Lecture Notes on
Kripke Semantics for Validity

15-816: Modal Logic
Frank Pfenning

Lecture 16
March 23, 2010

1 Introduction

In this lecture we continue the analysis of distributed computation through modal logic. We give a multiple-worlds interpretation of the modal logic of validity and find that it corresponds to IS4. However, when we generalize this to include possibility, we find that the our inference rules are sound for IS4, but not complete. The counterexamples gives rise to a new form of interpretation of modal logic we develop in the next lecture.

2 Examples in Multiple-World Intuitionistic Modal Logic

We reexamine the earlier examples in light of their proposed interpretation with respect to distributed computation.

$$\begin{array}{rcl} K^\Diamond & : & \Box(A \supset B) \supset (\Diamond A \supset \Diamond B) \mathbin{@} h \\ & = & \lambda x @ h.\, \lambda y @ h.\, \mathbf{let}\, \langle h \leq \alpha \rangle\, z = y\, \mathbf{in}\, \langle h \leq \alpha \rangle ((x\, [h \leq \alpha])\, z) \end{array}$$

The function $K^\Diamond$ takes a mobile function x and a reference to a remote value at some world α, moves x to α, applies it there, and returns a reference to the answer here.

$$\begin{array}{rcl} T^\Box & : & \Box A \supset A \\ & = & \lambda x @ h.\, x\, [h \leq h] \end{array}$$

The function $T^\Box$ takes a mobile value of type A and unpacks it here.

$$\begin{array}{lcl} 4^{\Diamond} & : & \Diamond\Diamond A \supset \Diamond A \\ & = & \lambda x@h.\, \mathbf{let}\, \langle h \leq \alpha \rangle\, y = x\, \mathbf{in}\, \mathbf{let}\, \langle \alpha \leq \beta \rangle\, z = y\, \mathbf{in}\, \langle h \leq \beta \rangle z \end{array}$$

The function $4^{\Diamond}$ takes a reference to a remote reference to a value V of type A at some world β and return a direct reference to V.

3 Non-Local Actions

As discussed at the end of last lecture, disjunction creates the the necessity for an effect at a distance. We write down the substructural operational semantics rules to clarify this. A similar remark applies to falsehood. First we recall the located typing rules.

$$\frac{\Gamma \vdash M : A \mathbin{@} w}{\Gamma \vdash \mathbf{inl}\, M : A \vee B \mathbin{@} w}\, \vee I_1 \qquad \frac{\Gamma \vdash N : B \mathbin{@} w}{\Gamma \vdash \mathbf{inr}\, M : A \vee B \mathbin{@} w}\, \vee I_2$$

$$\frac{\Gamma \vdash M : A \vee B \mathbin{@} w \quad \Gamma, x{:}A@w \vdash N : C \mathbin{@} w'' \quad \Gamma, y{:}B@w \vdash N : C \mathbin{@} w''}{\Gamma \vdash \mathbf{case}\, M\, \mathbf{of}\, \mathbf{inl}\, x \Rightarrow N \mid \mathbf{inr}\, y \Rightarrow O : C \mathbin{@} w''}\, \vee E$$

Next the operational semantics. Observe that in the very first rule (eval/case) there is a non-local transfer of control, from w'' to w, even though w'' and w may not be interaccessible. In order to effect this transfer, the **case** construct should be annotated with the location of M. Then, when the value of M is returned at w, one bit of information need to be communicated from w to w'' so that the appropriate branch (either N or O) can be selected at w''.

$$\begin{array}{lcl} \mathsf{eval/case} & : & \mathsf{eval}\, (\mathbf{case}\, M\, \mathbf{of}\, \mathbf{inr}\, x \Rightarrow N \mid \mathbf{inr}\, y \Rightarrow O)\, w'' \\ & & \quad \twoheadrightarrow \quad \mathsf{eval}\, M\, w \bullet \mathsf{cont}\, (\mathbf{case}\, \_\, \mathbf{of}\, \mathbf{inr}\, x \Rightarrow N \mid \mathbf{inr}\, y \Rightarrow O) \\ \mathsf{eval/inl} & : & \mathsf{eval}\, (\mathbf{inl}\, M')\, w \quad \twoheadrightarrow \quad \mathsf{eval}\, M'\, w \bullet \mathsf{cont}\, (\mathbf{inl}\, \_)\, w \\ \mathsf{eval/inr} & : & \mathsf{eval}\, (\mathbf{inr}\, M')\, w \quad \twoheadrightarrow \quad \mathsf{eval}\, M'\, w \bullet \mathsf{cont}\, (\mathbf{inr}\, \_)\, w \\ \mathsf{cont/inl} & : & \mathsf{ret}\, V'\, w \bullet \mathsf{cont}\, (\mathbf{inl}\, \_)\, w \quad \twoheadrightarrow \quad \mathsf{ret}\, (\mathbf{inl}\, V')\, w \\ \mathsf{cont/inr} & : & \mathsf{ret}\, V'\, w \bullet \mathsf{cont}\, (\mathbf{inr}\, \_)\, w \quad \twoheadrightarrow \quad \mathsf{ret}\, (\mathbf{inr}\, V')\, w \\ \mathsf{ret/inl} & : & \mathsf{ret}\, (\mathbf{inl}\, V')\, w \bullet \mathsf{cont}\, (\mathbf{case}\, \_\, \mathbf{of}\, \mathbf{inr}\, x \Rightarrow N \mid \mathbf{inr}\, y \Rightarrow O)\, w'' \\ & & \quad \twoheadrightarrow \quad !\mathsf{bind}\, x\, V'\, w \bullet \mathsf{eval}\, N\, w'' \\ \mathsf{ret/inr} & : & \mathsf{ret}\, (\mathbf{inr}\, V')\, w \bullet \mathsf{cont}\, (\mathbf{case}\, \_\, \mathbf{of}\, \mathbf{inr}\, x \Rightarrow N \mid \mathbf{inr}\, y \Rightarrow O)\, w'' \\ & & \quad \twoheadrightarrow \quad !\mathsf{bind}\, y\, V'\, w \bullet \mathsf{eval}\, O\, w'' \end{array}$$

If all worlds are interaccessible (that is, we are working in IS5), this is implementable. But this oddity of the operational semantics also has its reflection in the truths we can prove. Consider:

$$\begin{array}{lcl} \Diamond/\vee & : & \Diamond(A \vee B) \supset (\Diamond A \vee \Diamond B) \mathbin{@} h \\ & = & \lambda x @ h.\, \mathbf{let}\, \langle h \leq \alpha \rangle\, x' = x\, \mathbf{in} \\ & & \quad \mathbf{case}\, x'\, \mathbf{of}\, \mathbf{inl}\, y \Rightarrow \langle h \leq \alpha \rangle y \mid \mathbf{inr}\, z \Rightarrow \langle h \leq \alpha \rangle z \end{array}$$

We see that possibility distributes over disjunction without any assumption about accssibility between worlds. For distributed computation, the intution is as follows. We have a remote value of type $A \vee B$. This must be either a left or a right injection of a value of type A or B, respective, so we have a remote value of type A or a remote value of type B.

What is not considered is *why* this information should be available *here*: we have to "peek" at the remote value to see which it is and also bind a new value remotely. And indeed, by invoking the sequent calculus we see that possibility does *not* distribute over disjunction.

$$\frac{\cdot; \Diamond(A \vee B) \Longrightarrow \Diamond A \vee \Diamond B}{\cdot; \cdot \Longrightarrow \Diamond(A \vee B) \supset \Diamond A \vee \Diamond B}\ \supset R$$

At this point in the proof attempt we are stuck, because neither $\Diamond A$ nor $\Diamond B$ can be proved by itself, and the $\Diamond L$ rule is not applicable since the judgment on the right concerns truth rather than possibility.

4 Interpreting Validity

We would hope that the necessity operator $\Box$ that internalizes the validity judgment would coincide with the $\Box$ modality in one of the intuitionistic modal logics we considered in the previous lecture. Instead of guessing a priori what this might be, we just develop it as we try to relate proofs in the earlier judgmental formulation and the multiple-worlds formulation. For this purpose it is convenient to work in the sequent calculus. We therefore present the multiple-worlds sequent calculus in Figure 1. We write $\Gamma^{\leq}$ for the restriction of Γ to assumptions of the form $w \leq w'$. Also note that $w \leq \alpha$ in the context introduces a new α that should be distinct from all other worlds in the antecedent or conclusion. We write $\Gamma^{\leq} \vdash w \leq w'$ if the hypotheses in $\Gamma^{\leq}$ entail that w' is accessible from w according to the current assumptions about the accessibility relation.

How do we now interpret a sequent $\Delta; \Gamma \Longrightarrow A$ from the modal logic of validity? It is pretty easy to see that it should be something like -?-, $\Gamma @ h \Longrightarrow$

$$\frac{P \mathbin{@} w \in \Gamma}{\Gamma \Longrightarrow P \mathbin{@} w}\ \mathsf{init}$$

$$\frac{\Gamma, A@w \Longrightarrow B \mathbin{@} w}{\Gamma \Longrightarrow A \supset B \mathbin{@} w}\ \supset R$$

$$\frac{\Gamma, A \supset B \mathbin{@} w \Longrightarrow A \mathbin{@} w \quad \Gamma, A \supset B \mathbin{@} w, B \mathbin{@} w \Longrightarrow C \mathbin{@} w''}{\Gamma, A \supset B \mathbin{@} w \Longrightarrow C \mathbin{@} w''}\ \supset L$$

$$\frac{\Gamma \Longrightarrow A \mathbin{@} w}{\Gamma \Longrightarrow A \vee B \mathbin{@} w}\ \vee R_1 \qquad \frac{\Gamma \Longrightarrow B \mathbin{@} w}{\Gamma \Longrightarrow A \vee B \mathbin{@} w}\ \vee R_2$$

$$\frac{\Gamma, A \vee B@w, A@w \Longrightarrow C \mathbin{@} w'' \quad \Gamma, A \vee B@w, B@w \Longrightarrow C \mathbin{@} w''}{\Gamma, A \vee B@w \Longrightarrow C \mathbin{@} w''}\ \vee L$$

$$\text{no } \bot R \qquad \frac{}{\Gamma, \bot@w \Longrightarrow C \mathbin{@} w''}\ \bot L$$

$$\frac{\Gamma, w \leq \alpha \Longrightarrow A \mathbin{@} \alpha}{\Gamma \Longrightarrow \Box A \mathbin{@} w}\ \Box R^\alpha \qquad \frac{\Gamma^{\leq} \vdash w \leq w' \quad \Gamma, \Box A \mathbin{@} w, A \mathbin{@} w' \Longrightarrow C \mathbin{@} w''}{\Gamma, \Box A \mathbin{@} w \Longrightarrow C \mathbin{@} w''}\ \Box L$$

$$\frac{\Gamma^{\leq} \vdash w \leq w' \quad \Gamma \Longrightarrow A \mathbin{@} w'}{\Gamma \Longrightarrow \Diamond A \mathbin{@} w}\ \Diamond R \qquad \frac{\Gamma, \Diamond A \mathbin{@} w, w \leq \alpha, A \mathbin{@} \alpha \Longrightarrow C \mathbin{@} w''}{\Gamma, \Diamond A \mathbin{@} w \Longrightarrow C \mathbin{@} w''}\ \Diamond L^\alpha$$

Figure 1: Intuitionistic multiple-worlds sequent calculus

$A \mathbin{@} h$ so that the truth assumptions in Γ and the succedent A are in the same world. The question is how to translation Δ. It is clear that they need to be assumptions about truth of formulas $\Box B_i@w_i$ such that h is reachable from w_i so they can actually be used in the proof of $A \mathbin{@} h$.

First, some notation. For a context $\Gamma = (A_1, \ldots, A_n)$ we write $\Gamma@h = (A_1@h, \ldots, A_n@h)$. Similarly, for a context $\Delta = (B_1, \ldots, B_m)$ and worlds $\vec{w} = (w_1, \ldots, w_m)$ we write $(\Box\Delta)@\vec{w} = (\Box B_1@w_1, \ldots, \Box B_m@w_m)$. We write Ψ for a context of reachability hypotheses and $\Psi \vdash \vec{w} \leq h$ if $\Psi \vdash w_i \leq h$ for all $1 \leq i \leq m$. With this notation we try:

Theorem 1 (Multiple World Semantics of Validity) *If $\Delta; \Gamma \Longrightarrow A$ then for any h, $\vec{w}$, and Ψ such that $\Psi \vdash \vec{w} \leq h$ we have $\Psi, (\Box\Delta)@\vec{w}, \Gamma@h \Longrightarrow A \mathbin{@} h$.*

Proof: By induction on the structure of the given derivation. We show some representative cases.

Case:

$$\frac{P \in \Gamma}{\Delta; \Gamma \Longrightarrow P}\ \mathsf{init}$$

Then

$$\frac{P@h \in \Gamma@h}{\Psi, (\Box\Delta)@\vec{w}, \Gamma@h \Longrightarrow P \mathbin{@} h}\ \mathsf{init}$$

Cases: Other rules that apply (non-modal) left or right rules to A or an assumption in Γ translate directly into the corresponding rules in the multiple-world semantics.

Case:

$$\frac{\Delta', B; \Gamma, B \Longrightarrow A}{\Delta', B; \Gamma \Longrightarrow A}\ \mathsf{valid}$$

Then we construct:

$$\frac{\begin{array}{ll}\text{assumption} & \text{i.h.} \\ \Psi \vdash w \leq h & \Psi, (\Box\Delta')@\vec{w}, \Box B@w, \Gamma@h, B@h \Longrightarrow A \mathbin{@} h\end{array}}{\Psi, (\Box\Delta')@\vec{w}, \Box B@w, \Gamma@h \Longrightarrow A \mathbin{@} h}\ \Box L$$

Case:

$$\frac{\Delta; \bullet \Longrightarrow A'}{\Delta; \Gamma \Longrightarrow \Box A'}\ \Box R$$

Then we construct

$$\frac{\dfrac{\Psi, h \leq \alpha, (\Box\Delta)@\vec{w} \Longrightarrow A \mathbin{@} \alpha}{\Psi, h \leq \alpha, (\Box\Delta)@\vec{w}, \Gamma@h \Longrightarrow A \mathbin{@} \alpha}\ \text{weaken}}{\Psi, (\Box\Delta)@\vec{w}, \Gamma@h \Longrightarrow \Box A \mathbin{@} h}\ \Box R^{\alpha}$$

and $\Psi, h \leq \alpha \vdash \vec{w} \leq \alpha$ by transitivity since $\Psi \vdash \vec{w} \leq h$ by assumption.

Case:

$$\frac{\Delta, B; \Gamma', \Box B \Longrightarrow A}{\Delta; \Gamma', \Box B \Longrightarrow A}\ \Box L$$

Then we construct

$$\dfrac{\overset{\text{i.h.}}{\Psi, (\Box\Delta)@\vec{w}, \Box B@h, \Gamma'@h, \Box B@h \Longrightarrow A \mathbin{@} h}}{\Psi, (\Box\Delta)@\vec{w}, \Gamma'@h, \Box B@h \Longrightarrow A \mathbin{@} h}\ \text{contract}$$

where the induction hypothesis can be applied since $\Psi \vdash \vec{w} \leq h$ by assumption and $\Psi \vdash h \leq h$ by reflexivity. □

We see that proofs in the two systems are closely related. Rules for ordinary intuitionistic connectives are translated one-to-one, and $\Box R$ is mapped to $\Box R$. An application of the judgmental rule valid becomes an application of $\Box L$, and an application of $\Box L$ vanishes in a contraction. We also see that we need transitivity (for $\Box R$) and reflexivity (for $\Box L$), so the appropriate target for the translation is IS4.

We can easily extend this translation to include possibility, which means that the intuitionstic modal logic of validity and possibility is sound with respect to the Kripke semantics IS4 (see Exercise 3).

5 Incompleteness

We have already seen that in the presence of disjunction or falsehood, $\Diamond(A \vee B) \supset \Diamond A \vee \Diamond B$ and $\Diamond\bot \supset \bot$ are true in the Kripke semantics, but not in the logic of possibility. In that sense, the logic of possibility is incomplete for its IS4 semantics.

One may wonder if this is still the case in some fragments. If we consider the pure logic of validity (without $\Diamond$), then the logic of validity is sound and complete with respect to IS4. A proof-theoretic argument for this can be found in [**?**] and it is far from trivial.

What about if we have implication, necessity, and possibility, but not disjunction or falsehood? We can try to reverse the steps of the soundness proof to see where things might go awry. The correspondence for $\Box$ is very close, except that we need weakening in one place ($\Box R$) and contraction in another ($\Box L$). Contraction is a reversible operation, but weakening can not necessarily be reversed. So if we have

$$\dfrac{\Psi, h \leq \alpha, (\Box\Delta)@\vec{w}, \Gamma@h \Longrightarrow A \mathbin{@} \alpha}{\Psi, (\Box\Delta)@\vec{w}, \Gamma@h \Longrightarrow \Box A \mathbin{@} h}\ \Box R^{\alpha}$$

and compare to

$$\frac{\Delta; \bullet \Longrightarrow A}{\Delta; \Gamma \Longrightarrow \Box A}\ \Box R$$

the question is whether we can strengthen the premise to

$$\Psi, h \leq \alpha, (\Box\Delta)@\vec{w} \Longrightarrow A \mathbin{@} \alpha?$$

In other words, is there any way that the assumptions $\Gamma@h$ can still be used after we move to a new world α?

Certainly, this seems possible. For example, Γ coould contain assumptions $B \supset \Box C@h$ and $B@h$. So, when we start from the multiple-worlds proof, it is not straightforward to construct the proof using validity.

We can use this insight to construct a counterexample to the completeness of the rules for validity relative to IS4 even with just implication, necessity, and possibly. Consider

$$(\Diamond A \supset \Box B) \supset \Box(A \supset B)$$

We give a sequent derivation using worlds, where we assume A and B are atomic and elide hypotheses unused hypotheses.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{h \leq \alpha \vdash h \leq \alpha}\quad\dfrac{}{A@\alpha \Longrightarrow A \mathbin{@} \alpha}\ \textsf{init}}{h \leq \alpha, A@\alpha \Longrightarrow \Diamond A \mathbin{@} h}\ \Diamond R\quad\dfrac{\dfrac{}{h \leq \alpha \vdash h \leq \alpha}\quad\dfrac{}{B@\alpha \Longrightarrow B \mathbin{@} \alpha}\ \textsf{init}}{h \leq \alpha, \Box B@h \Longrightarrow B \mathbin{@} \alpha}\ \Box L}{\Diamond A \supset \Box B@h, h \leq \alpha, A@\alpha \Longrightarrow B \mathbin{@} \alpha}\ \supset L}{\Diamond A \supset \Box B@h, h \leq \alpha \Longrightarrow A \supset B \mathbin{@} \alpha}\ \supset R}{\Diamond A \supset \Box B@h \Longrightarrow \Box(A \supset B) \mathbin{@} h}\ \Box R^{\alpha}}{(\Diamond A \supset \Box B) \supset \Box(A \supset B) \mathbin{@} h}\ \supset R$$

Note that we use no property of accessibility, so the above is a theorem in all modal logics given via a multiple-world semantics. It exploits precisely the failure of strengthening after the $\Box R^{\alpha}$ rule: the assumption $\Diamond A \supset \Box B$ is used in an essential way above that inference.

On the other hand, $(\Diamond A \supset \Box B) \supset \Box(A \supset B)$ it is not a theorem of the logic of validity and possibility, because introducing the $\Box$ on the right-hand side will wipe out the context and the hypothesis $(\Diamond A \supset \Box B)$. Hence the rules are incomplete with respect to IS4.

6 Axiomatic Presentations of Modal Logic Revisited

We now review the axiomatic presentation of various intuitionistic modal logics. First, we have the axioms for intuitionistic logic and the rule of modus ponens, which we don't review here. We refer to the modal logic of validity and possibility as JS4 (called *judgmental S4*). In addition we have the rule of necessitation

$$\frac{\vdash A}{\vdash \Box A}\ \mathsf{nec}$$

and the following axioms, with the accessibility property and the logics in which they hold:

$K^{\Box}$	:	$\Box(A \supset B) \supset (\Box A \supset \Box B)$	none	IK, JS4
$K^{\Diamond}$	:	$\Box(A \supset B) \supset (\Diamond A \supset \Diamond B)$	none	IK, JS4
$T^{\Box}$	:	$\Box A \supset A$	reflexivity	IS4, IS5, JS4
$T^{\Diamond}$	:	$A \supset \Diamond A$	reflexivity	IS4, IS5, JS4
$4^{\Box}$	:	$\Box A \supset \Box\Box A$	transitivity	IS4, IS5, JS4
$4^{\Diamond}$	:	$\Diamond\Diamond A \supset \Diamond A$	transitivity	IS4, IS5, JS4
$5^{\Diamond\Box}$	:	$\Diamond\Box A \supset \Box A$	symmetry	IS5
$5^{\Box\Diamond}$	:	$\Diamond A \supset \Box\Diamond A$	symmetry	IS5

In addition we have, in all intuitionistic Kripke-modal logics, but *not* in the logics of validity and possibility (JS4):

$\Diamond/\vee$	:	$\Diamond(A \vee B) \supset \Diamond A \vee \Diamond B$	IK, IS4, IS5
$\Diamond/\bot$	:	$\Diamond\bot \supset \bot$	IK, IS4, IS5
$\Diamond/\supset$	:	$(\Diamond A \supset \Box B) \supset \Box(A \supset B)$	IK, IS4, IS5

That fact that these axioms are sound and complete with respect to the definition of the various logic via natural deduction using explicit worlds is given by Simpson [**?**]. The soundness and completeness of the axioms for JS4 was proven in Lecture 9.

Exercises

Exercise 1 *Prove that the intuitionistic modal sequent calculus with multiple worlds satisfies identity and cut.*

Exercise 2 *Formulate and prove the relationship between the intuitionistic modal sequent calculus with multiple worlds and intuitionistic natural deduction with multiple worlds. You may use identity and cut from Exercise 1 as needed.*

Exercise 3 *Prove that the rules for possibility are sound under the interpretation into IS4 given in Section 4.*

Exercise 4 *Write out the proof term for* $(\Diamond A \supset \Box B) \supset \Box(A \supset B)$ @ h *and give its operational interpretation.*

Exercise 5 *Write out the proof terms for* $5^{\Box\Diamond}$ *and* $5^{\Diamond\Box}$ *and give their operational interpretation as programs.*

References

[DP01] Rowan Davies and Frank Pfenning. A modal analysis of staged computation. *Journal of the ACM*, 48(3):555–604, May 2001.

[Sim94] Alex K. Simpson. *The Proof Theory and Semantics of Intuitionistic Modal Logic*. PhD thesis, University of Edinburgh, 1994.