Revision

Logics considered

1. Classical logic
2. Modal logic
3. Intuitionistic logic
4. Minimal logic (briefly)
5. Hoare logic (the odd one out)

Pervasive principles

Notions that apply to all decent logics:

1. Satisfaction relation $\Vdash$
2. Semantic entailment $\models$ and validity
3. Syntactic entailment $\vdash$ (natural deduction or sequent calculus)
4. Soundness and completeness ($\models = \vdash$)

Kripke semantics is also pervasive in that it applies to both modal logic and intuitionistic logic (actually, also minimal logic).

Kinds of inference systems

- Natural deduction (and λ-calculus)
- Sequent calculus
  - Multiplicative SC for propositional classical logic
  - (Additive) SC for minimal logic, as a framework for
  - Uniform proofs
- Tableaux (notations for proofs designed to make our lives easier; we considered tableaux for Hoare logic; there are tableaux for other logics, e.g., predicate logic)

Semantics

Semantics of logical formulæ

- In logics, meaning is often described by a **satisfaction relation**

$$M \models A$$

  that describes when a **situation** M satisfies a formula A.
- It varies between logics what formulæ and situations are.

Satisfaction relation for proposition classical logic

This one is straightforward:

$M \models A \wedge B$ iff $M \models A$ and $M \models B$

$M \models A \vee B$ iff $M \models A$ or $M \models B$

$M \models A \rightarrow B$ iff whenever $M \models A$ then $M \models B$

$M \models \neg A$ iff $M \not\models A$

$M \models \top$ always

$M \models \bot$ never

$M \models p$ iff $[\![p]\!]_M = 1$

Satisfaction relations of modal logic and intuitionistic logic

The satisfaction relations of modal logic and intuitionistic logic are more interesting.

- A situation in modal logic or intuitionistic is a pair (M, x) consisting of a Kripke model M and a world x in M.
- One usually writes

$$x \Vdash A$$

("x **forces** A") instead of $(M, x) \models A$.

Forcing for modal logic

The forcing relation looks basically like the satisfaction relation of classical propositional logic, except for the rules

$x \Vdash p$	iff	$p \in L(x)$
$x \Vdash \Box A$	iff for each $y \in W$ with $R(x, y)$ we have $y \Vdash A$	
$x \Vdash \Diamond A$	iff there is a $y \in W$ with $R(x, y)$ such that $y \Vdash A$	

Forcing intuitionistic logic

The forcing relation looks basically like the satisfaction relation of classical propositional logic, except for the rules

$$x \Vdash p \quad \text{iff} \quad p \in L(x)$$

$$x \Vdash A \to B \quad \text{iff} \quad \text{for all } y \text{ with } x \leq y, \text{ if } y \Vdash A \text{ then } y \Vdash B.$$

Semantic entailment

Definition. Let Γ be a set of formulæ, and let B a formula. We say that Γ **semantically entails** B and write

$$\Gamma \models B$$

if every situation that satisfies all formulæ in Γ also satisfies B.

(Warning: $\Gamma \models B$ differs from $M \models B$.)

Validity

Definition. A formula A is called “valid” if every situation satisfies it, i.e. if

$$\models A.$$

Soundness and completeness

Soundness: If the syntactic entailment $\Gamma \vdash A$ is derivable, then the semantic entailment $\Gamma \models A$ holds.

Completeness: If the semantic entailment holds $\Gamma \models A$, then the syntactic entailment $\Gamma \vdash A$ is derivable.

Soundness and completeness can be stated and hold for

- all kinds of logics (e.g., propositional logic, predicate logic, classical logic, intuitionistic logic, modal logic);
- various inference systems (e.g., natural deduction or sequent calculus).

Natural deduction

ND for classical logic

Definition. A **natural deduction proof** in **classical** propositional logic of $\Gamma \vdash A$ is a finite tree whose leaves are formulæ in Γ and which is built by using only the rules below.

$$\frac{A \quad B}{A \wedge B}\wedge i \qquad \frac{A \quad B}{A}\wedge e \qquad \frac{A \quad B}{B}\wedge e$$

$$\frac{\begin{matrix}[A]\\ \vdots \\ B\end{matrix}}{A \rightarrow B}\rightarrow i \qquad \frac{A \rightarrow B \quad A}{B}\rightarrow e$$

$$\frac{\bot}{A}\bot e \qquad \frac{\begin{matrix}\neg A\\ \vdots \\ \bot\end{matrix}}{A} RAA$$

A different presentation of ND for classical logic

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge i \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge e \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge e$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \rightarrow i \qquad \frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \rightarrow e$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A} \bot e \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A} RAA \qquad \frac{}{\Gamma, A \vdash A} Ax$$

Note the Ax rule, which is not necessary in the other presentation.

ND for intuitionistic logic

Definition. A **ND proof** in intuitionistic propositional logic of $\Gamma \vdash A$ is a ND proof in classical logic of $\Gamma \vdash A$ that does not contain RAA.

Exercises

Give ND proofs for the formulæ below (you may use RAA when you are asked this in the exam):

$$(A \to B) \to ((B \to C) \to (A \to C))$$

$$(\neg B \to \neg A) \to (A \to B) \qquad \text{(contrapositive)}$$

$$((A \to B) \to A) \to A \qquad \text{(Pierce's law)}$$

$$(A \vee B) \to \neg(\neg A \wedge \neg B)$$

$$(\neg A \vee B) \to (A \to B)$$

$$(A \wedge B) \to \neg(\neg A \vee \neg B)$$

$$\neg(\neg A \vee \neg B) \to (A \wedge B).$$

Variable capture

- Consider e.g. the formula below, which holds e.g. for the natural numbers.

$$A = \forall x.\exists y.x < y$$

- Applying $\forall$-elimination with $t = y$ yields the following formula, which is not valid.

$$\exists y.y < y$$

- The mistake has been caused by **variable capture**: the variable y in t has been caught by the quantifier $\exists y$.

$\forall$-elimination in ND

$$\frac{\Gamma \vdash \forall x.A}{\Gamma \vdash A[t/x]}\,\forall e \quad \text{if } t \text{ is free for } x \text{ in } A$$

"t is free for x in A" has an unpleasantly technical definition. It is okay to say replace this condition by the more informal statement "if no variable capture occurs (when the substitution $[t/x]$ is applied)".

$\forall$-introduction

In the style with assumptions, the rule for $\forall$-introduction is

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}\,\forall i \quad \text{if } x \notin FV(\Gamma).$$

Intuitively,

$$\frac{A \text{ holds of an arbitrary } x}{A \text{ holds for all } x}\,.$$

The side condition $x \notin FV(\Gamma)$ is the formal way of saying that x is arbitrary.

$\exists$-elimination

$$\frac{\Gamma \vdash \exists x.A \quad \Gamma, A \vdash B}{\Gamma \vdash B}\,\exists e \quad \text{if } x \notin FV(\Gamma, B)$$

Intuitively,

$$\frac{\begin{array}{c}\text{there is an } x \text{ such that } A(x) \\ \text{an arbitrary } x \text{ s.t. } A(x) \text{ implies } B\end{array}}{B \text{ holds}}\,.$$

The side condition $x \notin FV(\Gamma, B)$ is the formal way of stating that x is arbitrary.

Exercise

Show the claims below, where $x \notin FV(B)$.

1. $\forall x.(A \to B) \vdash (\exists x.A) \to B$
2. $(\exists x.A) \to B \vdash \forall x.(A \to B)$
3. $\exists x.(A \land B) \vdash (\exists x.A) \land B$
4. $(\exists x.A) \land B \vdash \exists x.(A \land B)$

Solution for Ex. 1

Let $\Gamma = \forall x.(A \to B), \exists x.A$.

$$\dfrac{\dfrac{}{\Gamma \vdash \exists x.A}\,Ax \qquad \dfrac{\dfrac{\dfrac{}{\Gamma, A \vdash \forall x.A \to B}\,Ax}{\Gamma, A \vdash A \to B}\,\forall e \qquad \dfrac{}{\Gamma, A \vdash A}\,Ax}{\Gamma, A \vdash B}\,\to e}{\dfrac{\Gamma \vdash B}{\forall x.(A \to B) \vdash (\exists x.A) \to B}\,\to i}\,\exists e$$

The $\exists e$ is correct because $x \notin FV(\Gamma, B)$.

Solution for Ex. 2

Let $\Gamma = (\exists x.A) \to B, A$.

$$
\dfrac{\dfrac{}{\Gamma \vdash (\exists x.A) \to B}\,Ax \qquad \dfrac{\dfrac{}{\Gamma \vdash A}\,Ax}{\Gamma \vdash \exists x.A}\,\exists i}{\dfrac{\dfrac{\Gamma \vdash B}{(\exists x.A) \to B \vdash A \to B}\,\to i}{(\exists x.A) \to B \vdash \forall x.(A \to B)}\,\forall i}\,\to e
$$

The $\forall i$ is correct because $x \notin FV((\exists x.A) \to B)$.

Solution for Ex. 3

Let $C = A \wedge B$.

$$\dfrac{\dfrac{\dfrac{}{\exists x.C \vdash \exists x.C}\,Ax \qquad \dfrac{\dfrac{\dfrac{}{\exists x.C, C \vdash C}\,Ax}{\exists x.C, C \vdash A}\,\wedge e}{\exists x.C, C \vdash \exists x.A}\,\exists i}{\exists x.C \vdash \exists x.A}\,\exists e \qquad \dfrac{\dfrac{}{\exists x.C \vdash \exists x.C}\,Ax \qquad \dfrac{\dfrac{}{\exists x.C, C \vdash C}\,Ax}{\exists x.C, C \vdash B}\,\wedge e}{\exists x.C \vdash B}\,\exists e}{\exists x.C \vdash (\exists x.A) \wedge B}\,\wedge i$$

The left $\exists e$ is correct because $x \notin FV(\exists x.C, \exists x.A)$; the right $\exists e$ is correct because $x \notin FV(\exists x.C, B)$.

Hoare logic

Partial correctness vs. total correctness

There are two readings for a Hoare triple $(\!|\phi|\!)C(\!|\psi|\!)$:

- **Partial correctness**: if the initial state satisfies ϕ and C is executed **and** terminates, then the resulting state satisfies ψ. We write

$$\models_{par} (\!|\phi|\!)C(\!|\psi|\!).$$

- **Total correctness**: if the initial state satisfies ϕ, then C terminates and the resulting state satisfies ψ. We write

$$\models_{tot} (\!|\phi|\!)C(\!|\psi|\!).$$

Rules for partial correctness

$$\frac{(\!|\phi|\!)C_1(\!|\eta|\!) \quad (\!|\eta|\!)C_2(\!|\psi|\!)}{(\!|\phi|\!)C_1;C_2(\!|\psi|\!)}\ \text{Composition}$$

$$\frac{}{(\!|\psi[E/x]|\!)x = E(\!|\psi|\!)}\ \text{Assignment}$$

$$\frac{(\!|\phi \wedge B|\!)C_1(\!|\psi|\!) \quad (\!|\phi \wedge \neg B|\!)C_2(\!|\psi|\!)}{(\!|\phi|\!)\mathtt{if}\ B\ \mathtt{then}\ \{C_1\}\ \mathtt{else}\{C_2\}(\!|\psi|\!)}\ \text{If-statement}$$

$$\frac{(\!|\psi \wedge B|\!)C(\!|\psi|\!)}{(\!|\psi|\!)\mathtt{while}\ B\ \{C\}(\!|\psi \wedge \neg B|\!)}\ \text{Partial-while}$$

$$\frac{\vdash \phi' \to \phi \quad (\!|\phi|\!)C(\!|\psi|\!) \quad \psi \to \psi'}{(\!|\phi'|\!)C(\!|\psi'|\!)}\ \text{Implied}$$

Partial correctness of Fac1 (something very similar may be in the exam)

$\llparenthesis true \rrparenthesis$	
$\llparenthesis 1 = 0! \rrparenthesis$	Implied
$y = 1$	
$\llparenthesis y = 0! \rrparenthesis$	Assignment
$z = 0$	
$\llparenthesis y = z! \rrparenthesis$	Assignment
`while` $(z\,!=\,x)\{$	
$\llparenthesis y = z! \wedge z \neq x \rrparenthesis$	Invariant $\wedge$ guard
$\llparenthesis y * (z+1) = (z+1)! \rrparenthesis$	Implied
$z = z + 1$	
$\llparenthesis y * z = z! \rrparenthesis$	Assignment
$y = y * z$	
$\llparenthesis y = z! \rrparenthesis$	Assignment
$\}$	
$\llparenthesis y = z! \wedge \neg(z \neq x) \rrparenthesis$	Partial-while
$\llparenthesis y = x! \rrparenthesis$	Implied

The Total-while rule

The Total-while rule is like the Partial-while rule, but with augmented pre- and postconditions:

$$\frac{(\!|\eta \wedge B \wedge (0 \leq E = E_0)|\!)\, C\, (\!|\eta \wedge (0 \leq E < E_0)|\!)}{(\!|\eta \wedge (0 \leq E)|\!)\, \texttt{while}\, B\, \{C\}\, (\!|\eta \wedge \neg B|\!)} \text{ Total-while.}$$

- E is the variant, which decreases during every iteration: if $E = E_0$ before the loop, then it is strictly less than E_0 after it—but it remains non-negative.
- Technically, E_0 is a variable that does not occur anywhere else.

Total correctness of Fac1

$\llparenthesis x \geq 0 \rrparenthesis$	
$\llparenthesis 1 = 0! \wedge 0 \leq x - 0 \rrparenthesis$	Implied
$y = 1$	
$\llparenthesis y = 0! \wedge 0 \leq x - 0 \rrparenthesis$	Assignment
$z = 0$	
$\llparenthesis y = z! \wedge 0 \leq x - z \rrparenthesis$	Assignment
`while` $(z\,! = x)\{$	
$\llparenthesis y = z! \wedge z \neq x \wedge 0 \leq x - z = E_0 \rrparenthesis$	Invariant $\wedge$ guard
$\llparenthesis y * (z+1) = (z+1)! \wedge 0 \leq x - (z+1) < E_0 \rrparenthesis$	Implied
$z = z + 1$	
$\llparenthesis y * z = z! \wedge 0 \leq x - z < E_0 \rrparenthesis$	Assignment
$y = y * z$	
$\llparenthesis y = z! \wedge 0 \leq x - z < E_0 \rrparenthesis$	Assignment
$\}$	
$\llparenthesis y = z! \wedge \neg(z \neq x) \rrparenthesis$	Total-while
$\llparenthesis y = x! \rrparenthesis$	Implied

Sequent calculus

The sequent calculus in multiplicative form: Ax, Cut, introduction rules

$$\frac{}{A \vdash A}\,Ax \qquad \frac{\Gamma_2 \vdash \Delta_1, A, \Delta_3 \quad \Gamma_1, A, \Gamma_3 \vdash \Delta_2}{\Gamma_1, \Gamma_2, \Gamma_3 \vdash \Delta_1, \Delta_2, \Delta_3}\,Cut$$

$$\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\,L\wedge \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma' \vdash B, \Delta'}{\Gamma, \Gamma', \vdash A \wedge B, \Delta, \Delta'}\,R\wedge$$

$$\frac{\Gamma, A \vdash \Delta \quad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \vee B \vdash \Delta, \Delta'}\,L\vee \qquad \frac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}\,R\vee$$

$$\frac{}{\bot \vdash}\,L\bot \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \bot, \Delta}\,R\bot$$

$$\frac{\Gamma \vdash \Delta}{\Gamma, \top \vdash \Delta}\,L\top \qquad \frac{}{\vdash \top}\,R\top$$

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \rightarrow B \vdash \Delta, \Delta'}\,L \rightarrow \qquad \frac{\Gamma, A \vdash \Delta, B}{\Gamma \vdash A \rightarrow B, \Delta}\,R \rightarrow$$

The sequent calculus in multiplicative form: structural rules

$$\frac{\Gamma, A, B, \Gamma' \vdash \Delta}{\Gamma, B, A, \Gamma' \vdash \Delta}\, LE \qquad \frac{\Gamma \vdash \Delta, A, B, \Delta'}{\Gamma \vdash \Delta, B, A, \Delta'}\, RE$$

$$\frac{\Gamma, \Gamma' \vdash \Delta}{\Gamma, A, \Gamma' \vdash \Delta}\, LW \qquad \frac{\Gamma \vdash \Delta, \Delta'}{\Gamma \vdash \Delta, A, \Delta'}\, RW$$

$$\frac{\Gamma, A, A, \Gamma' \vdash \Delta}{\Gamma, A, \Gamma' \vdash \Delta}\, LC \qquad \frac{\Gamma \vdash \Delta, A, A, \Delta'}{\Gamma \vdash \Delta, A, \Delta'}\, RC$$

Additive form

The sequent calculus in additive form has different variants of $R\wedge$, $L\vee$, $L\rightarrow$ and Cut, e.g.,

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta} \, R\wedge \, .$$

In the presence of the structural rules, the additive variants are equivalent to the multiplicative variants.

Sequent calculus for predicate logic

The extra rules are

$$\frac{\Gamma, A[t/x] \vdash \Delta}{\Gamma, \forall x.A \vdash \Delta}\; L\forall \qquad \frac{\Gamma \vdash A, \Delta}{\Gamma \vdash \forall x.A, \Delta}\; R\forall$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, \exists x.A \vdash \Delta}\; L\exists \qquad \frac{\Gamma \vdash A[t/x], \Delta}{\Gamma \vdash \exists x.A, \Delta}\; R\exists,$$

where in $R\forall$ and $L\exists$ it must hold that $x \notin FV(\Gamma, \Delta)$, and in $L\forall$ and $R\exists$ it must hold that no variable capture occurs.

Exercises

Give proofs of the following judgments in the sequent calculus (in multiplicative form):

$$A \wedge (B \vee C) \vdash (A \wedge B) \vee C \qquad (1)$$

$$(\exists x.A) \wedge B \vdash \exists x.(A \wedge B) \qquad \text{where } x \notin FV(B) \qquad (2)$$

$$\forall x.(A \to B) \vdash (\exists x.A) \to B \qquad \text{where } x \notin FV(B) \qquad (3)$$

Solution to Ex. 1

$$
\dfrac{\dfrac{\dfrac{\dfrac{\overline{A \vdash A}\;Ax \qquad \overline{B \vdash B}\;Ax}{A, B \vdash A \wedge B}\;R\wedge \qquad \overline{C \vdash C}\;Ax}{A, B \vee C \vdash A \wedge B, C}\;L\vee}{A, B \vee C \vdash (A \wedge B) \vee C}\;R\vee}{A \wedge (B \vee C) \vdash (A \wedge B) \vee C}\;L\wedge
$$

Note that there are straightforward “dual” versions of this proof, i.e. versions that differ only w.r.t. the order in which $\wedge$ and $\vee$ are tackled.

Solution to Ex. 3

$$\dfrac{\dfrac{}{A \vdash A}\,Ax \qquad \dfrac{}{B \vdash B}\,Ax}{\dfrac{A \to B, A \vdash B}{\dfrac{\forall x.(A \to B), A \vdash B}{\dfrac{\forall x.(A \to B), \exists x.A \vdash B}{\forall x.(A \to B) \vdash (\exists x.A) \to B}\,R\to}\,L\exists}\,L\forall}$$

The $L\exists$ is correct because $x \notin FV(\forall x.(A \to B), B)$.

Simulating ND elimination rules in the sequent calculus

The elimination rules of ND are simulated essentially by a **left** introduction rule followed by a cut, e.g.,

$$\dfrac{\Gamma \vdash \forall x.A \qquad \dfrac{\dfrac{}{A[t/x] \vdash A[t/x]}\,Ax}{\forall x.A \vdash A[t/x]}\,L\forall}{\Gamma \vdash A[t/x]}\,Cut$$

Proof search

Proof search and sequent calculus

- Proof search tries to find a proof of a given goal $\Gamma \vdash A$.
- The challenge is to reduce the **search space** of possible proofs.
- According to current research, this is best attempted within the sequent calculus.
- The **minimal sequent calculus** in the next slide works very well as a framework for proof search.
- It is additive, cut-free, single-succedent.

The “minimal sequent calculus”

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

$$\frac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}\, L\wedge \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\, R\wedge$$

$$\frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}\, L\vee \qquad \frac{\Gamma \vdash A_i}{\Gamma \vdash A_1 \vee A_2}\, (i = 1, 2) R\vee$$

$$\frac{\Gamma \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \to B \vdash C}\, L \to \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\, R \to$$

$$\frac{\Gamma, A[t/x] \vdash B}{\Gamma, \forall x.A \vdash B}\, L\forall \qquad \frac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}\, R\forall$$

$$\frac{\Gamma, A \vdash B}{\Gamma, \exists x.A \vdash B}\, L\exists \qquad \frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x.A}\, R\exists$$

Uniform proofs

- Uniform proofs result from putting an extra constraint on the search space given by the minimal sequent calculus.
- The idea is that the goal is taken to pieces (by right rules) as long as possible; left rules are applied only when the goal is atomic.

Definition. A proof in the minimal sequent calculus is **uniform** if every sequent $\Gamma \vdash A$ with non-atomic succedent A is obtained from a right rule.

(Non-)Examples

The following proof is uniform:

$$\dfrac{\dfrac{\dfrac{}{p, q \vdash p}\,Ax}{p \wedge q \vdash p}\,L\wedge \qquad \dfrac{\dfrac{}{p, q \vdash q}\,Ax}{p \wedge q \vdash q}\,L\wedge}{p \wedge q \vdash p \wedge q}\,R\wedge\,.$$

The following proof is not uniform:

$$\dfrac{\dfrac{\dfrac{}{p, q \vdash p}\,Ax \qquad \dfrac{}{p, q \vdash q}\,Ax}{p, q \vdash p \wedge q}\,L\wedge}{p \wedge q \vdash p \wedge q}\,L\wedge\,.$$

$\vee$ and $\exists$

Not all judgments $\Gamma \vdash A$ that are provable in the minimal sequent calculus have uniform proofs. This is because of $\vee$ and $\exists$: e.g., a uniform proof of $\exists x.p(x) \vdash \exists x.p(x)$ would have to look as follows:

$$\frac{\begin{array}{c}\vdots\\ \exists x.p(x) \vdash p(x)\end{array}}{\exists x.p(x) \vdash \exists x.p(x)}\ R\exists,$$

but this proof cannot be completed, because $\exists x.p(x) \vdash p(x)$ is not valid (because the fact that $p(x)$ holds for some x doesn't imply that $p(x)$ holds for an arbitrary x), and therefore not provable. Similarly for $\vee$.

The λ-calculus

The λ-calculus

The material from the λ-calculus lecture is relevant for the exam. (Have a good look at the notion of inhabited types.)