HOL: Propositional Logic

Overview

- Natural deduction
- Rule application in Isabelle/HOL

Rule notation

$$\frac{A_1 \ldots A_n}{A} \quad \text{instead of} \quad [\![A_1 \ldots A_n]\!] \Longrightarrow A$$

Natural Deduction

Natural deduction

Two kinds of rules for each logical operator $\oplus$:

Natural deduction

Two kinds of rules for each logical operator $\oplus$:

Introduction: how can I prove $A \oplus B$?

Natural deduction

Two kinds of rules for each logical operator $\oplus$:

Introduction: how can I prove $A \oplus B$?

Elimination: what can I prove from $A \oplus B$?

Natural deduction for propositional logic

$$\frac{\qquad}{A \wedge B}\ \texttt{conjI} \qquad\qquad \frac{\qquad\qquad}{\qquad}\ \texttt{conjE}$$

$$\frac{\qquad}{\qquad}\quad \frac{\qquad}{\qquad}\ \texttt{disjI1/2} \qquad\qquad \frac{\qquad\qquad}{\qquad}\ \texttt{disjE}$$

$$\frac{\qquad}{\qquad}\ \texttt{impI} \qquad\qquad \frac{\qquad\qquad}{\qquad}\ \texttt{impE}$$

$$\frac{\qquad\qquad}{\qquad}\ \texttt{iffI} \qquad\qquad \frac{\qquad}{\qquad}\ \texttt{iffD1} \qquad \frac{\qquad}{\qquad}\ \texttt{iffD2}$$

$$\frac{\qquad}{\qquad}\ \texttt{notI} \qquad\qquad \frac{\qquad}{\qquad}\ \texttt{notE}$$

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}$$ conjI

——— conjE

——— ——— disjI1/2

——— disjE

——— impI

——— impE

——— iffI

——— iffD1 ——— iffD2

——— notI

——— notE

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}$$ conjI

$$\frac{\qquad}{\qquad}$$ conjE

$$\frac{}{A \vee B} \quad \frac{}{A \vee B}$$ disjI1/2

$$\frac{\qquad}{\qquad}$$ disjE

$$\frac{\qquad}{\qquad}$$ impI

$$\frac{\qquad}{\qquad}$$ impE

$$\frac{\qquad}{\qquad}$$ iffI

$$\frac{\qquad}{\qquad}$$ iffD1

$$\frac{\qquad}{\qquad}$$ iffD2

$$\frac{\qquad}{\qquad}$$ notI

$$\frac{\qquad}{\qquad}$$ notE

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}$$ `conjI`

$$\frac{}{}$$ `conjE`

$$\frac{A}{A \vee B} \quad \frac{B}{A \vee B}$$ `disjI1/2`

$$\frac{}{}$$ `disjE`

$$\frac{}{}$$ `impI`

$$\frac{}{}$$ `impE`

$$\frac{}{}$$ `iffI`

$$\frac{}{}$$ `iffD1`

$$\frac{}{}$$ `iffD2`

$$\frac{}{}$$ `notI`

$$\frac{}{}$$ `notE`

Natural deduction for propositional logic

$$\frac{A \qquad B}{A \wedge B}\ \texttt{conjI} \qquad\qquad \frac{\qquad\qquad}{\qquad\qquad}\ \texttt{conjE}$$

$$\frac{A}{A \vee B}\ \frac{B}{A \vee B}\ \texttt{disjI1/2} \qquad\qquad \frac{\qquad\qquad}{\qquad\qquad}\ \texttt{disjE}$$

$$\frac{}{A \longrightarrow B}\ \texttt{impI} \qquad\qquad \frac{\qquad\qquad}{\qquad\qquad}\ \texttt{impE}$$

$$\frac{\qquad\qquad}{\qquad\qquad}\ \texttt{iffI} \qquad\qquad \frac{\qquad}{\qquad}\ \texttt{iffD1} \qquad \frac{\qquad}{\qquad}\ \texttt{iffD2}$$

$$\frac{\qquad\qquad}{\qquad\qquad}\ \texttt{notI} \qquad\qquad \frac{\qquad}{\qquad}\ \texttt{notE}$$

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}\ \texttt{conjI} \qquad \frac{\quad}{\quad}\ \texttt{conjE}$$

$$\frac{A}{A \vee B}\ \frac{B}{A \vee B}\ \texttt{disjI1/2} \qquad \frac{\quad}{\quad}\ \texttt{disjE}$$

$$\frac{A \Longrightarrow B}{A \longrightarrow B}\ \texttt{impI} \qquad \frac{\quad}{\quad}\ \texttt{impE}$$

$$\frac{\quad}{\quad}\ \texttt{iffI} \qquad \frac{\quad}{\quad}\ \texttt{iffD1} \qquad \frac{\quad}{\quad}\ \texttt{iffD2}$$

$$\frac{\quad}{\quad}\ \texttt{notI} \qquad \frac{\quad}{\quad}\ \texttt{notE}$$

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}$$ conjI

$$\frac{\qquad\qquad}{}$$ conjE

$$\frac{A}{A \vee B} \quad \frac{B}{A \vee B}$$ disjI1/2

$$\frac{\qquad\qquad}{}$$ disjE

$$\frac{A \Longrightarrow B}{A \longrightarrow B}$$ impI

$$\frac{\qquad\qquad}{}$$ impE

$$\frac{\qquad\qquad}{A = B}$$ iffI

$$\frac{\qquad\qquad}{}$$ iffD1

$$\frac{\qquad\qquad}{}$$ iffD2

$$\frac{\qquad\qquad}{}$$ notI

$$\frac{\qquad\qquad}{}$$ notE

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}\ \texttt{conjI} \qquad \frac{\qquad}{\qquad}\ \texttt{conjE}$$

$$\frac{A}{A \vee B}\ \frac{B}{A \vee B}\ \texttt{disjI1/2} \qquad \frac{\qquad}{\qquad}\ \texttt{disjE}$$

$$\frac{A \Longrightarrow B}{A \longrightarrow B}\ \texttt{impI} \qquad \frac{\qquad}{\qquad}\ \texttt{impE}$$

$$\frac{A \Longrightarrow B \quad B \Longrightarrow A}{A = B}\ \texttt{iffI} \qquad \frac{\qquad}{\qquad}\ \texttt{iffD1} \quad \frac{\qquad}{\qquad}\ \texttt{iffD2}$$

$$\frac{\qquad}{\qquad}\ \texttt{notI} \qquad \frac{\qquad}{\qquad}\ \texttt{notE}$$

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}\ \texttt{conjI} \qquad\qquad \frac{\qquad\qquad}{}\ \texttt{conjE}$$

$$\frac{A}{A \vee B}\ \ \frac{B}{A \vee B}\ \texttt{disjI1/2} \qquad\qquad \frac{\qquad\qquad}{}\ \texttt{disjE}$$

$$\frac{A \Longrightarrow B}{A \longrightarrow B}\ \texttt{impI} \qquad\qquad \frac{\qquad\qquad}{}\ \texttt{impE}$$

$$\frac{A \Longrightarrow B \quad B \Longrightarrow A}{A = B}\ \texttt{iffI} \qquad\qquad \frac{\qquad}{}\ \texttt{iffD1} \qquad \frac{\qquad}{}\ \texttt{iffD2}$$

$$\frac{\qquad\qquad}{\neg A}\ \texttt{notI} \qquad\qquad \frac{\qquad}{}\ \texttt{notE}$$

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}\ \texttt{conjI} \qquad\qquad \overline{\qquad\qquad\qquad}\ \texttt{conjE}$$

$$\frac{A}{A \vee B}\ \frac{B}{A \vee B}\ \texttt{disjI1/2} \qquad\qquad \overline{\qquad\qquad\qquad}\ \texttt{disjE}$$

$$\frac{A \Longrightarrow B}{A \longrightarrow B}\ \texttt{impI} \qquad\qquad \overline{\qquad\qquad\qquad}\ \texttt{impE}$$

$$\frac{A \Longrightarrow B \quad B \Longrightarrow A}{A = B}\ \texttt{iffI} \qquad\qquad \overline{\qquad\qquad}\ \texttt{iffD1} \qquad \overline{\qquad\qquad}\ \texttt{iffD2}$$

$$\frac{A \Longrightarrow False}{\neg A}\ \texttt{notI} \qquad\qquad \overline{\qquad\qquad}\ \texttt{notE}$$

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}\ \texttt{conjI} \qquad \frac{A \wedge B}{C}\ \texttt{conjE}$$

$$\frac{A}{A \vee B} \quad \frac{B}{A \vee B}\ \texttt{disjI1/2} \qquad \frac{\qquad}{}\ \texttt{disjE}$$

$$\frac{A \Longrightarrow B}{A \longrightarrow B}\ \texttt{impI} \qquad \frac{\qquad}{}\ \texttt{impE}$$

$$\frac{A \Longrightarrow B \quad B \Longrightarrow A}{A = B}\ \texttt{iffI} \qquad \frac{\qquad}{}\ \texttt{iffD1} \qquad \frac{\qquad}{}\ \texttt{iffD2}$$

$$\frac{A \Longrightarrow False}{\neg A}\ \texttt{notI} \qquad \frac{\qquad}{}\ \texttt{notE}$$

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}\ \texttt{conjI} \qquad \frac{A \wedge B \quad [\![A;B]\!] \Longrightarrow C}{C}\ \texttt{conjE}$$

$$\frac{A}{A \vee B}\ \frac{B}{A \vee B}\ \texttt{disjI1/2} \qquad \frac{\qquad}{\qquad}\ \texttt{disjE}$$

$$\frac{A \Longrightarrow B}{A \longrightarrow B}\ \texttt{impI} \qquad \frac{\qquad}{\qquad}\ \texttt{impE}$$

$$\frac{A \Longrightarrow B \quad B \Longrightarrow A}{A = B}\ \texttt{iffI} \qquad \frac{\qquad}{\qquad}\ \texttt{iffD1} \qquad \frac{\qquad}{\qquad}\ \texttt{iffD2}$$

$$\frac{A \Longrightarrow False}{\neg A}\ \texttt{notI} \qquad \frac{\qquad}{\qquad}\ \texttt{notE}$$

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}\ \texttt{conjI} \qquad \frac{A \wedge B \quad [\![A;B]\!] \Longrightarrow C}{C}\ \texttt{conjE}$$

$$\frac{A}{A \vee B}\ \frac{B}{A \vee B}\ \texttt{disjI1/2} \qquad \frac{A \vee B}{C}\ \texttt{disjE}$$

$$\frac{A \Longrightarrow B}{A \longrightarrow B}\ \texttt{impI} \qquad \frac{}{}\ \texttt{impE}$$

$$\frac{A \Longrightarrow B \quad B \Longrightarrow A}{A = B}\ \texttt{iffI} \qquad \frac{}{}\ \texttt{iffD1} \qquad \frac{}{}\ \texttt{iffD2}$$

$$\frac{A \Longrightarrow False}{\neg A}\ \texttt{notI} \qquad \frac{}{}\ \texttt{notE}$$

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}\ \texttt{conjI} \qquad \frac{A \wedge B \quad [\![A;B]\!] \Longrightarrow C}{C}\ \texttt{conjE}$$

$$\frac{A}{A \vee B}\ \frac{B}{A \vee B}\ \texttt{disjI1/2} \qquad \frac{A \vee B \quad A \Longrightarrow C \quad B \Longrightarrow C}{C}\ \texttt{disjE}$$

$$\frac{A \Longrightarrow B}{A \longrightarrow B}\ \texttt{impI} \qquad \frac{}{}\ \texttt{impE}$$

$$\frac{A \Longrightarrow B \quad B \Longrightarrow A}{A = B}\ \texttt{iffI} \qquad \frac{}{}\ \texttt{iffD1} \qquad \frac{}{}\ \texttt{iffD2}$$

$$\frac{A \Longrightarrow False}{\neg A}\ \texttt{notI} \qquad \frac{}{}\ \texttt{notE}$$

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}\ \texttt{conjI} \qquad \frac{A \wedge B \quad [\![A;B]\!] \Longrightarrow C}{C}\ \texttt{conjE}$$

$$\frac{A}{A \vee B}\ \frac{B}{A \vee B}\ \texttt{disjI1/2} \qquad \frac{A \vee B \quad A \Longrightarrow C \quad B \Longrightarrow C}{C}\ \texttt{disjE}$$

$$\frac{A \Longrightarrow B}{A \longrightarrow B}\ \texttt{impI} \qquad \frac{A \longrightarrow B}{C}\ \texttt{impE}$$

$$\frac{A \Longrightarrow B \quad B \Longrightarrow A}{A = B}\ \texttt{iffI} \qquad \frac{}{}\ \texttt{iffD1} \qquad \frac{}{}\ \texttt{iffD2}$$

$$\frac{A \Longrightarrow False}{\neg A}\ \texttt{notI} \qquad \frac{}{}\ \texttt{notE}$$

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}\ \texttt{conjI} \qquad \frac{A \wedge B \quad [\![A;B]\!] \Longrightarrow C}{C}\ \texttt{conjE}$$

$$\frac{A}{A \vee B}\ \frac{B}{A \vee B}\ \texttt{disjI1/2} \qquad \frac{A \vee B \quad A \Longrightarrow C \quad B \Longrightarrow C}{C}\ \texttt{disjE}$$

$$\frac{A \Longrightarrow B}{A \longrightarrow B}\ \texttt{impI} \qquad \frac{A \longrightarrow B \quad A \quad B \Longrightarrow C}{C}\ \texttt{impE}$$

$$\frac{A \Longrightarrow B \quad B \Longrightarrow A}{A = B}\ \texttt{iffI} \qquad \frac{}{}\ \texttt{iffD1} \qquad \frac{}{}\ \texttt{iffD2}$$

$$\frac{A \Longrightarrow False}{\neg A}\ \texttt{notI} \qquad \frac{}{}\ \texttt{notE}$$

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}\ \texttt{conjI} \qquad \frac{A \wedge B \quad [\![A;B]\!] \Longrightarrow C}{C}\ \texttt{conjE}$$

$$\frac{A}{A \vee B}\ \frac{B}{A \vee B}\ \texttt{disjI1/2} \qquad \frac{A \vee B \quad A \Longrightarrow C \quad B \Longrightarrow C}{C}\ \texttt{disjE}$$

$$\frac{A \Longrightarrow B}{A \longrightarrow B}\ \texttt{impI} \qquad \frac{A \longrightarrow B \quad A \quad B \Longrightarrow C}{C}\ \texttt{impE}$$

$$\frac{A \Longrightarrow B \quad B \Longrightarrow A}{A = B}\ \texttt{iffI} \qquad \frac{A{=}B}{\quad}\ \texttt{iffD1} \qquad \frac{A{=}B}{\quad}\ \texttt{iffD2}$$

$$\frac{A \Longrightarrow False}{\neg A}\ \texttt{notI} \qquad \frac{\quad}{\quad}\ \texttt{notE}$$

Natural deduction for propositional logic

$$\frac{A \quad B}{A \land B}\ \texttt{conjI} \qquad \frac{A \land B \quad [\![A;B]\!] \Longrightarrow C}{C}\ \texttt{conjE}$$

$$\frac{A}{A \lor B}\ \frac{B}{A \lor B}\ \texttt{disjI1/2} \qquad \frac{A \lor B \quad A \Longrightarrow C \quad B \Longrightarrow C}{C}\ \texttt{disjE}$$

$$\frac{A \Longrightarrow B}{A \longrightarrow B}\ \texttt{impI} \qquad \frac{A \longrightarrow B \quad A \quad B \Longrightarrow C}{C}\ \texttt{impE}$$

$$\frac{A \Longrightarrow B \quad B \Longrightarrow A}{A = B}\ \texttt{iffI} \qquad \frac{A{=}B}{A \Longrightarrow B}\ \texttt{iffD1} \quad \frac{A{=}B}{B \Longrightarrow A}\ \texttt{iffD2}$$

$$\frac{A \Longrightarrow False}{\neg A}\ \texttt{notI} \qquad \frac{}{}\ \texttt{notE}$$

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}\ \texttt{conjI} \qquad \frac{A \wedge B \quad [\![A;B]\!] \Longrightarrow C}{C}\ \texttt{conjE}$$

$$\frac{A}{A \vee B}\ \frac{B}{A \vee B}\ \texttt{disjI1/2} \qquad \frac{A \vee B \quad A \Longrightarrow C \quad B \Longrightarrow C}{C}\ \texttt{disjE}$$

$$\frac{A \Longrightarrow B}{A \longrightarrow B}\ \texttt{impI} \qquad \frac{A \longrightarrow B \quad A \quad B \Longrightarrow C}{C}\ \texttt{impE}$$

$$\frac{A \Longrightarrow B \quad B \Longrightarrow A}{A = B}\ \texttt{iffI} \qquad \frac{A{=}B}{A \Longrightarrow B}\ \texttt{iffD1} \quad \frac{A{=}B}{B \Longrightarrow A}\ \texttt{iffD2}$$

$$\frac{A \Longrightarrow False}{\neg A}\ \texttt{notI} \qquad \frac{\neg A \quad A}{C}\ \texttt{notE}$$

Natural deduction for propositional logic

$$\frac{A \quad B}{A \wedge B}\ \texttt{conjI} \qquad \frac{A \wedge B \quad [\![A;B]\!] \Longrightarrow C}{C}\ \texttt{conjE}$$

$$\frac{A}{A \vee B}\ \frac{B}{A \vee B}\ \texttt{disjI1/2} \qquad \frac{A \vee B \quad A \Longrightarrow C \quad B \Longrightarrow C}{C}\ \texttt{disjE}$$

$$\frac{A \Longrightarrow B}{A \longrightarrow B}\ \texttt{impI} \qquad \frac{A \longrightarrow B \quad A \quad B \Longrightarrow C}{C}\ \texttt{impE}$$

$$\frac{A \Longrightarrow B \quad B \Longrightarrow A}{A = B}\ \texttt{iffI} \qquad \frac{A{=}B}{A \Longrightarrow B}\ \texttt{iffD1} \quad \frac{A{=}B}{B \Longrightarrow A}\ \texttt{iffD2}$$

$$\frac{A \Longrightarrow \mathit{False}}{\neg A}\ \texttt{notI} \qquad \frac{\neg A \quad A}{C}\ \texttt{notE}$$

Operational reading

$$\frac{A_1 \ldots A_n}{A}$$

Operational reading

$$\frac{A_1 \ldots A_n}{A}$$

Introduction rule:

To prove A it suffices to prove $A_1 \ldots A_n$.

Operational reading

$$\frac{A_1 \ldots A_n}{A}$$

Introduction rule:

To prove A it suffices to prove $A_1 \ldots A_n$.

Elimination rule

If I know A_1 and want to prove A
it suffices to prove $A_2 \ldots A_n$.

Equality

$$\frac{}{t = t}\ \texttt{refl} \qquad \frac{s = t}{t = s}\ \texttt{sym} \qquad \frac{r = s \quad s = t}{r = t}\ \texttt{trans}$$

Equality

$$\frac{}{t = t}\ \texttt{refl} \qquad \frac{s = t}{t = s}\ \texttt{sym} \qquad \frac{r = s \quad s = t}{r = t}\ \texttt{trans}$$

$$\frac{s = t \quad A(s)}{A(t)}\ \texttt{subst}$$

Equality

$$\frac{}{t = t}\ \texttt{refl} \qquad \frac{s = t}{t = s}\ \texttt{sym} \qquad \frac{r = s \quad s = t}{r = t}\ \texttt{trans}$$

$$\frac{s = t \quad A(s)}{A(t)}\ \texttt{subst}$$

Rarely needed explicitly — used implicitly by *simp*

More rules

$$\frac{A \longrightarrow B \quad A}{B}\ \texttt{mp}$$

More rules

$$\frac{A \longrightarrow B \quad A}{B}\ \texttt{mp}$$

$$\frac{\neg A \Longrightarrow False}{A}\ \texttt{ccontr} \qquad \frac{\neg A \Longrightarrow A}{A}\ \texttt{classical}$$

More rules

$$\frac{A \longrightarrow B \quad A}{B}\ \texttt{mp}$$

$$\frac{\neg\, A \Longrightarrow \mathit{False}}{A}\ \texttt{ccontr} \qquad \frac{\neg\, A \Longrightarrow A}{A}\ \texttt{classical}$$

Remark:

`ccontr` and `classical` are not derivable from the ND-rules.

More rules

$$\frac{A \longrightarrow B \quad A}{B}\ \texttt{mp}$$

$$\frac{\neg A \Longrightarrow \mathit{False}}{A}\ \texttt{ccontr} \qquad \frac{\neg A \Longrightarrow A}{A}\ \texttt{classical}$$

Remark:

`ccontr` and `classical` are not derivable from the ND-rules.

They make the logic “classical”, i.e. “non-constructive”.

Proof by assumption

$$\frac{A_1 \quad \ldots \quad A_n}{A_i}\ \texttt{assumption}$$

Rule application: the rough idea

Applying rule $[\![A_1; \ldots ; A_n]\!] \Longrightarrow A$ to subgoal C:

Rule application: the rough idea

Applying rule $[\![A_1; \ldots ; A_n]\!] \Longrightarrow A$ to subgoal C:

- Unify A and C

Rule application: the rough idea

Applying rule $\llbracket A_1; \ldots ; A_n \rrbracket \Longrightarrow A$ to subgoal C:

- Unify A and C
- Replace C with n new subgoals $A_1 \ldots A_n$

Rule application: the rough idea

Applying rule $[\![A_1; \ldots ; A_n]\!] \Longrightarrow A$ to subgoal C:

- Unify A and C
- Replace C with n new subgoals $A_1 \ldots A_n$

Working backwards, like in Prolog!

Rule application: the rough idea

Applying rule $[\![A_1; \ldots ; A_n]\!] \Longrightarrow A$ to subgoal C:

- Unify A and C
- Replace C with n new subgoals $A_1 \ldots A_n$

Working backwards, like in Prolog!

Example: rule: $[\![?P; ?Q]\!] \Longrightarrow ?P \wedge ?Q$

subgoal: *1.* $A \wedge B$

Rule application: the rough idea

Applying rule $[\![A_1; \ldots ; A_n]\!] \Longrightarrow A$ to subgoal C:

- Unify A and C
- Replace C with n new subgoals $A_1 \ldots A_n$

Working backwards, like in Prolog!

Example: rule: $[\![?P; ?Q]\!] \Longrightarrow ?P \wedge ?Q$

subgoal: *1.* $A \wedge B$

Result: *1.* A

2. B

Rule application: the details

Rule: $[\![A_1; \ldots ; A_n]\!] \Longrightarrow A$

Subgoal: 1. $[\![B_1; \ldots ; B_m]\!] \Longrightarrow C$

Rule application: the details

Rule:	$[\![A_1; \ldots ; A_n]\!] \Longrightarrow A$
Subgoal:	1. $[\![B_1; \ldots ; B_m]\!] \Longrightarrow C$
Substitution:	$\sigma(A) \equiv \sigma(C)$

Rule application: the details

Rule:	$[\![A_1; \ldots ; A_n]\!] \Longrightarrow A$
Subgoal:	1. $[\![B_1; \ldots ; B_m]\!] \Longrightarrow C$
Substitution:	$\sigma(A) \equiv \sigma(C)$
New subgoals:	1. $\sigma([\![B_1; \ldots ; B_m]\!] \Longrightarrow A_1)$
	$\vdots$
	n. $\sigma([\![B_1; \ldots ; B_m]\!] \Longrightarrow A_n)$

Rule application: the details

Rule: $[\![A_1; \ldots ; A_n]\!] \Longrightarrow A$

Subgoal: 1. $[\![B_1; \ldots ; B_m]\!] \Longrightarrow C$

Substitution: $\sigma(A) \equiv \sigma(C)$

New subgoals: 1. $\sigma([\![B_1; \ldots ; B_m]\!] \Longrightarrow A_1)$

$\vdots$

n. $\sigma([\![B_1; \ldots ; B_m]\!] \Longrightarrow A_n)$

Command:

apply(*rule <rulename>*)

Proof by assumption

apply *assumption*

proves

$$1.\ \llbracket B_1; \ldots ; B_m \rrbracket \Longrightarrow C$$

by unifying C with one of the B_i

Proof by assumption

apply *assumption*

proves

1. $[\![B_1; \ldots ; B_m]\!] \Longrightarrow C$

by unifying *C* with one of the B_i (backtracking!)

Applying elimination rules

apply*(erule <elim-rule>)*

Like *rule* but also

- unifies first premise of rule with an assumption
- eliminates that assumption

Applying elimination rules

apply*(erule <elim-rule>)*

Like *rule* but also

- unifies first premise of rule with an assumption
- eliminates that assumption

Example:

Rule: $[\![?P \wedge ?Q; [\![?P; ?Q]\!] \Longrightarrow ?R]\!] \Longrightarrow ?R$

Subgoal: $1.\ [\![X; A \wedge B; Y]\!] \Longrightarrow Z$

Applying elimination rules

apply(*erule <elim-rule>*)

Like *rule* but also

- unifies first premise of rule with an assumption
- eliminates that assumption

Example:

Rule: $[\![?P \wedge ?Q; [\![?P; ?Q]\!] \Longrightarrow ?R]\!] \Longrightarrow ?R$

Subgoal: $1.\ [\![X; A \wedge B; Y]\!] \Longrightarrow Z$

Unification: $?P \wedge ?Q \equiv A \wedge B$ and $?R \equiv Z$

Applying elimination rules

apply(*erule <elim-rule>*)

Like *rule* but also

- unifies first premise of rule with an assumption
- eliminates that assumption

Example:

Rule: $[\![?P \wedge ?Q; [\![?P; ?Q]\!] \Longrightarrow ?R]\!] \Longrightarrow ?R$

Subgoal: $1.\ [\![\ X; A \wedge B; Y\ ]\!] \Longrightarrow Z$

Unification: $?P \wedge ?Q \equiv A \wedge B$ and $?R \equiv Z$

New subgoal: $1.\ [\![\ X; Y\ ]\!] \Longrightarrow [\![\ A; B\ ]\!] \Longrightarrow Z$

Applying elimination rules

apply(*erule <elim-rule>*)

Like *rule* but also

- unifies first premise of rule with an assumption
- eliminates that assumption

Example:

Rule: $\llbracket ?P \wedge ?Q; \llbracket ?P; ?Q \rrbracket \Longrightarrow ?R \rrbracket \Longrightarrow ?R$

Subgoal: $1.\ \llbracket X; A \wedge B; Y \rrbracket \Longrightarrow Z$

Unification: $?P \wedge ?Q \equiv A \wedge B$ and $?R \equiv Z$

New subgoal: $1.\ \llbracket X; Y \rrbracket \Longrightarrow \llbracket A; B \rrbracket \Longrightarrow Z$

same as: $1.\ \llbracket X; Y; A; B \rrbracket \Longrightarrow Z$

How to prove it by natural deduction

- Intro rules decompose formulae to the right of $\Longrightarrow$.

  apply(*rule <intro-rule>*)

How to prove it by natural deduction

- Intro rules decompose formulae to the right of $\Longrightarrow$.

  apply_(rule <intro-rule>)_

- Elim rules decompose formulae on the left of $\Longrightarrow$.

  apply_(erule <elim-rule>)_

Demo: propositional proofs

$\Longrightarrow$ vs $\longrightarrow$

To facilitate application of theorems:

write them like this $[\![A_1; \ldots; A_n]\!] \Longrightarrow A$

not like this $A_1 \wedge \ldots \wedge A_n \longrightarrow A$

HOL: Predicate Logic

Parameters

Subgoal:

1. $\bigwedge x_1 \ldots x_n$. *Formula*

The x_i are called parameters of the subgoal.
Intuition: local constants, i.e. arbitrary but fixed values.

Parameters

Subgoal:

1. $\bigwedge x_1 \ldots x_n$. *Formula*

The x_i are called parameters of the subgoal.
Intuition: local constants, i.e. arbitrary but fixed values.

Rules are automatically lifted over $\bigwedge x_1 \ldots x_n$ and applied directly to *Formula*.

Scope

- Scope of parameters: whole subgoal
- Scope of $\forall$, $\exists$, $\ldots$: ends with *;* or $\Longrightarrow$

Scope

- Scope of parameters: whole subgoal
- Scope of $\forall$, $\exists$, $\ldots$: ends with *;* or $\Longrightarrow$

$$\bigwedge x\ y.\ [\![\ \forall y.\ P\ y \longrightarrow Q\ z\ y;\ \ Q\ x\ y\ ]\!] \Longrightarrow \exists x.\ Q\ x\ y$$

means

$$\bigwedge x\ y.\ [\![\ (\forall y_1.\ P\ y_1 \longrightarrow Q\ z\ y_1);\ \ Q\ x\ y\ ]\!] \Longrightarrow \exists x_1.\ Q\ x_1\ y$$

α-Conversion

Bound variables are renamed automatically to avoid name clashes with other variables.

Natural deduction for quantifiers

$$\frac{}{\forall x.\ P(x)}\ \texttt{allI} \qquad \frac{}{}\ \texttt{allE}$$

$$\frac{}{}\ \texttt{exI} \qquad \frac{}{}\ \texttt{exE}$$

Natural deduction for quantifiers

$$\frac{\bigwedge x.\ P(x)}{\forall x.\ P(x)}\ \texttt{allI} \qquad \frac{}{}\ \texttt{allE}$$

$$\frac{}{}\ \texttt{exI} \qquad \frac{}{}\ \texttt{exE}$$

Natural deduction for quantifiers

$$\frac{\bigwedge x.\ P(x)}{\forall x.\ P(x)}\ \texttt{allI} \qquad \frac{}{\quad}\ \texttt{allE}$$

$$\frac{}{\exists x.\ P(x)}\ \texttt{exI} \qquad \frac{}{\quad}\ \texttt{exE}$$

Natural deduction for quantifiers

$$\frac{\bigwedge x.\ P(x)}{\forall x.\ P(x)}\ \texttt{allI} \qquad \frac{}{}\ \texttt{allE}$$

$$\frac{P(?x)}{\exists x.\ P(x)}\ \texttt{exI} \qquad \frac{}{}\ \texttt{exE}$$

Natural deduction for quantifiers

$$\frac{\bigwedge x.\ P(x)}{\forall x.\ P(x)}\ \texttt{allI} \qquad \frac{\forall x.\ P(x) \qquad\qquad\qquad\qquad}{R}\ \texttt{allE}$$

$$\frac{P(?x)}{\exists x.\ P(x)}\ \texttt{exI} \qquad \frac{\qquad\qquad\qquad\qquad\qquad\qquad}{}\ \texttt{exE}$$

Natural deduction for quantifiers

$$\frac{\bigwedge x.\ P(x)}{\forall x.\ P(x)}\ \texttt{allI} \qquad \frac{\forall x.\ P(x) \quad P(?x) \Longrightarrow R}{R}\ \texttt{allE}$$

$$\frac{P(?x)}{\exists x.\ P(x)}\ \texttt{exI} \qquad \frac{\qquad\qquad\qquad}{}\ \texttt{exE}$$

Natural deduction for quantifiers

$$\frac{\bigwedge x.\ P(x)}{\forall x.\ P(x)}\ \texttt{allI} \qquad \frac{\forall x.\ P(x) \quad P(?x) \Longrightarrow R}{R}\ \texttt{allE}$$

$$\frac{P(?x)}{\exists x.\ P(x)}\ \texttt{exI} \qquad \frac{\exists x.\ P(x)}{R}\ \texttt{exE}$$

Natural deduction for quantifiers

$$\frac{\bigwedge x.\ P(x)}{\forall x.\ P(x)}\ \texttt{allI} \qquad \frac{\forall x.\ P(x) \quad P(?x) \Longrightarrow R}{R}\ \texttt{allE}$$

$$\frac{P(?x)}{\exists x.\ P(x)}\ \texttt{exI} \qquad \frac{\exists x.\ P(x) \quad \bigwedge x.\ P(x) \Longrightarrow R}{R}\ \texttt{exE}$$

Natural deduction for quantifiers

$$\frac{\bigwedge x.\ P(x)}{\forall x.\ P(x)}\ \texttt{allI} \qquad \frac{\forall x.\ P(x) \quad P(?x) \Longrightarrow R}{R}\ \texttt{allE}$$

$$\frac{P(?x)}{\exists x.\ P(x)}\ \texttt{exI} \qquad \frac{\exists x.\ P(x) \quad \bigwedge x.\ P(x) \Longrightarrow R}{R}\ \texttt{exE}$$

- `allI` and `exE` introduce new parameters ($\bigwedge x$).

Natural deduction for quantifiers

$$\frac{\bigwedge x.\ P(x)}{\forall x.\ P(x)}\ \texttt{allI} \qquad \frac{\forall x.\ P(x) \quad P(?x) \Longrightarrow R}{R}\ \texttt{allE}$$

$$\frac{P(?x)}{\exists x.\ P(x)}\ \texttt{exI} \qquad \frac{\exists x.\ P(x) \quad \bigwedge x.\ P(x) \Longrightarrow R}{R}\ \texttt{exE}$$

- `allI` and `exE` introduce new parameters ($\bigwedge x$).
- `allE` and `exI` introduce new unknowns ($?x$).

Instantiating rules

apply(*rule_tac x* = $term$ *in* $rule$)

Like *rule*, but *?x* in $rule$ is instantiated by $term$ before application.

Instantiating rules

apply(*rule_tac x* = $term$ *in* $rule$)

Like *rule*, but *?x* in $rule$ is instantiated by $term$ before application.

Similar: *erule_tac*

Instantiating rules

apply(*rule_tac x* = $term$ *in* $rule$)

Like *rule*, but *?x* in $rule$ is instantiated by $term$ before application.

Similar: *erule_tac*

! *x* is in $rule$, not in the goal **!**

A quantifier proof

1. $\forall a.\ \exists b.\ a = b$

A quantifier proof

1. $\forall a.\ \exists b.\ a = b$

apply*(rule allI)*

A quantifier proof

1. $\forall a.\ \exists b.\ a = b$

apply*(rule allI)*

1. $\bigwedge a.\ \exists b.\ a = b$

A quantifier proof

1. $\forall$ *a.* $\exists$ *b. a = b*

apply*(rule allI)*

1. $\bigwedge$*a.* $\exists$ *b. a = b*

apply*(rule_tac x = "a" in exI)*

A quantifier proof

1. $\forall a.\ \exists b.\ a = b$

apply*(rule allI)*

1. $\bigwedge a.\ \exists b.\ a = b$

apply*(rule_tac x = "a" in exI)*

1. $\bigwedge a.\ a = a$

A quantifier proof

1. $\forall a.\ \exists b.\ a = b$

apply*(rule allI)*

1. $\bigwedge a.\ \exists b.\ a = b$

apply*(rule_tac x = "a" in exI)*

1. $\bigwedge a.\ a = a$

apply*(rule refl)*

Demo: quantifier proofs

More proof methods

Forward proofs: frule and drule

“Forward” rule: $A_1 \Longrightarrow A$

Subgoal: 1. $[\![B_1; \ldots ; B_n]\!] \Longrightarrow C$

Forward proofs: frule and drule

"Forward" rule:	$A_1 \Longrightarrow A$
Subgoal:	1. $[\![B_1; \ldots ; B_n]\!] \Longrightarrow C$
Substitution:	$\sigma(B_i) \equiv \sigma(A_1)$

Forward proofs: frule and drule

"Forward" rule:	$A_1 \Longrightarrow A$
Subgoal:	1. $[\![B_1; \ldots ; B_n]\!] \Longrightarrow C$
Substitution:	$\sigma(B_i) \equiv \sigma(A_1)$
New subgoal:	1. $\sigma([\![B_1; \ldots ; B_n; A]\!] \Longrightarrow C)$

Forward proofs: frule and drule

“Forward” rule: $A_1 \Longrightarrow A$

Subgoal: 1. $[\![B_1; \ldots ; B_n]\!] \Longrightarrow C$

Substitution: $\sigma(B_i) \equiv \sigma(A_1)$

New subgoal: 1. $\sigma([\![B_1; \ldots ; B_n; A]\!] \Longrightarrow C)$

Command:

apply(*frule* $rulename$)

Forward proofs: frule and drule

"Forward" rule:	$A_1 \Longrightarrow A$
Subgoal:	1. $[\![B_1; \ldots ; B_n]\!] \Longrightarrow C$
Substitution:	$\sigma(B_i) \equiv \sigma(A_1)$
New subgoal:	1. $\sigma([\![B_1; \ldots ; B_n; A]\!] \Longrightarrow C)$

Command:

apply(*frule* $rulename$)

Like *frule* but also deletes B_i:

apply(*drule* $rulename$)

frule and drule: the general case

Rule: $[\![A_1; \ldots ; A_m]\!] \Longrightarrow A$

Creates additional subgoals:

1. $\sigma([\![B_1; \ldots ; B_n]\!] \Longrightarrow A_2)$

$\vdots$

m-1. $\sigma([\![B_1; \ldots ; B_n]\!] \Longrightarrow A_m)$

m. $\sigma([\![B_1; \ldots ; B_n; A]\!] \Longrightarrow C)$

Forward proofs: OF

r[OF r $_1 \ldots$ *r* $_n$*]*

Prove assumption 1 of theorem *r* with theorem *r* $_1$, and assumption 2 with theorem *r* $_2$, and ...

Forward proofs: OF

$r[OF\ r_1 \ldots r_n]$

Prove assumption 1 of theorem r with theorem r_1, and assumption 2 with theorem r_2, and ...

Rule r	$[\![A_1; \ldots ; A_m]\!] \Longrightarrow A$
Rule r_1	$[\![B_1; \ldots ; B_n]\!] \Longrightarrow B$
Substitution	$\sigma(B) \equiv \sigma(A_1)$
$r[OF\ r_1]$	

Forward proofs: OF

r[OF $r_1 \ldots r_n$]

Prove assumption 1 of theorem *r* with theorem r_1, and assumption 2 with theorem r_2, and ...

Rule *r*	$[\![A_1; \ldots ; A_m]\!] \Longrightarrow A$
Rule r_1	$[\![B_1; \ldots ; B_n]\!] \Longrightarrow B$
Substitution	$\sigma(B) \equiv \sigma(A_1)$
r[OF r_1]	$\sigma([\![B_1; \ldots; B_n; A_2; \ldots; A_m]\!] \Longrightarrow A)$

Clarifying the goal

Clarifying the goal

- **apply**(*clarify*)
  Repeated application of safe rules
  without splitting the goal

Clarifying the goal

- **apply**(*clarify*)
  Repeated application of safe rules
  without splitting the goal
- **apply**(*clarsimp simp add: . . .*)
  Combination of *clarify* and *simp*.

Demo: proof methods