Computer Supported Modeling and Reasoning

David Basin, Achim D. Brucker, Jan-Georg Smaus, and Burkhart Wolff

April 2005

http://www.infsec.ethz.ch/education/permanent/csmr/

Propositional Logic: Natural Deduction

David Basin, Burkhart Wolff, and Jan-Georg Smaus

Natural Deduction

Developed by Gentzen [Gen35] and Prawitz [Pra65].

Designed to support 'natural' logical arguments:

- we make (temporary) assumptions;
- we derive new formulas by applying rules;
- there is also a mechanism for discharging assumptions.

Natural Deduction (2)

Derivations are trees

$$\cfrac{\cfrac{A \to (B \to C) \quad A}{B \to C}\ {\to}\text{-}E \qquad B}{C}\ {\to}\text{-}E$$

where the leaves are called assumptions.

Natural Deduction (2)

Derivations are trees

$$\dfrac{\dfrac{A \rightarrow (B \rightarrow C) \quad A}{B \rightarrow C}\,{\scriptstyle \rightarrow\text{-}E} \qquad B}{C}\,{\scriptstyle \rightarrow\text{-}E}$$

where the leaves are called assumptions.

Write $A_1, \ldots A_n \vdash A$ if there exists a derivation of A with assumptions $A_1, \ldots, A_n$, e.g. $A \rightarrow (B \rightarrow C), A, B \vdash C$.

Natural Deduction (2)

Derivations are trees

$$\dfrac{\dfrac{A \rightarrow (B \rightarrow C) \quad A}{B \rightarrow C}\,\rightarrow\text{-}E \qquad B}{C}\,\rightarrow\text{-}E$$

where the leaves are called assumptions.

Write $A_1, \ldots A_n \vdash A$ if there exists a derivation of A with assumptions $A_1, \ldots, A_n$, e.g. $A \rightarrow (B \rightarrow C), A, B \vdash C$.

A proof is a derivation with no (open) assumptions.

Natural Deduction: an Abstract Example

- Language $\mathcal{L} = \{\heartsuit, \clubsuit, \spadesuit, \diamondsuit\}$.

Natural Deduction: an Abstract Example

- Language $\mathcal{L} = \{\heartsuit, \clubsuit, \spadesuit, \diamondsuit\}$.
- Deductive system given by rules of proof:

$$\frac{\diamondsuit}{\clubsuit}\,\alpha \qquad \frac{\diamondsuit}{\spadesuit}\,\beta \qquad \frac{\clubsuit \qquad \spadesuit}{\heartsuit}\,\gamma$$

How do you read these rules?

Natural Deduction: an Abstract Example

- Language $\mathcal{L} = \{\heartsuit, \clubsuit, \spadesuit, \diamondsuit\}$.
- Deductive system given by rules of proof:

$$\frac{\diamondsuit}{\clubsuit}\,\alpha \qquad \frac{\diamondsuit}{\spadesuit}\,\beta \qquad \frac{\clubsuit \quad \spadesuit}{\heartsuit}\,\gamma \qquad \begin{array}{c}[\diamondsuit]\\ \vdots \\ \heartsuit \\ \hline \heartsuit\end{array}\,\delta$$

How about this one?

Natural Deduction: an Abstract Example

- Language $\mathcal{L} = \{\heartsuit, \clubsuit, \spadesuit, \diamondsuit\}$.
- Deductive system given by rules of proof:

$$\frac{\diamondsuit}{\clubsuit}\,\alpha \qquad \frac{\diamondsuit}{\spadesuit}\,\beta \qquad \frac{\clubsuit \quad \spadesuit}{\heartsuit}\,\gamma \qquad \frac{\begin{array}{c}[\diamondsuit]\\ \vdots\\ \heartsuit\end{array}}{\heartsuit}\,\delta$$

How about this one?

N.B. $\alpha, \beta, \gamma, \delta$ just name the rules.

Proof of ♥

The rules:

$$\frac{\diamondsuit}{\clubsuit}\,\alpha \qquad \frac{\diamondsuit}{\spadesuit}\,\beta \qquad \frac{\clubsuit \quad \spadesuit}{\heartsuit}\,\gamma \qquad \frac{\begin{matrix}[\diamondsuit] \\ \vdots \\ \heartsuit\end{matrix}}{\heartsuit}\,\delta$$

The proof:

Proof of ♥

The rules:

$$\frac{\diamondsuit}{\clubsuit}\,\alpha \qquad \frac{\diamondsuit}{\spadesuit}\,\beta \qquad \frac{\clubsuit \qquad \spadesuit}{\heartsuit}\,\gamma \qquad \frac{\begin{array}{c}[\diamondsuit]\\ \vdots \\ \heartsuit\end{array}}{\heartsuit}\,\delta$$

The proof:

$$\diamondsuit$$

We make an assumption. The assumption is now open.

Proof of ♥

The rules:

$$\frac{\diamondsuit}{\clubsuit}\,\alpha \qquad \frac{\diamondsuit}{\spadesuit}\,\beta \qquad \frac{\clubsuit \quad \spadesuit}{\heartsuit}\,\gamma \qquad \frac{\begin{array}{c}[\diamondsuit]\\ \vdots \\ \heartsuit\end{array}}{\heartsuit}\,\delta$$

The proof:

$$\frac{\diamondsuit}{\clubsuit}\,\alpha$$

We apply α.

Proof of ♥

The rules:

$$\frac{\diamondsuit}{\clubsuit}\,\alpha \qquad \frac{\diamondsuit}{\spadesuit}\,\beta \qquad \frac{\clubsuit \qquad \spadesuit}{\heartsuit}\,\gamma \qquad \frac{\begin{array}{c}[\diamondsuit]\\ \vdots \\ \heartsuit\end{array}}{\heartsuit}\,\delta$$

The proof:

$$\frac{\diamondsuit}{\clubsuit}\,\alpha \qquad \frac{\diamondsuit}{\spadesuit}\,\beta$$

Similarly with β.

Proof of ♥

The rules:

$$\frac{\diamondsuit}{\clubsuit}\,\alpha \qquad \frac{\diamondsuit}{\spadesuit}\,\beta \qquad \frac{\clubsuit \quad \spadesuit}{\heartsuit}\,\gamma \qquad \frac{\begin{array}{c}[\diamondsuit]\\ \vdots \\ \heartsuit\end{array}}{\heartsuit}\,\delta$$

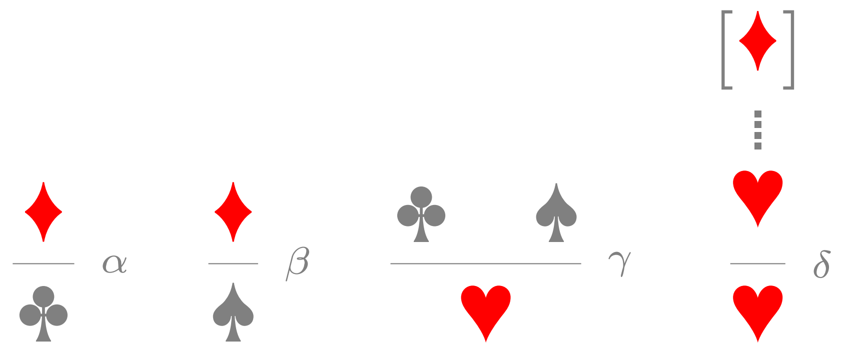
The proof:

$$\frac{\dfrac{\diamondsuit}{\clubsuit}\,\alpha \qquad \dfrac{\diamondsuit}{\spadesuit}\,\beta}{\heartsuit}\,\gamma$$

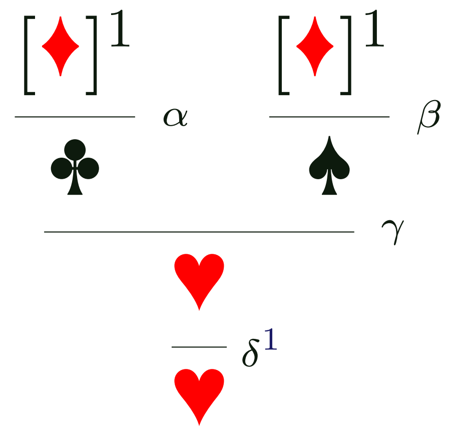
We apply γ.

Proof of ♥

The rules:



The proof:



We apply δ, discharging two occurrences of ♦. We mark the brackets and the rule with a label so that it is clear which assumption is discharged in which step. The derivation is now a proof: it has no open assumptions (all discharged).

Deductive System: Rules of Propositional Logic

We have rules for conjunction, implication, disjunction, falsity and negation.

Some rules introduce, others eliminate connectives.

Rules of Propositional Logic: Conjunction

- Rules of two kinds: introduce connectives

$$\frac{A \quad B}{A \wedge B}\ \wedge\text{-}I$$

Rules of Propositional Logic: Conjunction

- Rules of two kinds: introduce and eliminate connectives

$$\frac{A \quad B}{A \wedge B}\ \wedge\text{-}I \qquad \frac{A \wedge B}{A}\ \wedge\text{-}EL \qquad \frac{A \wedge B}{B}\ \wedge\text{-}ER$$

Rules of Propositional Logic: Conjunction

- Rules of two kinds: introduce and eliminate connectives

$$\frac{A \quad B}{A \wedge B}\ \wedge\text{-}I \qquad \frac{A \wedge B}{A}\ \wedge\text{-}EL \qquad \frac{A \wedge B}{B}\ \wedge\text{-}ER$$

- Rules are schematic.
- Why valid? If all assumptions are true, then so is conclusion

$$\mathcal{A} \models A \wedge B \text{ iff } \mathcal{A} \models A \text{ and } \mathcal{A} \models B$$

Example Derivation with Conjunction

The rules:

$$\frac{A \quad B}{A \wedge B}\ \wedge\text{-}I$$

$$\frac{A \wedge B}{A}\ \wedge\text{-}EL$$

$$\frac{A \wedge B}{B}\ \wedge\text{-}ER$$

Example Derivation with Conjunction

The rules:

$$\frac{A \quad B}{A \wedge B} \; \wedge\text{-}I$$

$$\frac{A \wedge B}{A} \; \wedge\text{-}EL$$

$$\frac{A \wedge B}{B} \; \wedge\text{-}ER$$

$$\frac{A \wedge (B \wedge C)}{A} \; \wedge\text{-}EL$$

Example Derivation with Conjunction

The rules:

$$\frac{A \quad B}{A \wedge B}\ \wedge\text{-}I$$

$$\frac{A \wedge B}{A}\ \wedge\text{-}EL$$

$$\frac{A \wedge B}{B}\ \wedge\text{-}ER$$

$$\frac{A \wedge (B \wedge C)}{A}\ \wedge\text{-}EL \qquad \frac{A \wedge (B \wedge C)}{B \wedge C}\ \wedge\text{-}ER$$

Example Derivation with Conjunction

The rules:

$$\frac{A \quad B}{A \wedge B}\ \wedge\text{-}I$$

$$\frac{A \wedge B}{A}\ \wedge\text{-}EL$$

$$\frac{A \wedge B}{B}\ \wedge\text{-}ER$$

$$\frac{A \wedge (B \wedge C)}{A}\ \wedge\text{-}EL \qquad \frac{\dfrac{A \wedge (B \wedge C)}{B \wedge C}\ \wedge\text{-}ER}{C}\ \wedge\text{-}ER$$

Example Derivation with Conjunction

The rules:

$$\frac{A \quad B}{A \wedge B}\ \wedge\text{-}I$$

$$\frac{A \wedge B}{A}\ \wedge\text{-}EL$$

$$\frac{A \wedge B}{B}\ \wedge\text{-}ER$$

$$\dfrac{\dfrac{A \wedge (B \wedge C)}{A}\ \wedge\text{-}EL \qquad \dfrac{\dfrac{A \wedge (B \wedge C)}{B \wedge C}\ \wedge\text{-}ER}{C}\ \wedge\text{-}ER}{A \wedge C}\ \wedge\text{-}I$$

Example Derivation with Conjunction

The rules:

$$\frac{A \quad B}{A \wedge B} \wedge\text{-}I$$

$$\frac{A \wedge B}{A} \wedge\text{-}EL$$

$$\frac{A \wedge B}{B} \wedge\text{-}ER$$

$$\dfrac{\dfrac{A \wedge (B \wedge C)}{A} \wedge\text{-}EL \qquad \dfrac{\dfrac{A \wedge (B \wedge C)}{B \wedge C} \wedge\text{-}ER}{C} \wedge\text{-}ER}{A \wedge C} \wedge\text{-}I$$

Can we prove anything with just these three rules?

Rules of Propositional Logic: Implication

- Rules

$$\frac{\begin{array}{c}[A]\\ \vdots \\ B\end{array}}{A \to B}\ \to\text{-}I \qquad \frac{A \to B \quad A}{B}\ \to\text{-}E$$

Rules of Propositional Logic: Implication

- Rules

$$\dfrac{\begin{array}{c}[A]\\ \vdots\\ B\end{array}}{A \rightarrow B}\ \rightarrow\text{-}I \qquad \dfrac{A \rightarrow B \quad A}{B}\ \rightarrow\text{-}E$$

- $\rightarrow$-*E* is also called modus ponens.

Rules of Propositional Logic: Implication

- Rules

$$\dfrac{\begin{array}{c}[A] \\ \vdots \\ B\end{array}}{A \rightarrow B}\ \rightarrow\text{-}I \qquad \dfrac{A \rightarrow B \quad A}{B}\ \rightarrow\text{-}E$$

- $\rightarrow$-*E* is also called modus ponens.
- $\rightarrow$-*I* formalizes (bottom-up) strategy:
  To derive $A \rightarrow B$, derive B under the additional (local) assumption A.
  Top-down: we may discharge 0 or more occurences of A.

A Simple Proof

The simplest proof we can think of is the proof of $P \to P$.

$$P$$

A Simple Proof

The simplest proof we can think of is the proof of $P \rightarrow P$.

$$\frac{[P]^1}{P \rightarrow P} \rightarrow\text{-}I^1$$

Do you find this strange?

Examples with Conjunction and Implication

1. $A \to B \to A$
2. $A \land (B \land C) \to A \land C$
3. $(A \to B \to C) \to (A \to B) \to A \to C$

Object versus Meta: variables here can either represent object variables or metavariables.

Disjunction

- Rules

$$\frac{A}{A \vee B}\ \vee\text{-}IL \qquad \frac{B}{A \vee B}\ \vee\text{-}IR \qquad \frac{A \vee B \quad \begin{matrix}[A]\\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B]\\ \vdots \\ C\end{matrix}}{C}\ \vee\text{-}E$$

Disjunction

- Rules

$$\frac{A}{A \vee B}\ \vee\text{-}IL \qquad \frac{B}{A \vee B}\ \vee\text{-}IR \qquad \frac{A \vee B \quad \begin{matrix}[A]\\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B]\\ \vdots \\ C\end{matrix}}{C}\ \vee\text{-}E$$

- Formalizes case-split strategy for using $A \vee B$.

Disjunction: Example

- Rules

$$\frac{A}{A \lor B}\ \lor\text{-}IL \qquad \frac{B}{A \lor B}\ \lor\text{-}IR \qquad \frac{A \lor B \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C}\ \lor\text{-}E$$

- Example: formalize and prove

  When it rains then I wear my jacket.
  When it snows then I wear my jacket.
  It is raining or snowing.
  Therefore I wear my jacket.

Falsity and Negation

- Falsity

$$\frac{\bot}{A}\ \bot\text{-}E$$

No introduction rule!

Falsity and Negation

- Falsity

$$\frac{\bot}{A}\ \bot\text{-}E$$

No introduction rule!

- Negation: define $\neg A$ as $A \rightarrow \bot$. Rules for $\neg$ just special cases of rules for $\rightarrow$. Convenient to have

$$\frac{\neg A \quad A}{B}\ \neg\text{-}E \quad \text{derived by} \quad \frac{\dfrac{\neg A \quad A}{\bot}\ \rightarrow\text{-}E}{B}\ \bot\text{-}E$$

Intuitionistic versus Classical Logic

- Peirce's Law: $((A \to B) \to A) \to A$.
  Is this valid? Provable?

Intuitionistic versus Classical Logic

- Peirce's Law: $((A \to B) \to A) \to A$.
  Is this valid? Provable?

- It is provable in classical logic, obtained by adding

$$A \lor \neg A \quad \text{or} \quad \dfrac{\begin{array}{c}[\neg A] \\ \vdots \\ \bot\end{array}}{A}\,RAA \quad \text{or} \quad \dfrac{\begin{array}{c}[\neg A] \\ \vdots \\ A\end{array}}{A}\,\textit{classical} \quad .$$

Example of Classical Reasoning

There exist irrational numbers a and b such that a^b is rational.

Proof: Let b be $\sqrt{2}$ and consider whether or not b^b is rational.

Case 1: If rational, let $a = b = \sqrt{2}$

Case 2: If irrational, let $a = \sqrt{2}^{\sqrt{2}}$, and then

$$a^b = \sqrt{2}^{\sqrt{2}^{\sqrt{2}}} = \sqrt{2}^{(\sqrt{2}*\sqrt{2})} = \sqrt{2}^2 = 2$$

Overview of Rules

$$\frac{A \quad B}{A \wedge B}\ \wedge\text{-}I \qquad \frac{A \wedge B}{A}\ \wedge\text{-}EL \qquad \frac{A \wedge B}{B}\ \wedge\text{-}ER$$

$$\frac{A}{A \vee B}\ \vee\text{-}IL \qquad \frac{B}{A \vee B}\ \vee\text{-}IR \qquad \frac{A \vee B \quad \begin{matrix}[A]\\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B]\\ \vdots \\ C\end{matrix}}{C}\ \vee\text{-}E$$

$$\frac{\begin{matrix}[A]\\ \vdots \\ B\end{matrix}}{A \rightarrow B}\ \rightarrow\text{-}I \qquad \frac{A \rightarrow B \quad A}{B}\ \rightarrow\text{-}E \qquad \frac{\bot}{A}\ \bot\text{-}E$$

Deductive System: Derived Rules

Using the basic rules, we can derive new rules.

Example: Resolution rule.

Deductive System: Derived Rules

Using the basic rules, we can derive new rules.

Example: Resolution rule.

$$\frac{R \vee S \quad \neg S}{R}$$

It looks like this.

Deductive System: Derived Rules

Using the basic rules, we can derive new rules.

Example: Resolution rule.

$$\frac{R \vee S \quad \neg S}{R}$$

$$\neg S$$

$$\frac{R \vee S \qquad \qquad \qquad}{R}$$

We build a fragment of a derivation by writing the conclusion R and the assumptions $R \vee S$ and $\neg S$.

Deductive System: Derived Rules

Using the basic rules, we can derive new rules.

Example: Resolution rule.

$$\frac{R \lor S \quad \neg S}{R}$$

$$\dfrac{R \lor S \qquad \begin{matrix} \neg S \\ \vdots \\ R \end{matrix}}{R} \; \lor\text{-}E$$

Since we have assumption $R \lor S$, using $\lor$-*E* seems a good idea. So we should make assumptions R and S. First R. But that is a derivation of R from R!

Deductive System: Derived Rules

Using the basic rules, we can derive new rules.

Example: Resolution rule.

$$\frac{R \vee S \quad \neg S}{R} \qquad \frac{R \vee S \quad R \quad \begin{matrix} \neg S \quad S \\ \\ \end{matrix}}{R}\ \vee\text{-}E$$

So now S.

Deductive System: Derived Rules

Using the basic rules, we can derive new rules.

Example: Resolution rule.

$$\dfrac{R \vee S \quad \neg S}{R}$$

$$\dfrac{R \vee S \qquad R \qquad \dfrac{\neg S \quad S}{\bot}\ \to\text{-}E}{R}\ \vee\text{-}E$$

$\neg S$ and S allow us to apply $\to$-*E*.

Deductive System: Derived Rules

Using the basic rules, we can derive new rules.

Example: Resolution rule.

$$\frac{R \vee S \quad \neg S}{R}$$

$$\dfrac{R \vee S \qquad R \qquad \dfrac{\dfrac{\neg S \quad S}{\bot}\,{\to}\text{-}E}{R}\,\bot\text{-}E}{R}\,\vee\text{-}E$$

To apply $\vee$-*E* in the end, we need to derive R. But that's easy using $\bot$-*E*!

Deductive System: Derived Rules

Using the basic rules, we can derive new rules.

Example: Resolution rule.

$$\frac{R \vee S \quad \neg S}{R}$$

$$\dfrac{R \vee S \quad [R]^1 \quad \dfrac{\dfrac{\neg S \quad [S]^1}{\bot}\ \rightarrow\text{-}E}{R}\ \bot\text{-}E}{R}\ \vee\text{-}E^1$$

Finally, we can apply $\vee$-E. The derivation with open assumptions is a new rule that can be used like any other rule.

Alternative Deductive System Using Sequent Notation

One can base the deductive system around the derivability judgement, i.e., reason about $\Gamma \vdash A$ where $\Gamma \equiv A_1, \ldots, A_n$ instead of individual formulae.

Sequent Rules (for $\rightarrow$ / $\wedge$ Fragment)

$$\Gamma \vdash A \quad \text{(where } A \in \Gamma\text{)} \qquad \frac{\Gamma \vdash B}{A, \Gamma \vdash B}\ \textit{weaken}$$

Rules for assumptions and weakening

Sequent Rules (for $\rightarrow / \wedge$ Fragment)

$$\Gamma \vdash A \quad \text{(where } A \in \Gamma\text{)} \qquad \frac{\Gamma \vdash B}{A, \Gamma \vdash B}\ \textit{weaken}$$

Rules for assumptions and weakening

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge\text{-}I \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \wedge\text{-}EL \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \wedge\text{-}ER$$

$$\frac{A, \Gamma \vdash B}{\Gamma \vdash A \rightarrow B}\ \rightarrow\text{-}I \qquad \frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}\ \rightarrow\text{-}E$$

More rules can be derived.

Example: Refinement Style with Metavariables

$$\frac{}{\vdash A \wedge (B \wedge C) \rightarrow A \wedge C} \rightarrow\text{-}I$$

We want to show that $A \wedge (B \wedge C) \rightarrow A \wedge C$ is a tautology, i.e., that it is derivable without any assumptions.

Example: Refinement Style with Metavariables

$$\dfrac{\dfrac{}{A \wedge (B \wedge C) \vdash A \wedge C}\ \wedge\text{-}I}{\vdash A \wedge (B \wedge C) \to A \wedge C}\ \to\text{-}I$$

The topmost connective of the formula is $\to$, so the best rule to choose is $\to$-*I*.

Example: Refinement Style with Metavariables

$$\dfrac{\dfrac{}{A \land (B \land C) \vdash A}\ \land\text{-}EL \qquad \dfrac{}{A \land (B \land C) \vdash C}\ \land\text{-}ER}{\dfrac{A \land (B \land C) \vdash A \land C}{\vdash A \land (B \land C) \to A \land C}\ \to\text{-}I}\ \land\text{-}I$$

The topmost connective of the formula is $\land$, so the best rule to choose is $\land$-*I*.

Example: Refinement Style with Metavariables

$$\dfrac{\dfrac{\dfrac{A \wedge (B \wedge C) \vdash A \wedge {\color{red}?X}}{A \wedge (B \wedge C) \vdash A}\ \wedge\text{-}EL \qquad \dfrac{}{A \wedge (B \wedge C) \vdash C}\ \wedge\text{-}ER}{A \wedge (B \wedge C) \vdash A \wedge C}\ \wedge\text{-}I}{\vdash A \wedge (B \wedge C) \rightarrow A \wedge C}\ \rightarrow\text{-}I$$

Things are becoming less obvious. To know that $\wedge$-*EL* is the best rule for the r.h.s., you need to inspect the assumption $A \wedge (B \wedge C)$.

Example: Refinement Style with Metavariables

$$\dfrac{\dfrac{A \wedge (B \wedge C) \vdash A \wedge ?X}{A \wedge (B \wedge C) \vdash A}\ \wedge\text{-}EL \qquad \dfrac{\dfrac{}{A \wedge (B \wedge C) \vdash (?Y \wedge C)}\ \wedge\text{-}ER}{A \wedge (B \wedge C) \vdash C}\ \wedge\text{-}ER}{\dfrac{A \wedge (B \wedge C) \vdash A \wedge C}{\vdash A \wedge (B \wedge C) \rightarrow A \wedge C}\ \rightarrow\text{-}I}\ \wedge\text{-}I$$

Now it's becoming even more difficult. To know that $\wedge$-*ER* is the best rule for the l.h.s., you need to look deep into the assumption $A \wedge (B \wedge C)$.

Example: Refinement Style with Metavariables

$$
\dfrac{\dfrac{\dfrac{A \wedge (B \wedge C) \vdash A \wedge {?X}}{A \wedge (B \wedge C) \vdash A}\ \wedge\text{-}EL \qquad \dfrac{\dfrac{A \wedge (B \wedge C) \vdash {?Z} \wedge ({?Y} \wedge C)}{A \wedge (B \wedge C) \vdash ({?Y} \wedge C)}\ \wedge\text{-}ER}{A \wedge (B \wedge C) \vdash C}\ \wedge\text{-}ER}{A \wedge (B \wedge C) \vdash A \wedge C}\ \wedge\text{-}I}{\vdash A \wedge (B \wedge C) \rightarrow A \wedge C}\ \rightarrow\text{-}I
$$

Again you need to look at both sides of the $\vdash$ to decide what to do.

Example: Refinement Style with Metavariables

$$
\dfrac{
  \dfrac{A \wedge (B \wedge C) \vdash A \wedge {?X}}{A \wedge (B \wedge C) \vdash A}\;\wedge\text{-}EL
  \qquad
  \dfrac{
    \dfrac{A \wedge (B \wedge C) \vdash {?Z} \wedge ({?Y} \wedge C)}{A \wedge (B \wedge C) \vdash ({?Y} \wedge C)}\;\wedge\text{-}ER
  }{A \wedge (B \wedge C) \vdash C}\;\wedge\text{-}ER
}{
  \dfrac{A \wedge (B \wedge C) \vdash A \wedge C}{\vdash A \wedge (B \wedge C) \rightarrow A \wedge C}\;\rightarrow\text{-}I
}\;\wedge\text{-}I
$$

Solution for ${?Z} = A$, ${?Y} = B$ and ${?X} = (B \wedge C)$.

Comments about Proof Refinement

This crazy way of carrying out proofs is the (standard) way, which is used in many proof assistants (as Isabelle)!

- Refinement style is also called backward style proofs
- Refinement style means we work from goals to axioms
- metavariables are used to delay substitions

Isabelle allows other refinements/alternatives too (see labs).

How Are ND Proofs Built?

ND proofs build derivations under (possibly temporary) assumptions.

ND: Example for $\rightarrow / \wedge$ Fragment

Rules:

$$\frac{A \quad B}{A \wedge B}\ \wedge\text{-}I \qquad \frac{A \wedge B}{A}\ \wedge\text{-}EL$$

$$\frac{A \wedge B}{B}\ \wedge\text{-}ER \qquad \frac{\begin{matrix}[A]\\ \vdots \\ B\end{matrix}}{A \rightarrow B}\ \rightarrow\text{-}I$$

$$\frac{A \rightarrow B \quad A}{B}\ \rightarrow\text{-}E$$

Proof:

$$\cfrac{\cfrac{\cfrac{[A \wedge B]^1}{B}\ \wedge\text{-}EL \qquad \cfrac{[A \wedge B]^1}{A}\ \wedge\text{-}ER}{B \wedge A}\ \wedge\text{-}I}{A \wedge B \rightarrow B \wedge A}\ \rightarrow\text{-}I^1$$

Alternative Formalization Using Sequents

Rules (for $\rightarrow$ /$\wedge$ fragment). Here, Γ is a set of formulae.

$$\Gamma \vdash A \quad (\text{where } A \in \Gamma)$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge\text{-}I \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \wedge\text{-}EL \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \wedge\text{-}ER$$

$$\frac{A, \Gamma \vdash B}{\Gamma \vdash A \rightarrow B}\ \rightarrow\text{-}I \qquad \frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B}\ \rightarrow\text{-}E$$

Two representations equivalent. Sequent notation seems simpler in practice.

Example: Refinement Style with Metavariables

$$\frac{\dfrac{A \wedge (B \wedge C) \vdash A \wedge ?X}{A \wedge (B \wedge C) \vdash A} \qquad \dfrac{\dfrac{A \wedge (B \wedge C) \vdash ?Z \wedge (?Y \wedge C)}{A \wedge (B \wedge C) \vdash (?Y \wedge C)}}{A \wedge (B \wedge C) \vdash C}}{\dfrac{A \wedge (B \wedge C) \vdash A \wedge C}{\vdash A \wedge (B \wedge C) \rightarrow A \wedge C}}$$

Solution for $?Z = A$, $?Y = B$ and $?X = (B \wedge C)$.

We went through this example in detail last lecture.

Comments about Refinement

This crazy way of carrying out proofs is the (standard) Isabelle-way!

- Refinement style means we work from goals to axioms
- Metavariables used to delay commitments

Isabelle allows other refinements/alternatives too (see labs).

More Detailed Explanations

What are ND Systems and Proofs?

ND stands for Natural Deduction. It was explained in the previous lecture.

What is Sequent Notation?

The judgement $(\Gamma \vdash \phi)$ means that we can derive ϕ from the assumptions in Γ using certain rules. As, explained in the previous lecture, one can make such judgements the central objects of the deductive system.

Sequent Notation and Isabelle

In particular, the sequent style notation is more amenable to automation, and thus it is closer to what happens in Isabelle.

References

[Gen35] Gerhard Gentzen. Untersuchungen über das logische Schliessen. *Mathematische Zeitschrift*, 39:176–210, 405–431, 1935. English translation in [Sza69].

[Pra65] Dag Prawitz. *Natural Deduction: A proof theoretical study*. Almqvist and Wiksell, 1965.

[Sza69] M. E. Szabo. *The Collected Papers of Gerhard Gentzen*. North-Holland, 1969.