (Monadic Metalanguage and Lax Logic).

1 $\Gamma \overset{C}{\vdash} e : A$ iff $\Gamma \overset{L}{\vdash} e^\sharp : A$.
2 $\Gamma \overset{C}{\vdash} e : \bigcirc A$ iff $\Gamma \overset{L}{\vdash} e^\top \div A$.
3 If $e \overset{C}{\Longleftrightarrow}{}^*_C f$ then $e^\sharp = f^\sharp$.
4 $e \overset{C}{\Longleftrightarrow}{}^*_{REC} f$ iff $e^\sharp \overset{L}{\Longleftrightarrow}{}^*_{RE} f^\sharp$.

Proof. The typing properties (1) and (2) follow by an easy simultaneous induction on the definition of the translations, using inversion on the given typing derivations.

Part (3) confirms that the commuting reduction of the monadic metalanguage is not necessary in our formulation of lax logic—terms which differ by commuting reductions are actually equal (modulo the possible renaming of bound variables, as usual). This is easy to show by direct calculation, using elementary properties of substitution (Theorem 4).

Part (4) shows that the equational theory of the monadic metalanguage is respected by the translation. From left to right this follows by simple calculation for each possible conversion, using elementary properties of substitution. From right to left we define two reverse translations $M^\flat$ and $E^\perp$ as follows:

$$\begin{array}{rcl}
x^\flat & = & x \\
(\lambda x{:}A.\ M)^\flat & = & \lambda x{:}A.\ M^\flat \\
(M_1\ M_2)^\flat & = & M_1^\flat\ M_2^\flat \\
(\mathrm{val}\ E)^\flat & = & E^\perp \\
\\
(\mathrm{let\ val}\ x = M \ \mathrm{in}\ E)^\perp & = & \mathrm{let\ val}\ x = M^\flat \ \mathrm{in}\ E^\perp \\
M^\perp & = & \mathrm{val}\ M^\flat
\end{array}$$

We then show

1 if $\Gamma \overset{L}{\vdash} M : A$ then $\Gamma \overset{C}{\vdash} M^\flat : A$, and
2 if $\Gamma \overset{L}{\vdash} E \div A$ then $\Gamma \overset{C}{\vdash} E^\perp : \bigcirc A$.

The reverse translation preserves equality, which follows by simple calculations:

1 If $M \overset{L}{\Longleftrightarrow}{}^*_{RE} N$ then $M^\flat \overset{C}{\Longleftrightarrow}{}^*_{REC} N^\flat$.
2 If $E \overset{L}{\Longleftrightarrow}{}^*_{RE} F$ then $E^\perp \overset{C}{\Longleftrightarrow}{}^*_{REC} F^\perp$.
3 $(e^\sharp)^\flat \overset{C}{\Longleftrightarrow}{}^*_{REC} e$.
4 $(e^\top)^\perp \overset{C}{\Longleftrightarrow}{}^*_{REC} e$.

Therefore, $e^\sharp \overset{L}{\Longleftrightarrow}{}^*_{RE} f^\sharp$ implies $e \overset{C}{\Longleftrightarrow}{}^*_{REC} (e^\sharp)^\flat \overset{C}{\Longleftrightarrow}{}^*_{REC} (f^\sharp)^\flat \overset{C}{\Longleftrightarrow}{}^*_{REC} f$. □

We also conjecture a strong relationship between reduction sequences in the two calculi under the given translation, even though a direct simulation theorem fails. A further study of computational behavior is beyond the scope of this paper. The similarity of our techniques and those by Sabry and Wadler (1997) suggest an approach we intend to pursue in future work.

As an alternative to a direct term assignment for lax logic, we can use the embedding of lax logic in modal logic to give an account of the monadic metalanguage in modal logic. A proposal along similar lines has been made by S. Kobayashi (1997), with an emphasis on a categorical semantics. His natural deduction formulation, and therefore his programming language concepts, are not satisfactory. In particular, his system requires simultaneous substitutions in two rules to model validity (as in the system by Bierman and de Paiva (1996)), and also has a somewhat unmotivated interaction between possibility and falsehood. Our formulation below eliminates the first deficiency and can be extended to avoid the second.

We show the embedding from Section 7 on proof terms. First, we recall the embedding of propositions.

$$\begin{array}{rcl} (A \Rightarrow B)^+ & = & \Box A^+ \supset B^+ \\ (\bigcirc A)^+ & = & \Diamond \Box A^+ \\ P^+ & = & P \qquad \text{for atomic } P \end{array}$$

Intuitively, the type $\Box A$ denotes *stable values*, that is, values that survive effects. The type $\Diamond A$ denotes computations returning values of type A. In the monadic metalanguage, all values are stable, so a function $A \Rightarrow B$ accepts a stable value of type A and returns a value of type B, while $\bigcirc A$ is a computation which returns a stable value of type A. It is not clear if the possibility to consider values which are not stable is of much practical interest, but it is conceivable, for example, that an effect such as deallocation of memory could destroy some values, while others survive.

We assume that for every variable $x{:}A$ in the lax λ-calculus there is a corresponding variable $u_x{::}A^+$ in the modal λ-calculus. We define the translations M^+ and E^*.

$$\begin{array}{rcl} (\lambda x{:}A.\ M)^+ & = & \lambda x{:}\Box A^+.\ \text{let box}\, u_x = x \text{ in } M^+ \\ x^+ & = & u_x \\ (M\, N)^+ & = & M^+\, (\text{box}\, N^+) \\ (\text{val}\, E)^+ & = & \text{dia}\, E^* \\ \\ (\text{let val}\, x = M \,\text{in}\, E)^* & = & \text{let dia}\, x = M^+ \,\text{in}\, (\text{let box}\, u_x = x \text{ in } E^*) \\ M^* & = & \text{box}\, M^+ \end{array}$$

We write $M \overset{L}{\Longrightarrow}_R N$ for local reduction in the lax λ-calculus, and $M \overset{M}{\Longrightarrow}_R N$ for local reduction in the modal λ-calculus. Moreover, we write $M \overset{M}{\Longrightarrow}{}^*_R N$ for an arbitrary number of reductions. As before we use $\Longleftrightarrow^*_{RE}$ for the congruence relation generated by local reduction and expansion.

Theorem 8 (Lax λ-Calculus in Modal λ-Calculus).

1 $\Gamma \overset{L}{\vdash} M : A$ iff $\Gamma^+; \cdot \overset{M}{\vdash} M^+ : A^+$.
2 $\Gamma \overset{L}{\vdash} E \div A$ iff $\Gamma^+; \cdot \overset{M}{\vdash} E^* \div \Box A^+$.
3 If $M \overset{L}{\Longrightarrow}_R N$ then $M^+ \overset{M}{\Longrightarrow}{}^*_R N^+$.
4 If $E \overset{L}{\Longrightarrow}_R F$ then $E^* \overset{M}{\Longrightarrow}{}^*_R F^*$.
5 $M \overset{L}{\Longleftrightarrow}{}^*_{RE} N$ iff $M^+ \overset{M}{\Longleftrightarrow}{}^*_{RE} N^+$.
6 $E \overset{L}{\Longleftrightarrow}{}^*_{RE} F$ iff $E^* \overset{M}{\Longleftrightarrow}{}^*_{RE} F^*$.

Proof. The first two properties are verified as in the proof of Theorem 6.

The proof of the next two properties is by cases. We see that each reduction translates into precisely two consecutive reductions. Furthermore, if the original reductions are outermost, so are the two consecutive reductions on the image. This means that the structure of computations in the lax λ-calculus is preserved under the interpretation.

Finally, the preservation of equality from left to right is proven by cases, using elementary substitution properties. From right to left we define two inverse translations, M^- and $E^\$$:

$$\begin{array}{rcl}
(A \supset B)^- & = & A^- \Rightarrow B^- \\
(\Box A)^- & = & A^- \\
(\Diamond A)^- & = & \bigcirc A^- \\
P^- & = & P \\
\\
(\lambda x{:}A.\ M)^- & = & \lambda x{:}A^-.\ M^- \\
(M_1\ M_2)^- & = & M_1^-\ M_2^- \\
x^- & = & x \\
(\mathrm{box}\, M)^- & = & M^- \\
(\mathrm{let\ box}\, u = M \mathrm{\ in\ } N)^- & = & [M^-/x_u]N^- \\
u^- & = & x_u \\
(\mathrm{dia}\, E)^- & = & \mathrm{val}\, E^\$ \\
(\mathrm{let\ dia}\, x = M \mathrm{\ in\ } E)^\$ & = & \mathrm{let\ val}\, x = M^- \mathrm{\ in\ } E^\$ \\
(\mathrm{let\ box}\, u = M \mathrm{\ in\ } E)^\$ & = & [M^-/x_u]E^\$ \\
M^\$ & = & M^-
\end{array}$$

This translation satisfies

1. If $\Delta; \Gamma \vdash^M M : A$ then $\Delta^-, \Gamma^- \vdash^L M^- : A^-$.
2. If $\Delta; \Gamma \vdash^M E \div A$ then $\Delta^-, \Gamma^- \vdash^L E^\$ \sim A^-$.
3. $(M^+)^- = M$.
4. $(E^*)^\$ = E$.
5. If $M \overset{M}{\Longleftrightarrow}{}^*_{RE} N$ then $M^- \overset{L}{\Longleftrightarrow}{}^*_{RE} N^-$.
6. If $E \overset{M}{\Longleftrightarrow}{}^*_{RE} F$ then $E^\$ \overset{L}{\Longleftrightarrow}{}^*_{RE} F^\$$.

From this we directly conclude the reverse directions of the biconditionals in properties (5) and (6) of the theorem. □

9. Conclusion

We have presented a judgmental reconstruction of the modal logic of necessity and possibility, leading to a clean and simple formulation of natural deduction and associated proof terms. Because the definitions of logical connectives are orthogonal in this approach, other propositional connectives can easily be added with their usual introduction and elimination rules. We plan to investigate extensions to first-order logic and type theory, which require parametric judgments and more attention to the question when propositions are well-formed. We have also left the study of various normalization properties, as well as a formulation of a sequent calculus and cut elimination to a future paper.

The idea of separating truth and validity in a logical framework goes back to Avron et al. (1992) and is explored further by Miculan (1997). These systems, however, are rooted in Prawitz's (1965) classical treatment and do not take full advantage of the available judgmental notions. The resulting calculi are significantly more complex than our proposal and not immediately amenable to a computational interpretation.

Another approach to the explanation of modal logic is via Kripke structures. This uses the basic judgments "*proposition A is true in world w*", and "*world w' is reachable from world w*". While more verbose and requiring explicit reasoning about worlds, this approach is also more flexible in that various traditional modal logics can be expressed simply by varying the reachability judgment. Viganò (1997) and Miculan (1997) have conducted systematic studies of modal logic via Kripke structures from the point of view of logical frameworks.

In certain cases this can be simplified to obtain a formulation of natural deduction employing a stack of contexts, representing a path through the Kripke structure. Variations of this idea can be found in several papers (Martini and Masini, 1994; Pfenning and Wong, 1995; Davies and Pfenning, 2000), including a very fine-grained study of reduction (Goubault-Larrecq, 1996; 1997). These are natural for some applications of necessity, but it does not appear that similarly compact and elegant versions exist for possibility.

One particularly fruitful interpretation of $\Box A$ is as the *intensional type* for expressions denoting elements of type A. Embedding types of this form in a programming language means that we can compute with expressions as well as values. The term $\mathrm{box}\, M$ quotes the expression M, and the construct $\mathrm{let}\ \mathrm{box}\, u = M\ \mathrm{in}\ N$ binds u to the expression computed by M and then computes the value of N. The restrictions placed on the introduction rule for $\Box A$ mean that a term $\mathrm{box}\, M$ can only refer to other expression variables u but not value variables x. This is consistent with the intensional interpretation of $\Box A$, since we may not know an expression which denotes a given value and therefore cannot permit an arbitrary value as an expression.

The local reduction rules can be extended to an operational semantics by imposing a call-by-name or call-by-value strategy. In either case, we do not permit reductions under a box constructor, since this would violate its intensional nature.

If we choose a call-by-value strategy, we obtain a natural explanation of computation in multiple stages and, at a lower level, run-time code generation (Davies and Pfenning, 1996; Wickline et al., 1998; Davies and Pfenning, 2000). Alternatively, we can add constructs for pattern matching against an expression. If we also retain extensionality as given by the local expansions, we can obtain a calculus suitable as a meta-logical framework, that is, a logical framework in which we can reason about the specified logics (Despeyroux et al., 1997). The modal operator here serves to avoid the usual paradoxes which would arise if we incorrectly identify an expression with its denotation.

In this paper we have also shown how lax logic can be embedded naturally in modal logic with necessity and possibility. Following work by S. Kobayashi (1997) and Benton, Bierman, and de Paiva (1998), this yields a new formulation of Moggi's monadic metalanguage (1988; 1989; 1991). A possible future direction of research is to try to exploit the additional expressive power afforded by the modal logic as a semantic framework when compared to the monadic metalanguage.

Acknowledgments. We would like to thank two anonymous reviewers for their insightful comments and suggestions.

References

Aczel, P. (1999). The Russel-Prawitz modality. In Fairtlough, M., editor, *Informal Proceedings of the Workshop on Intuitionistic Modal Logics and Applications*, Trento, Italy.

Alechina, N., de Paiva, V., and Ritter, E. (1998). Relating categorical and Kripke semantics for intuitionistic modal logics. In *Proceedings of the Conference on Advances in Modal Logic (AIML'98)*, Uppsala, Sweden. CSLI.

Avron, A., Honsell, F. A., Mason, I. A., and Pollack, R. (1992). Using typed lambda calculus to implement formal systems on a machine. *Journal of Automated Reasoning*, 9(3):309–354. A preliminary version appeared as University of Edinburgh Report ECS-LFCS-87-31.

Benton, P. N., Bierman, G. M., and de Paiva, V. C. V. (1998). Computational types from a logical perspective. *Journal of Functional Programming*, 8(2):177–193.

Bierman, G. and de Paiva, V. (1996). Intuitionistic necessity revisited. Technical Report CSRP-96-10, School of Computer Science, University of Birmingham.

Davies, R. and Pfenning, F. (1996). A modal analysis of staged computation. In Steele, Jr., G., editor, *Proceedings of the 23rd Annual Symposium on Principles of Programming Languages*, pages 258–270, St. Petersburg Beach, Florida. ACM Press.

Davies, R. and Pfenning, F. (2000). A modal analysis of staged computation. *Journal of the ACM*. To appear. Preliminary version available as Technical Report CMU-CS-99-153, August 1999.

Despeyroux, J., Pfenning, F., and Schürmann, C. (1997). Primitive recursion for higher-order abstract syntax. In Hindley, R., editor, *Proceedings of the Third International Conference on Typed Lambda Calculus and Applications (TLCA'97)*, pages 147–163, Nancy, France. Springer-Verlag LNCS 1210. An extended version is available as Technical Report CMU-CS-96-172, Carnegie Mellon University.

Fairtlough, M. and Mendler, M. (1994). An intuitionistic modal logic with application to the formal verification of hardware. In Pacholski, L. and Tiuryn, J., editors, *Proceedings of the 8th Workshop on Computer Science Logic (CSL'94)*, pages 354–368, Kazimierz, Poland. Springer-Verlag LNCS 933.

Fairtlough, M. and Mendler, M. (1997). Propositional lax logic. *Information and Computation*, 137(1):1–33.

Fairtlough, M., Mendler, M., and Walton, M. (1997). First-order lax logic as a framework for constraint logic programming. Technical Report MIP-9714, University of Passau, Passau, Germany.

Gentzen, G. (1935). Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210, 405–431. English translation in M. E. Szabo, editor, *The Collected Papers of Gerhard Gentzen*, pages 68–131, North-Holland, 1969.

Goubault-Larrecq, J. (1996). On computational interpretations of the modal logic S4, parts I–III. Technical Reports 1996-33,34,35, Institut für Logik, Komplexität und Deduktionssysteme, Universität Karlsruhe, Karlsruhe, Germany.

Goubault-Larrecq, J. (1997). On computational interpretations of the modal logic S4, part IIIb. Technical Report 3164, INRIA, France.

Hodas, J. and Miller, D. (1994). Logic programming in a fragment of intuitionistic linear logic.

Information and Computation, 110(2):327–365. A preliminary version appeared in the Proceedings of the Sixth Annual IEEE Symposium on Logic in Computer Science, pages 32–42, Amsterdam, The Netherlands, July 1991.

Kobayashi, S. (1997). Monad as modality. *Theoretical Computer Science*, 175:29–74.

Martin-Löf, P. (1980). Constructive mathematics and computer programming. In *Logic, Methodology and Philosophy of Science VI*, pages 153–175. North-Holland.

Martin-Löf, P. (1994). Analytic and synthetic judgements in type theory. In Parrini, P., editor, *Kant and Contemporary Epistemology*, pages 87–99. Kluwer Academic Publishers.

Martin-Löf, P. (1996). On the meanings of the logical constants and the justifications of the logical laws. *Nordic Journal of Philosophical Logic*, 1(1):11–60.

Martini, S. and Masini, A. (1994). A computational interpretation of modal proofs. In Wansing, H., editor, *Proof Theory of Modal Logics*. Kluwer. Workshop proceedings.

Miculan, M. (1997). *Encoding Logical Theories of Programs*. PhD thesis, Dipartimento di Informatia, Università degli Studi di Pisa.

Moggi, E. (1988). Computational lambda-calculus and monads. Technical Report ECS-LFCS-88-86, University of Edinburgh.

Moggi, E. (1989). Computational lambda calculus and monads. In *Proceedings of the Fourth Symposium on Logic in Computer Science*, pages 14–23, Asilomar, California. IEEE Computer Society Press.

Moggi, E. (1991). Notions of computation and monads. *Information and Computation*, 93(1):55–92.

Pfenning, F. and Wong, H.-C. (1995). On a modal λ-calculus for S4. In Brookes, S. and Main, M., editors, *Proceedings of the Eleventh Conference on Mathematical Foundations of Programming Semantics*, New Orleans, Louisiana. *Electronic Notes in Theoretical Computer Science*, Volume 1, Elsevier.

Prawitz, D. (1965). *Natural Deduction*. Almquist & Wiksell, Stockholm.

Sabry, A. and Wadler, P. (1997). A reflection on call-by-value. *ACM Transactions on Programming Languages and Systems*, 19(6):916–941.

Viganò, L. (1997). *A Framework for Non-Classical Logics*. PhD thesis, Universität des Saarlandes.

Wickline, P., Lee, P., Pfenning, F., and Davies, R. (1998). Modal types as staging specifications for run-time code generation. *ACM Computing Surveys*, 30(3es).