Programming Languages

Deductive systems

Natural deduction for propositional logic

Deductive systems

Natural deduction for propositional logic

Bivalent semantics

Motivation

We want to be able to make **mathematically precise statements** about programs in different programming languages.

Examples of statements we would like to make

- The type `(Bool -> Int)` is syntactically well-formed.
- The expression `map` has type `((a -> b) -> [a] -> [b])`.
- The expression `map` has type `((a -> a) -> [a] -> [a])`.
- The expression `map` has type `Bool`.
- The program `while (true) {}` does not terminate.
- The result of evaluating `(factorial 7)` is 5040.
- The algorithms `quickSort` and `mergeSort` are indistinguishable.

We want to have mechanisms to prove such statements.

In this context, statements are called **judgments**.

Deductive systems

A **deductive system** is used to reason about **judgments**.

It is given by **inference rules**, of the form:

$$\frac{\langle \text{premise}_1 \rangle \quad \langle \text{premise}_2 \rangle \quad \ldots \quad \langle \text{premise}_n \rangle}{\langle \text{conclusion} \rangle} \langle \text{rule name} \rangle$$

Rules that have no premises ($n = 0$) are called **axioms**.

The premises are **sufficient conditions** for the conclusion.

- Reading from top to bottom:
  if we have evidence that the premises hold,
  we can deduce that the conclusion holds.
- Reading from bottom to top:
  if we want to prove that the conclusion holds,
  it suffices to prove that the premises hold.

Deductive systems

Example — the deductive system $\mathcal{A}$

System $\mathcal{A}$ predicates over judgments of the form "$X > Y$".
It includes three axioms:

$$\frac{}{\bigstar > \blacksquare}\,\text{ax1} \qquad \frac{}{\blacksquare > \blacktriangle}\,\text{ax2} \qquad \frac{}{\blacktriangle > \bullet}\,\text{ax3}$$

and a rule *schema*, where X, Y, Z are schematic variables (which can be instantiated arbitrarily):

$$\frac{X > Y \quad Y > Z}{X > Z}\,\text{trans}$$

- Prove the judgment $\bigstar > \bullet$ in two different ways.

Deductive systems

A **derivation** is a finite tree formed by inference rules.
It starts from certain premises and reaches a conclusion.

A judgment is **derivable** if there is some derivation with no premises that concludes it.

Deductive systems

Example — formulas

Assume an infinite set of *propositional variables* is given:

$$\mathcal{P} = \{P, Q, R, \ldots\}$$

The following system predicates over judgments of the form "X FORM".

$$\frac{P \in \mathcal{P}}{P \ \text{FORM}}\mathsf{FP} \qquad \frac{\tau \ \text{FORM} \quad \sigma \ \text{FORM}}{(\tau \wedge \sigma) \ \text{FORM}}\mathsf{F}\wedge \qquad \frac{\tau \ \text{FORM} \quad \sigma \ \text{FORM}}{(\tau \Rightarrow \sigma) \ \text{FORM}}\mathsf{F}\Rightarrow$$

$$\frac{\tau \ \text{FORM} \quad \sigma \ \text{FORM}}{(\tau \vee \sigma) \ \text{FORM}}\mathsf{F}\vee \qquad \frac{}{\bot \ \text{FORM}}\mathsf{F}\bot \qquad \frac{\tau \ \text{FORM}}{\neg\tau \ \text{FORM}}\mathsf{F}\neg$$

1. Derive the judgment $\neg(P \Rightarrow (Q \Rightarrow P)) \ \text{FORM}$.
2. Prove that if $\tau \ \text{FORM}$ is a derivable judgment, then τ has the same number of "(" as of ")".
   Proceed by structural induction on the derivation.

Deductive systems

Natural deduction for propositional logic

Bivalent semantics

Formulas of propositional logic

Formulas are the expressions that can be generated from the following grammar:

$$\tau, \sigma, \rho, \ldots ::= P \mid (\tau \wedge \sigma) \mid (\tau \Rightarrow \sigma) \mid (\tau \vee \sigma) \mid \bot \mid \neg\tau$$

Observation

Grammars define deductive systems in an abbreviated way.

An expression τ can be generated from the above grammar if and only if the judgment τ FORM is derivable in the previous system.

Notation conventions

1. We omit the outermost parentheses of formulas.

   $$\tau \wedge \neg(\sigma \vee \rho) \;=\; (\tau \wedge \neg(\sigma \vee \rho))$$

2. Implication is right-associative.

   $$\tau \Rightarrow \sigma \Rightarrow \rho \;=\; (\tau \Rightarrow (\sigma \Rightarrow \rho))$$

3. Caution: the connectives $(\wedge, \vee)$ are **not** commutative or associative.

   $$\tau \vee (\sigma \vee \rho) \;\neq\; (\tau \vee \sigma) \vee \rho \qquad \tau \wedge \sigma \;\neq\; \sigma \wedge \tau$$

Contexts and judgments

A **context** is a finite set of formulas.
We denote them with uppercase Greek letters ($\Gamma, \Delta, \Sigma, \ldots$).
For example:

$$\Gamma = \{P \Rightarrow Q, \neg Q\}$$

We usually omit the braces; e.g.: $P \Rightarrow Q, \neg Q$.

The system of **natural deduction** predicates over judgments of the form:

$$\Gamma \quad \vdash \quad \tau$$

Informally, a judgment states that from the hypotheses in the context Γ it is possible to deduce the thesis formula.

For example, the following will be derivable judgments:

$$P \Rightarrow Q \vdash \neg Q \Rightarrow \neg P \qquad P, Q \wedge R \vdash R \wedge P$$

Inference rules — axiom

The natural deduction system has many inference rules.

(We'll go step by step)

Axiom

$$\frac{}{\Gamma, \tau \vdash \tau}\,\text{ax}$$

Example

$$\frac{}{P \vdash P}\,\text{ax} \qquad \frac{}{P \Rightarrow Q, R \vdash P \Rightarrow Q}\,\text{ax} \qquad \frac{}{P, Q \wedge R, S \vdash Q \wedge R}\,\text{ax}$$

The following judgments are **not** derived by the rule ax:

$$P, Q \vdash R \qquad \vdash P \Rightarrow P \qquad P \wedge Q \vdash Q \wedge P \qquad \neg\neg P \vdash P$$

Inference rules — conjunction

Conjunction introduction

$$\frac{\Gamma \vdash \tau \quad \Gamma \vdash \sigma}{\Gamma \vdash \tau \wedge \sigma} \wedge_i$$

Conjunction elimination

$$\frac{\Gamma \vdash \tau \wedge \sigma}{\Gamma \vdash \tau} \wedge_{e_1} \qquad \frac{\Gamma \vdash \tau \wedge \sigma}{\Gamma \vdash \sigma} \wedge_{e_2}$$

1. Give a derivation of $P \wedge Q \vdash Q \wedge P$.
2. Give a derivation of $P \wedge (Q \wedge R) \vdash (P \wedge Q) \wedge R$.

Inference rules — implication

Implication introduction

$$\frac{\Gamma, \tau \vdash \sigma}{\Gamma \vdash \tau \Rightarrow \sigma} \Rightarrow_i$$

Implication elimination

(*modus ponens*)

$$\frac{\Gamma \vdash \tau \Rightarrow \sigma \quad \Gamma \vdash \tau}{\Gamma \vdash \sigma} \Rightarrow_e$$

1. Give a derivation of $\vdash P \Rightarrow P$
2. Give a derivation of $\vdash P \Rightarrow Q \Rightarrow (Q \wedge P)$
3. Give a derivation of $P \Rightarrow Q, Q \Rightarrow R \vdash P \Rightarrow R$.

Inference rules — disjunction

Disjunction introduction

$$\frac{\Gamma \vdash \tau}{\Gamma \vdash \tau \vee \sigma} \vee_{i_1} \qquad \frac{\Gamma \vdash \sigma}{\Gamma \vdash \tau \vee \sigma} \vee_{i_2}$$

Disjunction elimination

$$\frac{\Gamma \vdash \tau \vee \sigma \quad \Gamma, \tau \vdash \rho \quad \Gamma, \sigma \vdash \rho}{\Gamma \vdash \rho} \vee_e$$

1. Give a derivation of $\vdash P \Rightarrow (P \vee P)$.
2. Give a derivation of $\vdash (P \vee P) \Rightarrow P$.
3. Give a derivation of $P \vee Q \vdash Q \vee P$.

Inference rules — falsehood

The connective $\bot$ represents falsehood (contradiction, absurdity).

The connective $\bot$ has **no** introduction rules.

Falsehood elimination

(principle of explosion or *ex falso quodlibet*)

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \tau}\bot_e$$

1. Give a derivation of $(P \vee Q) \Rightarrow \bot \vdash P \Rightarrow Q$
2. Give a derivation of $(P \wedge Q) \Rightarrow \bot \vdash P \Rightarrow Q \Rightarrow R$
3. Show that there are infinitely many derivations of $\bot \vdash \bot$.

Inference rules — negation

Negation introduction

(intuitionistic reductio ad absurdum)

$$\frac{\Gamma, \tau \vdash \bot}{\Gamma \vdash \neg\tau}\neg_i$$

Negation elimination

$$\frac{\Gamma \vdash \tau \quad \Gamma \vdash \neg\tau}{\Gamma \vdash \bot}\neg_e$$

1. Give a derivation of $\vdash P \Rightarrow \neg\neg P$.
2. Give a derivation of $\vdash \neg(P \wedge \neg P)$.
3. Give a derivation of $P \vee Q \vdash \neg(\neg P \wedge \neg Q)$.

Intuitionistic natural deduction (**NJ**) — complete rules

$$\frac{}{\Gamma, \tau \vdash \tau}\,\mathrm{ax}$$

	Introduction	Elimination
$\wedge$	$\dfrac{\Gamma \vdash \tau \quad \Gamma \vdash \sigma}{\Gamma \vdash \tau \wedge \sigma}\wedge_i$	$\dfrac{\Gamma \vdash \tau \wedge \sigma}{\Gamma \vdash \tau}\wedge_{e_1}$ $\quad$ $\dfrac{\Gamma \vdash \tau \wedge \sigma}{\Gamma \vdash \sigma}\wedge_{e_2}$
$\Rightarrow$	$\dfrac{\Gamma, \tau \vdash \sigma}{\Gamma \vdash \tau \Rightarrow \sigma}\Rightarrow_i$	$\dfrac{\Gamma \vdash \tau \Rightarrow \sigma \quad \Gamma \vdash \tau}{\Gamma \vdash \sigma}\Rightarrow_e$
$\vee$	$\dfrac{\Gamma \vdash \tau}{\Gamma \vdash \tau \vee \sigma}\vee_{i_1}$ $\quad$ $\dfrac{\Gamma \vdash \sigma}{\Gamma \vdash \tau \vee \sigma}\vee_{i_2}$	$\dfrac{\Gamma \vdash \tau \vee \sigma \quad \Gamma, \tau \vdash \rho \quad \Gamma, \sigma \vdash \rho}{\Gamma \vdash \rho}\vee_e$
$\bot$	$\dfrac{\Gamma \vdash \bot}{\Gamma \vdash \tau}\bot_e$	
$\neg$	$\dfrac{\Gamma, \tau \vdash \bot}{\Gamma \vdash \neg\tau}\neg_i$	$\dfrac{\Gamma \vdash \tau \quad \Gamma \vdash \neg\tau}{\Gamma \vdash \bot}\neg_e$

Properties of the system

Theorem (Weakening)

(weakening)

If $\Gamma \vdash \tau$ is derivable, then $\Gamma, \sigma \vdash \tau$ is derivable.

$$\frac{\Gamma \vdash \tau}{\Gamma, \sigma \vdash \tau}\mathrm{W}$$

It can be proved by structural induction on the derivation.
(This will be done as an exercise in the practice session).

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{}{P \wedge Q, R \vdash P \wedge Q}\mathrm{ax}}{P \wedge Q, R \vdash Q}\wedge_{e_2} \quad \dfrac{\dfrac{}{P \wedge Q, R \vdash P \wedge Q}\mathrm{ax}}{P \wedge Q, R \vdash P}\wedge_{e_1}}{P \wedge Q, R \vdash Q \wedge P}\wedge_i}{R \vdash (P \wedge Q) \Rightarrow (Q \wedge P)}\Rightarrow_i$$

Derived rules

Let's see that the following rules are derived from the previous ones.
(It is not necessary to add them to the deductive system).

Modus tollens

$$\frac{\Gamma \vdash \tau \Rightarrow \sigma \quad \Gamma \vdash \neg\sigma}{\Gamma \vdash \neg\tau}\mathsf{MT}$$

Double negation introduction

$$\frac{\Gamma \vdash \tau}{\Gamma \vdash \neg\neg\tau}\neg\neg_i$$

Classical reasoning principles

Double negation elimination

Can the following rule be derived from the previous ones?

$$\frac{\Gamma \vdash \neg\neg\tau}{\Gamma \vdash \tau}\,\neg\neg_e$$

Law of Excluded Middle

Can the following rule be derived from the previous ones?

$$\frac{}{\Gamma \vdash \tau \vee \neg\tau}\,\mathsf{LEM}$$

It is not possible to derive these rules from the previous ones.

However, they can be derived from each other. Let's see that:

1. Using the rule LEM one can derive the rule $\neg\neg_e$.
2. Using the rule $\neg\neg_e$ one can derive the rule LEM.

Classical reasoning principles

The rules $\neg\neg_e$ and LEM are **classical** reasoning principles.
Another classical reasoning principle, equivalent to $\neg\neg_e$ and LEM:

Classical reductio ad absurdum (Proof by Contradiction)

$$\frac{\Gamma, \neg\tau \vdash \bot}{\Gamma \vdash \tau}\text{PBC}$$

Exercise

Show that using PBC one can derive LEM and vice versa.

Intuitionistic logic vs. classical logic

Two deductive systems

NJ intuitionistic natural deduction system.
NK classical natural deduction system.

- **NK** extends **NJ** with classical reasoning principles.
  Adding one of them suffices, for example $\neg\neg_e$.
- If a judgment is derivable in **NJ**, it is also derivable in **NK**.
- **NJ** is more restrictive. It does not allow using $\neg\neg_e$, LEM, PBC, etc.
- For doing mathematics, we commonly use classical logic.

Interest of intuitionistic logic in computing

- It allows reasoning about **information**.
  What does (there is life on Mars $\vee$ $\neg$there is life on Mars) mean?
- Derivations in **NJ** can be understood as programs.

Classical natural deduction (**NK**) — complete rules

$$\frac{}{\Gamma, \tau \vdash \tau}\,\mathsf{ax} \qquad \frac{\Gamma \vdash \neg\neg\tau}{\Gamma \vdash \tau}\,\neg\neg_e$$

	Introduction	Elimination
$\wedge$	$\dfrac{\Gamma \vdash \tau \quad \Gamma \vdash \sigma}{\Gamma \vdash \tau \wedge \sigma}\,\wedge_i$	$\dfrac{\Gamma \vdash \tau \wedge \sigma}{\Gamma \vdash \tau}\,\wedge_{e_1} \quad \dfrac{\Gamma \vdash \tau \wedge \sigma}{\Gamma \vdash \sigma}\,\wedge_{e_2}$
$\Rightarrow$	$\dfrac{\Gamma, \tau \vdash \sigma}{\Gamma \vdash \tau \Rightarrow \sigma}\,\Rightarrow_i$	$\dfrac{\Gamma \vdash \tau \Rightarrow \sigma \quad \Gamma \vdash \tau}{\Gamma \vdash \sigma}\,\Rightarrow_e$
$\vee$	$\dfrac{\Gamma \vdash \tau}{\Gamma \vdash \tau \vee \sigma}\,\vee_{i_1} \quad \dfrac{\Gamma \vdash \sigma}{\Gamma \vdash \tau \vee \sigma}\,\vee_{i_2}$	$\dfrac{\Gamma \vdash \tau \vee \sigma \quad \Gamma, \tau \vdash \rho \quad \Gamma, \sigma \vdash \rho}{\Gamma \vdash \rho}\,\vee_e$
$\bot$	$\dfrac{\Gamma \vdash \bot}{\Gamma \vdash \tau}\,\bot_e$	
$\neg$	$\dfrac{\Gamma, \tau \vdash \bot}{\Gamma \vdash \neg\tau}\,\neg_i$	$\dfrac{\Gamma \vdash \tau \quad \Gamma \vdash \neg\tau}{\Gamma \vdash \bot}\,\neg_e$

Deductive systems

Natural deduction for propositional logic

Bivalent semantics

Valuations

A valuation is a function $v : \mathcal{P} \to \{\mathtt{T}, \mathtt{F}\}$ that assigns truth values to propositional variables.

A valuation v **satisfies** a formula τ if $v \vDash \tau$, where:

$$
\begin{array}{rll}
v \vDash P & \text{if and only if} & v(P) = \mathtt{T} \\
v \vDash \tau \wedge \sigma & \text{if and only if} & v \vDash \tau \text{ and } v \vDash \sigma \\
v \vDash \tau \Rightarrow \sigma & \text{if and only if} & v \nvDash \tau \text{ or } v \vDash \sigma \\
v \vDash \tau \vee \sigma & \text{if and only if} & v \vDash \tau \text{ or } v \vDash \sigma \\
v \vDash \bot & \text{never holds} & \\
v \vDash \neg\tau & \text{if and only if} & v \nvDash \tau
\end{array}
$$

A valuation v satisfies a context Γ (notation: $v \vDash \Gamma$) if and only if v satisfies all the formulas in Γ.

A context Γ satisfies a formula τ (notation: $\Gamma \vDash \tau$) if and only if any valuation v that satisfies Γ also satisfies τ.

Valuations

Example

1. Prove that $P \wedge Q \vDash P$.
2. Prove that $P \vee Q, \neg Q \vDash P$.
3. Prove that $P \vee Q \vDash Q$ does not hold.
4. Prove that $P \vDash Q \vee \neg Q$.

Soundness and completeness

Theorem (Soundness and completeness)

The following are equivalent:

1. $\Gamma \vdash \tau$ is derivable in **NK**.
2. $\Gamma \vDash \tau$

Proof of soundness $\Gamma \vdash_{\mathbf{NK}} \tau$ implies $\Gamma \vDash \tau$

Assume that $\Gamma \vdash \tau$ is derivable in **NK**.
We prove that $\Gamma \vDash \tau$ by structural induction on the derivation.

We need to analyze 13 cases, one for each rule of **NK**.

For example, for the rule $\Rightarrow_e$:

$$\frac{\Gamma \vdash \tau \Rightarrow \sigma \quad \Gamma \vdash \tau}{\Gamma \vdash \sigma} \Rightarrow_e$$

We want to see that $\Gamma \vDash \sigma$.
Let v be such that $v \vDash \Gamma$ and let's see that $v \vDash \sigma$.
By IH we know that $\Gamma \vDash \tau \Rightarrow \sigma$ and that $\Gamma \vDash \tau$.
Since $v \vDash \Gamma$ we have that $v \vDash \tau \Rightarrow \sigma$ and $v \vDash \tau$.
By definition of $v \vDash \tau \Rightarrow \sigma$, we then have that $v \nvDash \tau$ or $v \vDash \sigma$.
But we had $v \vDash \tau$, so we conclude $v \vDash \sigma$.

- Try to prove the remaining 12 cases.

Proof of completeness ($\Gamma \models \tau$ implies $\Gamma \vdash_{\mathbf{NK}} \tau$)

Definition

1. A context Γ **determines** a variable $P \in \mathcal{P}$ if either $P \in \Gamma$ or $\neg P \in \Gamma$.
2. A context Γ **determines** a set of variables $X \subseteq \mathcal{P}$ if it determines all variables in X.

To prove the completeness theorem, we need:

Main Lemma

If Γ determines all the variables that appear in τ, then:

1. Either $\Gamma \vdash \tau$ is derivable in **NK**.
2. Or $\Gamma \vdash \neg\tau$ is derivable in **NK**.

Assume the lemma holds; we will prove it afterwards.

Proof of completeness ($\Gamma \models \tau$ implies $\Gamma \vdash_{\mathbf{NK}} \tau$)

Assume that $\sigma_1, \ldots, \sigma_n \models \tau$.
We want to see that $\sigma_1, \ldots, \sigma_n \vdash \tau$ is derivable in **NK**.

Let $\rho = (\sigma_1 \wedge \ldots \wedge \sigma_n) \Rightarrow \tau$. We know that $\models \rho$. Why?
It suffices to prove that $\vdash \rho$ is derivable in **NK**. Why?

Let $X = \{P_1, \ldots, P_n\}$ be the set of variables that appear in ρ.
Using LEM and $\vee_e$ we can consider 2^n cases, of the form:

$$\tilde{P}_1, \ldots, \tilde{P}_n \vdash \rho$$

where each $\tilde{P}_i$ is either P_i or $\neg P_i$.
By the main lemma, one of the following two cases occurs:

1. Either $\tilde{P}_1, \ldots, \tilde{P}_n \vdash \rho$ is derivable in **NK** (and we are done).
2. Or $\tilde{P}_1, \ldots, \tilde{P}_n \vdash \neg\rho$ is derivable in **NK**.
   By soundness, $\tilde{P}_1, \ldots, \tilde{P}_n \models \neg\rho$.
   Let v be a valuation such that $v(P_i) = \mathtt{T}$ if and only if $\tilde{P}_i = P_i$.
   Then $v \models \neg\rho$. Contradiction since we knew $\models \rho$.

Proof of the main lemma

Recall the statement:

Main Lemma

If Γ determines all the variables that appear in τ, then:

1. Either $\Gamma \vdash \tau$ is derivable in **NK**.
2. Or $\Gamma \vdash \neg\tau$ is derivable in **NK**.

We prove it by structural induction on τ.
There are 6 cases (P, $\wedge$, $\Rightarrow$, $\vee$, $\bot$, $\neg$).

For example, suppose $\tau = (\sigma \wedge \rho)$.
By the inductive hypothesis on σ, we know that:

1. Either $\Gamma \vdash \sigma$ is derivable in **NK**.
   By the inductive hypothesis on ρ, we know that:
   1.1 Either $\Gamma \vdash \rho$ is derivable in **NK** and we have $\Gamma \vdash \sigma \wedge \rho$.
   1.2 Or $\Gamma \vdash \neg\rho$ is derivable in **NK** and we have $\Gamma \vdash \neg(\sigma \wedge \rho)$.
2. Or $\Gamma \vdash \neg\sigma$ is derivable in **NK** and we have $\Gamma \vdash \neg(\sigma \wedge \rho)$.

- Try to prove the remaining 5 cases.

¿ ¿ ¿ ¿ ¿ ¿ ¿ ¿ ¿ ? ? ? ? ? ? ? ? ?

Recommended reading

Chapters 2 and 6 of the book by Sørensen and Urzyczyn.
Morten Sørensen and Paweł Urzyczyn. *Lectures on the Curry–Howard Isomorphism*
Elsevier, 2006.