General methods in proof theory for modal logic - Lecture 1

Björn Lellmann and Revantha Ramanayake

TU Wien

Tutorial co-located with TABLEAUX 2017, FroCoS 2017 and ITP 2017
September 24, 2017. Brasilia.

Outline of the tutorial

Lecture 1 An introduction to proof theory via the sequent calculus, and an introduction to normal modal logics defined via syntax and relational semantics.

Lecture 2 Limits of the sequent framework. Case study $S5$. No cutfree sequent calculus, but a hypersequent calculus

Lecture 3 Proof theoretic methods case study: cut-elimination methods for provability logics. The sequent calculus is not enough: other proof-theoretic formalisms (labelled, nested, display calculus) for obtaining analytic calculi for modal logics.

Lecture 4 Non-normal logics (and their neighbourhood semantics). Ackermann's lemma/Tseitin transformation to obtain logical rules. Case study: Mimamsa Deontic Logic.

Proof theory

- Proof theory treats a proof as a formal mathematical object, facilitating its analysis, and also the study of the provability relation, by mathematical techniques.
- A proof is typically defined by first defining a proof system
- Our emphasis is on structural proof theory: the study of various proof systems for logics and their structural properties, and using the proof system to study the logic of interest.
- There are essentially two degrees of freedom here: choose the logic and then choose/construct a proof system for the logic
- To begin with, let's start with a very familiar logic: propositional classical logic **Cp**. Classical logic consists of the set of formulae with evaluate to $\top$ under the usual truth table semantics.
- Let us introduce a proof system for it. This proof system is called a Hilbert calculus...

The Hilbert calculus **hCp** for classical logic **Cp**

- Classical language: countable set of propositional variables $p_1, p_2, \ldots$ and logical connectives $\to, \neg, \wedge, \vee, \bot, \top$.
- Every propositional variable and $\bot$ and $\top$ is a formula. If A and B are formulae, then so are $A \to B$, $\neg A$, $A \wedge B$, $A \vee B$
- The Hilbert calculus **hCp** consists of the following axiom schemata (schematic variable $\mathcal{A}, \mathcal{B}, \mathcal{C}$ stand for formulae):

Ax 1: $\mathcal{A} \to (\mathcal{B} \to \mathcal{A})$

Ax 2: $(\mathcal{A} \to (\mathcal{B} \to \mathcal{C})) \to ((\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to \mathcal{C}))$

Ax 3: $(\neg\mathcal{A} \to \neg\mathcal{B}) \to ((\neg\mathcal{A} \to \mathcal{B}) \to \mathcal{A})$

and other axioms for $\wedge, \vee, \top, \bot$ (omitted for brevity)

and a single rule called *modus ponens*:

$$\frac{\mathcal{A} \qquad \mathcal{A} \to \mathcal{B}}{\mathcal{B}}\ \text{MP}$$

Derivation of $A \to A$

Definition (derivation)

A formal proof or derivation of B is the finite sequence $C_1, C_2, \ldots, C_n \equiv B$ of formulae where each element C_j is an axiom instance or follows from two earlier elements by modus ponens.

$$\begin{array}{ll} \text{Ax 1:} & \mathcal{A} \to (\mathcal{B} \to \mathcal{A}) \\ \text{Ax 2:} & (\mathcal{A} \to (\mathcal{B} \to \mathcal{C})) \to ((\mathcal{A} \to \mathcal{B}) \to (\mathcal{A} \to \mathcal{C})) \\ \text{Ax 3:} & (\neg\mathcal{A} \to \neg\mathcal{B}) \to ((\neg\mathcal{A} \to \mathcal{B}) \to \mathcal{A}) \\ \text{MP:} & \mathcal{A} \quad \mathcal{A} \to \mathcal{B} / \mathcal{B} \end{array}$$

1	$((A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A)))$	Ax 2
2	$(A \to ((A \to A) \to A))$	Ax 1
3	$((A \to (A \to A)) \to (A \to A))$	MP: 1 and 2
4	$(A \to (A \to A))$	Ax 1
5	$A \to A$	MP: 3 and 4

A drawback of the Hilbert calculus: derivations lack a discernible structure

- Consider the derivation of $A \to A$:

1	$((A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A)))$	Ax 2
2	$(A \to ((A \to A) \to A))$	Ax 1
3	$((A \to (A \to A)) \to (A \to A))$	MP: 1 and 2
4	$(A \to (A \to A))$	Ax 1
5	$A \to A$	MP: 3 and 4

What is the relation of the derivation to $A \to A$? How could we construct its derivation? Is there an algorithm? and if so, what is its complexity? Is there a derivation of $(p \to p) \to \neg(p \to p)$?

There is no obvious structural relationship between $A \to A$ and its derivation (and MP is the culprit)

A new proof system: the sequent calculus **sCp**

$$\frac{}{p, X \vdash Y, p}\ \text{init} \qquad \frac{}{\bot, X \vdash Y}\ \bot\text{l} \qquad \frac{}{X \vdash Y, \top}\ \top\text{r}$$

$$\frac{X \vdash Y, A}{\neg A, X \vdash Y}\ \neg l \qquad \frac{A, X \vdash Y}{X \vdash Y, \neg A}\ \neg r$$

$$\frac{A, B, X \vdash Y}{A \wedge B, X \vdash Y}\ \wedge l \qquad \frac{X \vdash Y, A \qquad X \vdash Y, B}{X \vdash Y, A \wedge B}\ \wedge r$$

$$\frac{A, X \vdash Y \qquad B, X \vdash Y}{A \vee B, X \vdash Y}\ \vee l \qquad \frac{X \vdash Y, A, B}{X \vdash Y, A \vee B}\ \vee r$$

$$\frac{X \vdash Y, A \qquad B, X \vdash Y}{A \to B, X \vdash Y}\ \to l \qquad \frac{A, X \vdash Y, B}{X \vdash Y, A \to B}\ \to\text{r}$$

- No axioms, only rules built from sequents of the form $X \vdash Y$
- X, Y are multiset of formulae)
- X is the antecedent, Y the succedent
- Aside: original sequent calculus presented in Gentzen's (1935) highly readable work

$$\frac{}{p, X \vdash Y, p}\ \text{init} \qquad \frac{}{\bot, X \vdash Y}\ \bot\text{l} \qquad \frac{}{X \vdash Y, \top}\ \top\text{r}$$

$$\frac{X \vdash Y, A}{\neg A, X \vdash Y}\ \neg l \qquad \frac{A, X \vdash Y}{X \vdash Y, \neg A}\ \neg r$$

$$\frac{A, B, X \vdash Y}{A \wedge B, X \vdash Y}\ \wedge l \qquad \frac{X \vdash Y, A \qquad X \vdash Y, B}{X \vdash Y, A \wedge B}\ \wedge r$$

$$\frac{A, X \vdash Y \qquad B, X \vdash Y}{A \vee B, X \vdash Y}\ \vee l \qquad \frac{X \vdash Y, A, B}{X \vdash Y, A \vee B}\ \vee r$$

$$\frac{X \vdash Y, A \qquad B, X \vdash Y}{A \to B, X \vdash Y}\ \to l \qquad \frac{A, X \vdash Y, B}{X \vdash Y, A \to B}\ \to\text{r}$$

- Above the line are premises and below is the conclusion
- A 0-premise rule is called an initial sequent
- A derivation in the sequent calculus is an initial sequent or a rule applied to derivations of the premise(s).
- A derivation can be viewed a tree with vertices labelled by sequents. The root is the endsequent

$$\frac{}{p, X \vdash Y, p}\ \text{init} \qquad \frac{}{\bot, X \vdash Y}\ \bot\text{l} \qquad \frac{}{X \vdash Y, \top}\ \top\text{r}$$

$$\frac{X \vdash Y, A}{\neg A, X \vdash Y}\ \neg l \qquad \frac{A, X \vdash Y}{X \vdash Y, \neg A}\ \neg r$$

$$\frac{A, B, X \vdash Y}{A \wedge B, X \vdash Y}\ \wedge l \qquad \frac{X \vdash Y, A \qquad X \vdash Y, B}{X \vdash Y, A \wedge B}\ \wedge r$$

$$\frac{A, X \vdash Y \qquad B, X \vdash Y}{A \vee B, X \vdash Y}\ \vee l \qquad \frac{X \vdash Y, A, B}{X \vdash Y, A \vee B}\ \vee r$$

$$\frac{X \vdash Y, A \qquad B, X \vdash Y}{A \to B, X \vdash Y}\ \to l \qquad \frac{A, X \vdash Y, B}{X \vdash Y, A \to B}\ \to\text{r}$$

- A principal formula is the formula containing the newly introduced logical connective
- The auxiliary formula(e) are the formulae in the premises
- The multisets X and Y are the context

A derivation in **sCp**

$$
\cfrac{\cfrac{\cfrac{A, A \to (B \to C) \vdash C, A \qquad \cfrac{B, A \vdash C, A \qquad \cfrac{B, A \vdash C, B \qquad C, B, A \vdash C}{B \to C, B, A \vdash C}\;{\to}\mathrm{l}}{B, A, A \to (B \to C) \vdash C}\;{\to}\mathrm{l}}{A, A \to B, (A \to (B \to C)) \vdash C}\;{\to}\mathrm{l}}{\cfrac{A \to B, (A \to (B \to C)) \vdash A \to C}{(A \to (B \to C)) \vdash (A \to B) \to (A \to C)}\;{\to}\mathrm{r}}\;{\to}\mathrm{r}}{\vdash (A \to (B \to C)) \to ((A \to B) \to (A \to C))}\;{\to}\mathrm{r}
$$

- Actually, the above is not yet a derivation. Recall that the initial sequents have the form $p, X \vdash Y, p$ *not* $A, X \vdash Y, A$.
- The height of a derivation is the maximal number of sequents on a branch in the derivation.
- The size of a formula is the number of connectives in it plus one. Another useful representation of a formula is in terms of its grammar tree.
- Note that $A, X \vdash Y, A$ is derivable: Argument by induction on the size of a formula. The base case (A is a propositional variable) is already an initial sequent!

(Height-preserving) admissibility and invertibility

- A rule r is admissible in **sCp** if the conclusion of the rule is derivable whenever the premise(s) are derivable.
- If the height of the derivation of the conclusion is no greater than the height of the premise(s), then r is height-preserving admissible in **sCp**
- A rule r of **sCp** is invertible: if a sequent instantiating conclusion is derivable, then the corresponding sequents instantiating premise(s) are derivable. If the latter have height no greater than the former then it is height-preserving
- The weakening rules lw and rw are height-preserving admissible

$$\frac{X \vdash Y}{A, X \vdash Y}\,\text{lw} \qquad \frac{X \vdash Y}{X \vdash Y, A}\,\text{rw}$$

  Suppose we are given a derivation d of $X \vdash Y$. Induction on the height of d. Consider the last rule r. Insert A into premise of r via IH, and hence obtain A in conclusion.
- The induction argument is simply the method of proving result. Picture the transformation of d.

(Height-preserving) admissibility and invertibility

- Every rule in **sCp** is height-preserving invertible. Induction on the height of d
- Once again: the induction argument is simply the method of proving result. Picture the transformation of d.
- The contraction rules lc and rc are height-preserving admissible

$$\frac{A, A, X \vdash Y}{A, X \vdash Y}\text{lc} \qquad \frac{X \vdash Y, A, A}{X \vdash Y, A}\text{rc}$$

  Prove both claims simultaneously (why?). I.e. Let d be a derivation. If d is derives $A, A, X \vdash Y$ then $A, X \vdash Y$ is derivable, and if d derives $X \vdash Y, A, A$ then $X \vdash Y$ is derivable. Induction on the height of d. Use hp invertibility.
- Once again: the induction argument is simply the method of proving result. Picture the transformation of d.

Relating **sCp** to classical logic

- Let **Cp** denote the set of formulae that are derivable in **hCp**.
- Since **hCp** is a Hilbert calculus for classical logic, **Cp** is the set of theorems of classical logic.
- Equivalently, **Cp** consists of those formulae that evaluate to $\top$ under the truth table semantics.

Theorem

For every formula A: $\vdash A$ *is derivable in* **sCp** $\Leftrightarrow A \in$ **Cp**.

- To prove this, following Gentzen, introduce a sequent calculus version of MP called the cut rule. Formula A is the cutformula.

$$\frac{A \qquad A \to B}{B}\ \text{MP} \qquad\qquad \frac{X \vdash Y, A \qquad A, U \vdash V}{X, U \vdash Y, V}\ \mathit{cut}$$

- We will prove the theorem by showing the following:

1. $\Gamma \vdash \Delta$ is derivable in **sCp** $+\ \mathit{cut} \Leftrightarrow \wedge\Gamma \to \vee\Delta \in$ **Cp** (notation)
2. $\Gamma \vdash \Delta$ is derivable in **sCp** $+\ \mathit{cut}$ iff $\Gamma \vdash \Delta$ is derivable in **sCp**

$\vdash A$ is derivable in **sCp** $\overset{2.}{\Leftrightarrow} \vdash A$ is derivable in **sCp** $+\ \mathit{cut} \overset{1.}{\Leftrightarrow} A \in$ **Cp**

1a: $\Gamma \vdash \Delta$ is derivable in $\mathbf{sCp} + cut \Rightarrow \wedge\Gamma \to \vee\Delta \in \mathbf{Cp}$

- This direction is soundness. We want to show that what the calculus derives can be translated to a theorem of classical logic.
- Use semantics or **hCp** to establish this direction.
- Argue by induction on the height of derivation of $\Gamma \vdash \Delta$.
- Translations of the initial sequents are theorems of **Cp**

$$p, X \to Y, p \qquad \text{show that } p \wedge (\wedge X) \to (\vee Y) \vee p \in \mathbf{Cp}$$

$$\bot \wedge X \to Y \qquad \text{show that } \bot \wedge (\wedge X) \to (\vee Y) \in \mathbf{Cp}$$

- Inductive step. Show for each remaining rule ρ: if the translation of every premise is a theorem of **Cp** then so is the translation of the conclusion.

$$\frac{A, X \vdash B}{X \vdash A \to B} \qquad \text{need to show:} \qquad \frac{(A \wedge (\wedge X)) \to B}{(\wedge X) \to (A \to B)}$$

1b: $\bigwedge\Gamma \rightarrow \bigvee\Delta \in$ **Cp** $\Rightarrow \Gamma \vdash \Delta$ is derivable in **sCp** + *cut*

- Observe: $\vdash \bigwedge\Gamma \rightarrow \bigvee\Delta$ derivable in **sCp** + *cut* iff $\Gamma \vdash \Delta$ derivable **sCp** + *cut*
- Show that $\vdash$ Ax is derivable in **sCp** + *cut* for every axiom Ax in **hCp**. E.g.

$$
\dfrac{\dfrac{\dfrac{\dfrac{A, A \rightarrow (B \rightarrow C) \vdash C, A \qquad \dfrac{B, A \vdash C, A \qquad \dfrac{B, A \vdash C, B \qquad C, B, A \vdash C}{B \rightarrow C, B, A \vdash C}\,{\rightarrow}\mathrm{l}}{B, A, A \rightarrow (B \rightarrow C) \vdash C}\,{\rightarrow}\mathrm{l}}{A, A \rightarrow B, (A \rightarrow (B \rightarrow C)) \vdash C}\,{\rightarrow}\mathrm{l}}{A \rightarrow B, (A \rightarrow (B \rightarrow C)) \vdash A \rightarrow C}\,{\rightarrow}\mathrm{r}}{(A \rightarrow (B \rightarrow C)) \vdash (A \rightarrow B) \rightarrow (A \rightarrow C)}\,{\rightarrow}\mathrm{r}}{\vdash (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))}\,{\rightarrow}\mathrm{r}
$$

1b: $\wedge\Gamma \to \vee\Delta \in \mathbf{Cp} \Rightarrow \Gamma \vdash \Delta$ is derivable in $\mathbf{sCp} + cut$ (ctd)

- Now let us simulate MP in the sense: if $\vdash A$ and $\vdash A \to B$ is derivable, then $\vdash B$ is derivable:

$$\dfrac{\vdash A \qquad \dfrac{\vdash A \to B \qquad \dfrac{A \vdash A \qquad B \vdash B}{A \to B, A \vdash B} \to\text{l}}{A \vdash B}\ \text{cut}}{\vdash B}\ cut$$

- In this way we have that if A is derivable in **hCp** then $\vdash A$ is derivable in $\mathbf{sCp} + cut$
- It follows that

$$\begin{aligned} \wedge\Gamma \to \vee\Delta \in \mathbf{Cp} \quad &\Rightarrow \quad \vdash \wedge\Gamma \to \vee\Delta \text{ derivable in } \mathbf{sCp} + cut \\ &\Rightarrow \quad \Gamma \vdash \Delta \text{ derivable in } \mathbf{sCp} + cut \end{aligned}$$

2. $\Gamma \vdash \Delta$ derivable in **sCp** + *cut* iff $\Gamma \vdash \Delta$ derivable in **sCp**

- Right-to-left direction is trivial. Left-to-right is the cut-elimination theorem

Theorem (Gentzen cut-elimination theorem)

Suppose that δ is a derivation of $X \vdash Y$ in **sCp** + *cut. Then there is a transformation to eliminate instances of the cut-rule from δ to obtain a derivation δ' of $X \vdash Y$ in* **sCp***.*

- First argue how to get rid of a single cut in δ
- Suppose that we are given a derivation δ of $X \vdash Y$ containing a single occurrence of the cutrule as the last rule of the derivation. Argue by principal induction on the size of the cutformula and secondary induction on cutheight (sum of the premise derivation heights) that there is a cutfree derivation of $X \vdash Y$.
- Again: induction is method of proving; picture transformation
- If δ multiple cuts, repeat the argument, always choosing a topmost cut (i.e. a cut that has no cut above it in the derivation)

Proof of Gentzen's *Hauptsatz*

Consider a derivation concluding with the cut-rule:

$$\frac{X \vdash Y, A \qquad A, U \vdash V}{X, U \vdash Y, V}\ cut$$

- (Base case) A derivation of minimal height concluding in a cutrule must have the left and right premise as initial sequents.

  $$\frac{p, X \vdash Y, p \qquad q, U \vdash V, q}{\text{depends on whether cut-formula is } p \text{ or } q \text{ or something else}}\ \text{cut}$$

  In every case the conclusion is already an initial sequent so we don't need the cut!
- Argument when either initial sequent is ($\perp$l) or ($\top$r) is similar
- (Inductive case) Consider the following possibilities
  1. cut-formula A is not principal in one of the premises
  2. cut-formula A is principal in both premises

Proof of Gentzen's *Hauptsatz* II

A is not principal in one of the premises of the cutrule e.g.

$$\dfrac{\dfrac{\dfrac{\vdots}{X' \vdash^{k} Y', A}}{X \vdash^{k+1} Y, C \vee D, A}\, r \qquad \dfrac{\vdots}{A, U \vdash^{l} V, C \vee D}}{X, U \vdash Y, V, C \vee D}\,\text{cut}$$

Superscript indicates height. Cutheight is $k + l + 1$. Lift the cut upwards...

$$\dfrac{\dfrac{\vdots}{X' \vdash^{k} Y', A} \qquad \dfrac{\vdots}{A, U \vdash^{l} V, C \vee D}}{X', U \vdash Y', V, C \vee D}\,\text{cut}$$

Derivation has reduced cutheight $k + l$ $(< k + l + 1)$ so apply induction hypothesis to get cutfree derivation $X', U \vdash Y', V, C \vee D$.

Apply rule r to $X', U \vdash Y', V, C \vee D$ to get cutfree derivation of $X, U \vdash Y, V, C \vee D$. Cutfree derivation has greater height!

Proof of Gentzen's *Hauptsatz* III

- The cutformula A is principal in both premises e.g.

$$\dfrac{\dfrac{\begin{matrix}\vdots\\ A, X \vdash^{k} Y, B\end{matrix}}{X \vdash^{k+1} Y, A \to B}\to r \qquad \dfrac{\begin{matrix}\vdots\\ U \vdash^{l} V, A\end{matrix} \qquad \begin{matrix}\vdots\\ B, U \vdash^{m} V\end{matrix}}{A \to B, U \vdash^{1+\max l,m} V}\to l}{X, U \vdash Y, V}\text{cut}$$

Lift the cut upwards...

$$\dfrac{\begin{matrix}\vdots\\ A, X \vdash Y, B\end{matrix} \qquad \begin{matrix}\vdots\\ B, U \vdash V\end{matrix}}{A, X, U \vdash Y, V}\text{cut}$$

Since size $|B|$ of the cutformula smaller than before $(A \to B)$ apply the induction hypothesis to get cutfree derivation of $A, X, U \vdash Y, V$.

Proof of Gentzen's *Hauptsatz* IV

From above: apply the induction hypothesis to obtain a cutfree derivation of $A, X, U \vdash Y, V$. Now proceed:

$$\dfrac{\begin{matrix}\vdots \\ U \vdash V, A\end{matrix} \qquad \begin{matrix}\vdots \\ A, X, U \vdash Y, V\end{matrix}}{X, U, U \vdash Y, V, V}$$

Since the size $|A|$ of the cutformula is smaller than before $(A \to B)$ apply the induction hypothesis to obtain a cutfree derivation of $X, U, U \vdash Y, V, V$ (the duplicates are because we applied cut twice)

By admissibility of lc and rc we get $X, U \vdash Y, V$ as required.

- cutfree proof is typically much longer than proof with cuts
- Cut-elimination: eliminating lemmata from a math. proof
- Computational interpretations

Hilbert calculus **hCp** and sequent calculus **sCp** compared

$$\frac{}{p, X \vdash Y, p}\ \text{init} \qquad \frac{}{\bot, X \vdash Y}\ \bot\text{l} \qquad \frac{}{X \vdash Y, \top}\ \top\text{r}$$

$$\frac{X \vdash Y, A}{\neg A, X \vdash Y}\ \neg l \qquad \frac{A, X \vdash Y}{X \vdash Y, \neg A}\ \neg r$$

$$\frac{A, B, X \vdash Y}{A \wedge B, X \vdash Y}\ \wedge l \qquad \frac{X \vdash Y, A \qquad X \vdash Y, B}{X \vdash Y, A \wedge B}\ \wedge r$$

$$\frac{A, X \vdash Y \qquad B, X \vdash Y}{A \vee B, X \vdash Y}\ \vee l \qquad \frac{X \vdash Y, A, B}{X \vdash Y, A \vee B}\ \vee r$$

$$\frac{X \vdash Y, A \qquad B, X \vdash Y}{A \to B, X \vdash Y}\ \to l \qquad \frac{A, X \vdash Y, B}{X \vdash Y, A \to B}\ \to\text{r}$$

- We have traded many axioms and few rules in **hCp** for no axioms and many rules in **sCp**. So what's the point?
- The aim was to remove MP to obtain the subformula property: every formula in the premise(s) is a subformula of a formula in the conclusion
- To do this we first introduced a more general version of MP (the cut rule) and showed how it could be eliminated

sCp has the Subformula property, **hCp** does not

- Subformula property: every formula in the premise(s) is a subformula of a formula in the conclusion
- If all the rules of the calculus satisfy this property, the calculus is analytic
- Analyticity is crucial to using the calculus (for consistency, decidability. . .) as we shall see
- Unlike in the Hilbert calculus, the proof has a nice structure!
- To be precise: there are properties weaker than the subformula property which can be useful (e.g. analytic cut). The point is to meaningfully relate the premises to the conclusion.

Applications: Consistency of classical logic

Consistency of classical logic is the statement that $A \wedge \neg A \notin \mathbf{Cp}$.

Theorem

Classical logic is consistent.

Proof by contradiction. Suppose that $A \wedge \neg A \in \mathbf{Cp}$. Then $A \wedge \neg A$ is derivable in **sCp** (completeness). Let us try to derive it (read upwards from $\vdash A \wedge \neg A$):

$$\dfrac{\vdash A \qquad \dfrac{A \vdash}{\vdash \neg A}}{\vdash A \wedge \neg A}$$

So $\vdash A$ and $A \vdash$ are derivable. Thus $\vdash$ must be derivable in $\mathbf{sCp} + \mathit{cut}$ (use cut) and hence in **sCp** (by cut-elimination). This is impossible (why?) QED.

Applications: Decidability of classical logic

Theorem

Decidability of **Cp***.*

- Starting from a given formula A, repeatedly apply the rules backwards (choosing some formula as principal).
- Since each rule reduces the complexity of the sequent (a logical connective is deleted), the backward proof search terminates under any choice of principal formulae
- There are only finitely many backward proof searches. If one is a derivation, then $A \in \mathbf{Cp}$ otherwise it is not.
- Note: argument (as above) fails in $\mathbf{sCp} + lc + rc$. Suppose your favourite calculus obliges the inclusion of contraction in some way (e.g. most calculi for intuitionistic logic). Then other arguments may be available.
- Substructural logics side comment: deleting weakening from **Ip** leads to $\mathbf{FL}_{ec}$ (proved decidable by Kripke, 1959).
- Deleting weakening and exchange leads to $\mathbf{FL}_c$ proved undecidable (Chvalovsky and Horcik, 2016)

Modal Logics

"Modal languages are simple yet expressive languages for talking about relational structures"
Modal Logic (Blackburn, Venema and de Rijke)

- Augment the usual boolean connectives ($\neg$, $\wedge$, $\vee$, $\rightarrow$, $\bot$, $\top$) with modal operators like (but not limited to) $\Diamond$ and $\Box$.
- No variable binding, so the language is simpler than first-order.
- A relational structure is a set with a collection of relations on the set.

- Relational structures appear everywhere.
- E.g. to describe mathematical structures, theoretical computer science (model program execution as a set of states, where the binary relations model the behaviour of the program), knowledge representation, economics, computational linguistics
- We could already imagine that first-order and second-order languages are well-equipped to talk about relational structures
- The point is that modal languages are very simple languages to describe relational structures

Modal language

- Let $\mathcal{V}$ be a set of variables. The formulae of modal logic are:

  $$\mathcal{F} \ ::= \ \mathcal{V} \mid \mathcal{F} \wedge \mathcal{F} \mid \mathcal{F} \vee \mathcal{F} \mid \mathcal{F} \rightarrow \mathcal{F} \mid \neg \mathcal{F} \mid \Box \mathcal{F}$$

  with $\Diamond A$ abbreviating the formula $\neg \Box \neg A$
- Equivalently $\Box A$ abbreviating $\neg \Diamond \neg A$.

- Alternatively we could include both $\Diamond$ and $\Box$ in the signature
- So $\Diamond A$ and $\Box A$ are said to be duals of each other
- Recall $\forall A = \neg \exists \neg A$.

Some standard interpretations of the modal operators

1. $\Diamond A$ as 'it is possibly the case that A'. So $\Box A$ reads 'it is not possible that not A' or simply 'it is necessarily the case that A'.

   So what can we say about statement like $A \to \Diamond A$ and $\Diamond A \to \Box\Diamond A$? Do these follow as a logical consequence?

2. Epistemic logic. Read $\Box A$ as 'the agent knows A'. Or have lots of modal operators and read $\Box_i A$ as 'the i^{th} agent knows A.

   Since we use the word knowledge, we would expect $\Box A \to A$ ('if the agent knows A then A'—contrast with belief) . But is it the case that $A \to \Box A$ ('if A, then the agent knows it')? What about $\Box A \to \Box\Box A$?

Some standard interpretations (cont.)

1. Provability. Read $\Box A$ as 'it is provable in Peano arithmetic that A'. It may be shown that $\Box(\Box A \to A) \to \Box A$ (Löb formula) holds.

2. Temporal language. Read $\Diamond A$ as 'A holds in some future time' and $\blacklozenge A$ as 'A held at some past time'.
(what is $\Box A$ and $\blacksquare A$?)

3. Propositional dynamic logic. $\langle\pi\rangle A$ as 'some terminating execution of program π from the present state leads to a state bearing information A' . So $[\pi]A$ is 'every execution of program π from the present state leads to a state bearing information A'

Talking about relational structures via the modal language

- A frame consists of a nonempty set W of worlds and a binary relation $R \subseteq W \times W$.
- A model is a pair (F, V) where $F = (W, R)$ is a frame and V is a function mapping each propositional variable to a subset $V(p) \subseteq W$ 'valuation'.
- Truth (satisfaction) at a world w in a model M is defined via:

$$
\begin{array}{rcl}
M, w \models p & \text{iff} & w \in V(p) \\
M, w \models A \wedge B & \text{iff} & M, w \models A \text{ and } M, w \models B \\
M, w \models A \vee B & \text{iff} & M, w \models A \text{ or } M, w \models B \\
M, w \models A \rightarrow B & \text{iff} & M, w \not\models A \text{ or } M, w \models B \\
M, w \models \neg A & \text{iff} & M, w \not\models A \\
M, w \models \Box A & \text{iff} & \forall v \in W.(Rwv \Rightarrow M, v \models A) \\
M, w \models \Diamond A & \text{iff} & \exists v \in W.(Rwv \;\&\; M, v \models A)
\end{array}
$$

- If $M, w \models A$ then A is satisfied in M at w.

Validity I

- A frame is a formalisation of the phenomenon we wish to capture (time as a linearly ordered set).
- A model 'dresses up' the frame with information (the program executes at $t = 4$).
- Since logic is concerned with reasoning (invariant under local information), we need to consider those things that hold under all possible models.
- A formula is valid at a world w of a frame $F = (W, R)$ if it is satisfied at w in every model (F, V)
- A formula is valid if it is valid on all frames at every world
- Classical theorems (i.e. $A \in \mathbf{Cp}$) are valid

Validity II

Definition

Formula A is valid at a world w in a frame F ($F, w \models A$) if *for all valuations* V it is the case that $(F, V), w \models A$.

Formula A is valid on the frame F if it is valid at every world in F.

Formula A is valid on a class $\mathcal{F}$ of frames if A is valid on every frame in $\mathcal{F}$.

- Given a class $\mathcal{F}$ of frames, the set $\Lambda_{\mathcal{F}}$ of formulae valid on $\mathcal{F}$ is called the logic of $\mathcal{F}$.
- The definition of validity utilises second-order quantification: 'over all valuations V' (over all subsets of W).

The logics of various frame classes

- The logic of all frames
- The logic of transitive frames i.e.

  $$\{ A \,|\, F \models A \text{ for every frame } F \text{ s.t. } F \models \forall xyz.(Rxy \wedge Ryz \rightarrow Rxz)\}$$

- The logic of reflexive frames

  $$\{ A \,|\, F \models A \text{ for every frame } F \text{ s.t. } F \models \forall x.Rxx\}$$

- The logic of finite (irreflexive) transitive trees (cannot be described by a first-order formula!)

Syntactic definition of modal logics

- The semantic definition we have seen is in terms of the structures the modal language intends to talk about i.e. relational structures.
- The valid formulae then represent the properties that are invariant under local information
- When we are concerned solely about such valid formulae, it makes sense to abstract away the details of the relational structure.
- Recall we have seen this before! Instead of talking about the theorems of classical logic as those that are valued $\top$ under all truth table valuations, we generated the set of theorems by consideration of the provability relation
- In other words, we want nice syntactic mechanisms for generating $\Lambda_{\mathcal{F}}$ for a given class $\mathcal{F}$ of frames

A Hilbert calculus **hK** for the normal modal logic **K**

- Define the Hilbert calculus **hK** to be the extension of the Hilbert calculus **hCp** for classical propositional logic with the following axioms and rule:

$$\Box(A \to B) \to (\Box A \to \Box B) \qquad\qquad \Box A \leftrightarrow \neg\Diamond\neg B$$

$$\frac{A}{\Box A}\ \text{necessitation}$$

- Axiom top left is called the normality axiom.
- Axiomatic extensions of **hK** are called normal modal logics.
- Non-normal modal logics are also interesting, they will be discussed in Lecture 4
- Syntactically speaking, the normal axiom permits modus ponens under $\Box$; necessitation allows us to add boxes.

Soundness and completeness of **hK** wrt semantics

- The claim is that **K** is the logic of all frames i.e. $\mathbf{K} = \Lambda_{\mathcal{F}}$ where $\mathcal{F}$ is the class of all frames.
- What is derivable in **hK** is valid on all frames (soundness)
- A formula valid on all frames is derivable (completeness)
- Soundness of the axioms. Let M be an arbitrary model and w some world in M. Show that each axiom holds on M at w.
- Next show soundness of the rules. Supposing that the premises are valid show that the conclusion is also valid
- Completeness entails showing that if A is valid on all frames, then A is a theorem of the Hilbert calculus. We omit the argument here since we can obtain the result using the sequent calculus introduced later.

Some axiomatic extensions of **hK**

- Consider the following axioms

4 :	$\Box p \to \Box\Box p$	(or perhaps more clearly $\Diamond\Diamond p \to \Diamond p$)
T :	$\Box p \to p$	(or perhaps more clearly $p \to \Diamond p$)
L :	$\Box(\Box p \to p) \to \Box p$	(Löb axiom)

- We claim that the addition of these axioms to **hK** yield the following logics:

K4	the logic of transitive frames
K*T*	the logic of reflexive frames
K*L*	the logic of finite (irreflexive) transitive trees

- For historical reasons, axiom T is reflexivity (and not transitivity!)
- Check soundness. Completeness is non-trivial.

Obtaining a sequent calculus for **K**

- Let's try to derive the normality axiom $\Box(A \to B) \to (\Box A \to \Box B)$ in **sCp**:

$$\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A \qquad B \vdash B}{A \to B, A \vdash B} \to l}{\vdots}}{\Box(A \to B), \Box A \vdash \Box B}}{\dfrac{\Box(A \to B) \vdash (\Box A \to \Box B)}{\vdash \Box(A \to B) \to (\Box A \to \Box B)} \to r} \to r$$

- How to fill in the ...?
- We might 'guess' the following

$$\frac{X \vdash A}{\Box X \vdash \Box A} \Box K$$

- Here $\Box X$ is notation

$$X = \{A_1, \ldots, A_n\} \qquad \Box X = \{\Box A_1, \ldots, \Box A_n\}$$

A sequent calculus **sK** for the modal logic K

- Add the $\Box$K rule to the sequent calculus for classical logic.

$$\frac{X \vdash A}{\Box X \vdash \Box A}\ \Box K$$

- We claim that **sK** is sound and complete for **K**
- Soundness. In the case of **sCp** we argued soundness from premise to conclusion. For the $\Box K$ rule, it is easier to argue contrapositively. Suppose that $\wedge \Box X \rightarrow \Box A$ is not valid. We need to show that $\wedge X \rightarrow A$ is not valid.
- Completeness: Show that sK derives all the axioms of hK and simulates all the rules.
- The $\Box K$ rule simulates necessitation. Add the cut-rule to simulate MP
- Since we ultimately want a calculus with the subformula property, we need to show (surprise. . .) cut-elimination.

Cut-elimination for *sK*

- Recall the Gentzen-style cut-elimination (primary induction on size of cutformula, secondary induction on cutheight)
  1. Base case. Consider when the cutheight is minimal.
  2. Inductive case. Either the cutformula is principal in both premises or it is not principal in at least one premise.
- Let us consider the case of principal cuts (i.e. cutformula is principal in both premises)

$$\dfrac{\dfrac{X \vdash A}{\Box X \vdash \Box A}\,\Box\mathrm{K} \qquad \dfrac{A, Y \vdash C}{\Box A, \Box Y \vdash \Box C}\,\Box\mathrm{K}}{\Box X, \Box Y \vdash \Box C}\,\mathrm{cut}$$

Lift cut, then apply induction hypothesis, finally reapply $\Box$K

$$\dfrac{X \vdash A \qquad A, Y \vdash C}{X, Y \vdash C}\,\mathrm{cut}$$

induction hypothesis yields cutfree:

$$\dfrac{X, Y \vdash C}{\Box X, \Box Y \vdash \Box C}\,\Box\mathrm{K}$$

A sequent calculus **sK**4 for **K**4

- Recall: **K**4 is the logic of transitive frames (T is for reflexive, remember?)
- Here is the rule encountered in the literature.

$$\frac{\Box X, X \vdash A}{\Box X \vdash \Box A}\,\Box 4$$

- Soundness and completeness of **sK**4 wrt **K**4
- Check soundness of $\Box 4$ and derive the 4 axiom.
- Simulating modus ponens leads us to introduce the cutrule. . .
- . . . subformula property considerations motivate us to eliminate the cutrule. . .
- . . . blah blah. . .