

CL 2002:

Computational Logic

(Lecture 10)

Sergei N. Artemov

November 26, 2002

*Computer Science Program
CUNY Graduate Center*

This lecture plan

1. Modal logic: time and knowledge
2. Basic systems of modal logic
3. Possible worlds semantics
4. Gentzen style proof systems for modal logics
5. Cut-elimination and completeness theorem for **S4**
6. Gödel's embedding of **Int** into **S4**

Modal logic: time and knowledge

Propositional logic is decidable but too restrictive. First order and higher order logics have unlimited expressive power but are not decidable. Modal logic appeared as an attempt to extend propositional logic by additional connectives preserving certain nice features like decidability.

Minimal format: propositional connectives plus unary connective “modality” \Box . Intended readings of new atoms $\Box F$ are

1. Epistemic - existential: “ F is known”, “ F is provable”, etc,
2. Temporal - universal: “ F holds in all possible situations”, “in the future F will always hold”, etc.

Usually preserves decidability.

History and Applications

McKinsey-Tarski (1948): topological semantics $\Box F = \text{interior}(F)$, provides a mathematical model for intuitionism, logic of approximate measurements, leads to logics for dynamic systems, etc.

Kripke (1959): possible worlds à la Leibniz, by far the most widely used semantics.

Hoare (1969): partial correctness statements $A\{G\}B = \text{“if } A \text{ holds before the execution of } G \text{ then } B \text{ holds afterward”}$, a classic of program verification. Recently Tony Hoare was knighted by the British Queen.

Pratt (1976): logic of programs, $[C]\varphi = \varphi$ holds while C is executed, each $[C]$ is an **S4**-modality. Kripke style semantics where possible worlds are machine states. Stanford University Network = (SUN).

Pnueli (1977): branching temporal logic = logic of concurrency. The language of verification and model checking. Turing award in CS.

Logic of Knowledge: *a core AI topic, $K_A(\varphi) = \text{“agent } A \text{ knows } \varphi\text{”}, \text{ multiple modalities.}$*

Joe Halpern (1990s): Common knowledge operator cannot be expressed via individual knowledge operators. Problem: build a logic of knowledge that distinguishes hard and easy problems. Prime factorization example.

Basic systems of modal logic

System **K**:

A1. *Propositional axioms and rules*

A2. $\Box(F \rightarrow G) \rightarrow (\Box F \rightarrow \Box G)$ *(distribution)*

Nec. Necessitation rule: $\frac{\vdash F}{\vdash \Box F}$

System **K4** is **K** +

A3. $\Box F \rightarrow \Box \Box F$ *(positive introspection/transitivity)*

System **S4** is **K4** +

A4. $\Box F \rightarrow F$ *(reflexivity)*

System **S5** is **S4** +

A5. $\neg \Box F \rightarrow \Box(\neg \Box F)$ *(negative introspection)*

Some of derivations in \mathbf{K} (hence in all other modal logics).

Theorem: \Box and \wedge commute

$$\begin{array}{ll} A \rightarrow (B \rightarrow A \wedge B) & A \wedge B \rightarrow A \\ \Box(A \rightarrow (B \rightarrow A \wedge B)) & \Box(A \wedge B \rightarrow A) \\ \Box A \rightarrow \Box(B \rightarrow A \wedge B) & \Box(A \wedge B) \rightarrow \Box A \\ \Box A \rightarrow (\Box B \rightarrow \Box(A \wedge B)) & \Box(A \wedge B) \rightarrow \Box B \\ (\Box A \wedge \Box B) \rightarrow \Box(A \wedge B) & \Box(A \wedge B) \rightarrow (\Box A \wedge \Box B) \end{array}$$

Theorem: \Box factors out through \vee :

$$\begin{array}{l} A \rightarrow A \vee B \\ \Box(A \rightarrow A \vee B) \\ \Box A \rightarrow \Box(A \vee B) \\ \Box B \rightarrow \Box(A \vee B) \\ (\Box A \vee \Box B) \rightarrow \Box(A \vee B) \end{array}$$

But not $\Box(A \vee B) \rightarrow (\Box A \vee \Box B)$!
Consider B to be $\neg A$. Whatever intended reading of modality you take $\Box(A \vee \neg A) \rightarrow (\Box A \vee \Box \neg A)$ cannot be valid.

Modality dual to \Box : $\Diamond F \equiv \neg\Box\neg F$.

Intended semantics is derivative from the one for $\Box F$:

if $\Box F$ denotes “ F holds in all possible situations”,
then $\Diamond F$ stands for “ F holds in at least one possible situation”

(the latter has been usually described as $\Box F$ denotes “ F is necessary” and $\Diamond F$ stands for “ F is possible”)

Exercise: $\mathbf{S4} \vdash A \rightarrow \Diamond A$ (thus $\mathbf{S4} \vdash \Box A \rightarrow \Diamond A$).

Indeed: $\mathbf{S4} \vdash \Box\neg A \rightarrow \neg A$, $\mathbf{S4} \vdash \neg\neg A \rightarrow \neg\Box\neg A$, $\mathbf{S4} \vdash A \rightarrow \neg\Box\neg A$.

In many respects modal logics behave like normal logical systems. In particular, they are closed under substitution:

If $\Gamma(p) \vdash F(p)$ then $\Gamma(p/A) \vdash F(p/A)$ for any A

Modal logics admit equivalent substitution:

*For **L=K**, **K4**, **S4**, **S5**, if $\mathbf{L} \vdash A \Leftrightarrow B$ then $\mathbf{L} \vdash F(p/A) \Leftrightarrow F(p/B)$ for any formula $F(p)$*

NOTE: Deduction Theorem fails for **L=K**, **K4**, **S4**, **S5**. Indeed, in all of those logics $A \vdash \Box A$, by Necessitation, however, none of them derives $A \rightarrow \Box A$. To prove that we need to develop some sort of negative test for **L**, for example, some sort of formal semantics true/false in a certain class of models along with a corresponding *soundness theorem*. Then by showing that F is false we can establish that F is not derivable.

One more example:

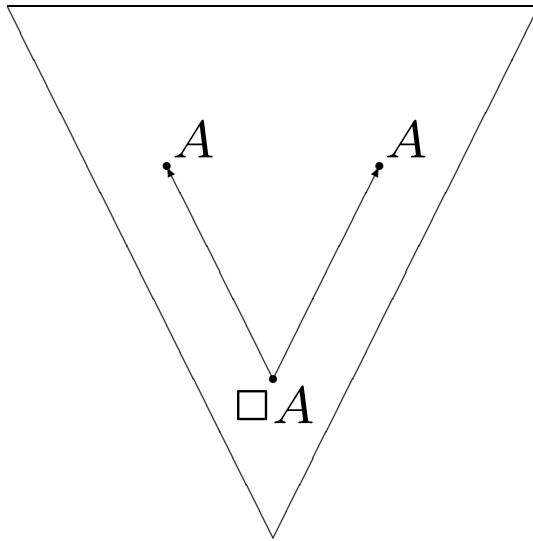
Derivation in **K4**, **S4**, **S5** that $F \rightarrow \Box F$ holds not only for $F \equiv \Box A$ (transitivity axiom), but for $F \equiv \Box A \vee \Box B$ as well.

$$\begin{aligned} & \Box A \rightarrow \Box A \vee \Box B \\ & \Box(\Box A \rightarrow \Box A \vee \Box B) \\ & \Box A \rightarrow \Box \Box A \\ & \Box \Box A \rightarrow \Box(\Box A \vee \Box B) \\ & \Box A \rightarrow \Box(\Box A \vee \Box B) \\ & \Box B \rightarrow \Box A \vee \Box B \\ & \Box(\Box B \rightarrow \Box A \vee \Box B) \\ & \Box B \rightarrow \Box \Box B \\ & \Box \Box B \rightarrow \Box(\Box A \vee \Box B) \\ & \Box B \rightarrow \Box(\Box A \vee \Box B) \\ & \Box A \vee \Box B \rightarrow \Box(\Box A \vee \Box B) \end{aligned}$$

Possible Worlds Semantics by Saul Kripke.

Classical logic, propositional and quantified alike, gives a static picture of the world. A classical interpretation (model) is an assignment of truth values to atoms of the language. Modal logic has a striking ability to capture adequately a very natural semantics of “possible worlds” which can be traced back to Leibniz. The possible worlds universe consists of a collection of classical models W connected by a binary accessibility relation $R(a, b)$ “world b is accessible from world a ”. In other words, the possible worlds constitute an ordered graph, not necessarily finite. Whereas classical connectives operate within individual worlds (i.e. nodes in W), modality reaches out to all the worlds accessible from a given one (possible worlds):

$\Box F$ holds in a iff F holds in all b 's accessible from a .



Model Kripke is a triple $K = (W, R, \models)$, where W is a nonempty set (elements of which are called “possible worlds”), R a binary relation on W , and \models a truth assignment having form: “world \models formula” such that each propositional letter gets some truth value in any world from W . We assume also that for any $x \in W$ both $x \models \text{true}$ and $x \not\models \text{false}$.

The definition of $x \models F$ (read as *a formula F is true in a world x , or x forces F*) goes by induction on F :

$x \models A \wedge B$ iff “ $x \models A$ and $x \models B$ ”

$x \models A \vee B$ iff “ $x \models A$ or $x \models B$ ”

$x \models \neg A$ iff “ $x \not\models A$ ”

$x \models \Box A$ iff “ $y \models A$ for all y such that $R(x, y)$ ”

By default, we assume that $A \rightarrow B$ stands for $\neg A \vee B$, thus imposing the classical truth tables on boolean connectives at every given node. From the definition it is clear that a Kripke model is a collection of classical models connected by some sort of binary “accessibility” relation.

Modality \Box is the only connective able to reach out to other possible worlds, i.e. nodes of the model accessible from a given one.

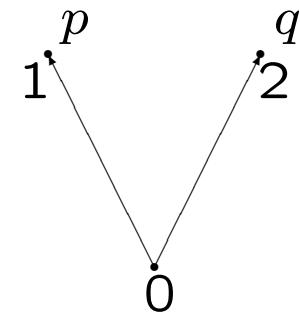
We may regard $\Box F$ as a sort of restricted universal quantifier “for all possible worlds F holds”. It turns out that such limited quantification enables us to express some important features like time and process termination without compromising the decidability of the propositional logic.

$\Diamond F$ holds in x iff F holds in some y accessible from x .

Example

Consider a three-element “V-shaped” model with $W = \{0, 1, 2\}$ given by an oriented graph below. According to this graph, $R(0, 1)$, $R(0, 2)$, and neither of $R(1, 2)$, $R(2, 1)$, $R(1, 0)$, $R(2, 0)$, $R(0, 0)$, $R(1, 1)$, $R(2, 2)$ holds.

Notational convention: we label the nodes with propositional variables true at a given node. By default, all variables not listed next to a node are assumed false at this node. In particular, $1 \models p$, $2 \models q$, $1 \not\models q$, $2 \not\models p$, $0 \not\models p$, $0 \not\models q$, and all other variables are false at all nodes.



Question: for each of the formulas $\Box p$, $\Box q$, $\Box(p \wedge q)$, $\Box p \wedge \Box q$, $\Box(p \vee q)$, $\Box p \vee \Box q$, list the nodes where this formula is true.

Answer:

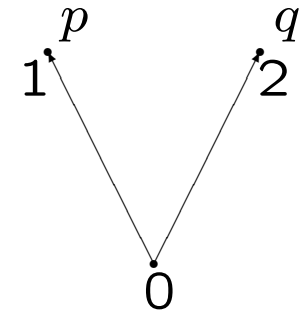
$\Box p$ is true at 1 and 2, but not at 0. Indeed, the set of accessible worlds for either 1 or 2 is empty, thus *FOR ALL* worlds accessible from each of them p holds. $\Box p$ is false at 0, since p fails at 2 which is accessible from 0.

Likewise, $\Box q$ holds at 1 and 2, but not in 0.

Formula $p \wedge q$ is false at every node. Formula $\Box(p \wedge q)$ is true at 1 and 2, but not at 0, so do $\Box p \wedge \Box q$ and $\Box p \vee \Box q$.

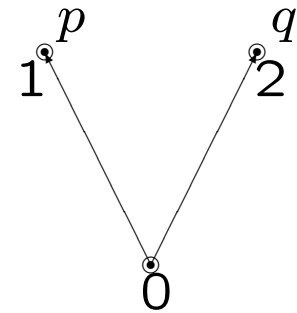
Formula $p \vee q$ is true at 1 and 2, but not at 0. Formula $\Box(p \vee q)$ is true at every node. Indeed, it is true at 1 and 2 by trivial reasons (above), hence it also true at 0, since $p \vee q$ is true at every possible world for it.

Note, that $0 \not\models \Box(p \vee q) \rightarrow (\Box p \vee \Box q)$!. Hence we have found a model where this formula fails.



Truth value of a modal formula very much depends upon specific details of accessibility relation.

For example, consider the same model as above, but with all nodes made *reflexive*, i.e. $R(0,0)$, $R(1,1)$, and $R(2,2)$ (we denote reflexive worlds by “circled” nodes, as on the picture). The same formulas now have quite a different meaning.



In particular, $\Box p$ is true at 1, but not at 0 and 2. Likewise, $\Box p$ is true at 2, but not at 0 and 1.

It turned out that each of the modal logics under consideration is complete with respect to a corresponding class of Kripke models which can be characterized by the property of accessibility relation only.

Definition. A formula F is true in a model K (notation: $K \models F$) if F holds at every node of K . A formula F is valid (in a given class of models) if it is true in every model (of this class).

Consolidated Soundness Theorem

- If $\mathbf{K} \vdash F$ then F is valid in all models.
- If $\mathbf{K4} \vdash F$ then F is valid in all transitive models.
- If $\mathbf{S4} \vdash F$ then F is valid in all transitive reflexive models.
- If $\mathbf{S5} \vdash F$ then F is valid in all transitive reflexive symmetric models .

Proof. A pretty straightforward induction on the length of derivation in a given logic. We first prove that axioms are true in every model. Then we check that rules when applied to formulas true in all models (of a given class) produce a formula true in every such model as well.

Soundness of \mathbf{K} .

A1. Propositional axioms

are true at every node since each node is a classical model.

A2. $\Box(F \rightarrow G) \rightarrow (\Box F \rightarrow \Box G)$ (distribution)

We have to prove that A2 is true at every node x of every model. Suppose $x \models \Box(F \rightarrow G)$ and $x \models \Box F$, then for every y accessible from x both $F \rightarrow G$ and F hold, hence G does. Since G holds for every y accessible from x , the formula $\Box G$ holds at x .

Modus Ponens: $\frac{F \rightarrow G, F}{G}$. Obviously holds at each node.

Nec.: $\frac{\vdash F}{\vdash \Box F}$

By contrapositive, suppose there is a model K , where $\Box F$ is false at some node x . Then there should be a node y (accessible from x), where F is false. Therefore, F is false in K .

Soundness of **K4**

A3. $\Box F \rightarrow \Box\Box F$ *(positive introspection/transitivity)*

Suppose $x \models \Box F$. In order to establish that $x \models \Box\Box F$ consider any y accessible from x and check that $y \models \Box F$. To do this, we have to consider any z accessible from y and prove that $z \models F$. The latter holds since z is also accessible from x (transitivity!), and thus $x \models \Box F$ yields $z \models F$.

Soundness of **S4**

A4. $\Box F \rightarrow F$ *(reflexivity)*

Suppose $x \models \Box F$. Then $y \models F$ for all y accessible from x , in particular, for $y = x$. Thus $x \models F$.

Soundness of **S5**

A5. $\neg\Box F \rightarrow \Box(\neg\Box F)$ *(negative introspection)*

Suppose $x \models \neg\Box F$, then $y \not\models F$ for some y accessible from x . In order to establish that $x \models \Box\neg\Box F$ consider any z accessible from x and check that $z \models \neg\Box F$. Since accessibility here is symmetric, x is accessible from z . By transitivity, y is also accessible from z . Thus we have found a node y accessible from z and such that $y \not\models F$. Thus $z \models \neg\Box F$.

To show that $p \rightarrow \Box p$ is not derivable in modal logic, it now suffices to build a countermodel $K = (W, R, \models)$ for this formula. Consider $W = \{0, 1\}$ and let accessibility be a complete graph on W , i.e. $R(0,0), R(0,1), R(1,0), R(1,1)$. Put $0 \models p$ and $1 \not\models p$. Clearly, K is a legitimate **S5** model, since R is an equivalence relation on W .

Moreover, $0 \models p$, but $0 \not\models \Box p$, since $1 \not\models p$ and 1 is accessible from 0 . Therefore, $0 \not\models p \rightarrow \Box p$.

By the soundness theorem, **S5** $\not\vdash p \rightarrow \Box p$, thus none of the other logics **K**, **K4**, **S4** does.

Completeness Theorem

- $\mathbf{K} \vdash F$ iff F is valid in all models.
- $\mathbf{K4} \vdash F$ iff F is valid in all transitive models.
- $\mathbf{S4} \vdash F$ iff F is valid in all transitive reflexive models.
- $\mathbf{S5} \vdash F$ iff F is valid in all transitive reflexive symmetric models .

Proof. By the maximal consistent sets construction (sometimes called *canonical model*). We will establish completeness of $\mathbf{S4}$ along with cut-elimination below.

Exercise. Prove that all logics \mathbf{K} , $\mathbf{K4}$, $\mathbf{S4}$, $\mathbf{S5}$ are distinct. Hint: show that each next axiom is not derivable in the previous system, use models.

Gentzen style proof systems contain the usual classical rules and modal rules for **K**:

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

for **K4**:

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

Gentzen style proof system for **S4** is called **S4G** and contains the classical rules plus two modal rules

$$\frac{A, \Gamma \Rightarrow \Delta}{\Box A, \Gamma \Rightarrow \Delta} (\Box \Rightarrow)$$

and

$$\frac{\Box \Gamma \Rightarrow A}{\Box \Gamma \Rightarrow \Box A} (\Rightarrow \Box)$$

where $(\Box\{A_1, \dots, A_n\} = \{\Box A_1, \dots, \Box A_n\})$.

By **S4**⁻ we mean the system **S4** without cut rule.

Consolidated Completeness Theorem for **S4**

The following are equivalent

1. **S4G**⁻ ⊢ $\Gamma \Rightarrow \Delta$
2. **S4G** ⊢ $\Gamma \Rightarrow \Delta$
3. **S4** ⊢ $\bigwedge \Gamma \Rightarrow \bigvee \Delta$
4. $\bigwedge \Gamma \Rightarrow \bigvee \Delta$ *is true at a every **S4**-model.*
5. $\bigwedge \Gamma \Rightarrow \bigvee \Delta$ *is true at a every finite **S4**-model.*

Corollary for **S4:** Kripke completeness, cut elimination, equivalence of Gentzen Hilbert systems, finite model property.

Proof. $1 \Rightarrow 2$ and $4 \Rightarrow 5$ are trivial, $2 \Rightarrow 3$ is an easy exercise, $3 \Rightarrow 4$ is the soundness theorem shown above. It suffices now to show $5 \Rightarrow 1$. The latter is proven by the contrapositive: if $\mathbf{S4G}^- \not\vdash \Gamma \Rightarrow \Delta$, then $\bigwedge \Gamma \Rightarrow \bigvee \Delta$ has a finite **S4**-countermodel.

(The proof is given in class)

Gödel's embedding of **Int** into **S4**:

1. translate **Int**-formula F into a classical language \square :

$$tr(F) = \text{“box each subformula of } F\text{”},$$

2. test the translation in **S4**.

Theorem (Gödel (1933), McKinsey & Tarski (1948))

$$\mathbf{Int} \text{ proves } F \Leftrightarrow \mathbf{S4} \text{ proves } tr(F)$$

Proof. Given in class.

The mission of building *BHK* semantics has not been accomplished yet, since **S4** itself still has not been given an exact provability model

$$\mathbf{Int} \hookrightarrow \mathbf{S4} \hookrightarrow ? \hookrightarrow \mathit{REAL\ PROOFS}$$