Automated Reasoning

Lecture 3: Natural Deduction and Starting with Isabelle

Jacques Fleuriot
jdf@inf.ed.ac.uk
Recap

- Last time I introduced **natural deduction**
- We saw the rules for $\land$ and $\lor$:

  \[
  \frac{P}{P \land Q} \quad (\text{conjI}) \quad \frac{P}{P \lor Q} \quad (\text{disjI}_1) \quad \frac{Q}{P \lor Q} \quad (\text{disjI}_2)
  \]

  \[
  \frac{P \land Q}{P} \quad (\text{conjunct}_1) \quad \frac{P \land Q}{Q} \quad (\text{conjunct}_2)
  \]

  \[
  [P] \quad [Q]
  \]

  \[
  \vdots \quad \vdots
  \]

  \[
  \frac{P \lor Q}{R} \quad R \quad R \quad (\text{disjE})
  \]

But what about the other connectives $\rightarrow$, $\leftrightarrow$ and $\neg$?
Rules for Implication

\[
\begin{array}{c}
[P] \\
\vdots \\
Q \\
\hline \\
P \rightarrow Q
\end{array}
\quad \text{(implI)}
\]

**IMPI forward**: If on the assumption that \( P \) is true, \( Q \) can be shown to hold, then we can conclude \( P \rightarrow Q \).

**IMPI backward**: To prove \( P \rightarrow Q \), assume \( P \) is true and prove that \( Q \) follows.

\[
\begin{array}{c}
P \rightarrow Q \\
P
\hline \\
Q
\end{array}
\quad \text{(mp)}
\]

The **modus ponens** rule.

\[
\begin{array}{c}
[Q] \\
\vdots \\
P \rightarrow Q \\
P \\
\hline \\
R
\end{array}
\quad \text{(impE)}
\]

Another possible implication rule is this one. Note: this is not necessarily a standard ND rule but may be useful in mechanized proofs.
Rules for $\leftrightarrow$

These rules are derivable from the rules for $\land$ and $\to$, using the abbreviation $P \leftrightarrow Q \equiv (P \to Q) \land (Q \to P)$.

Note: In Isabelle, the $\leftrightarrow$ is also denoted by $\equiv$. 
Rules for False and Negation

It is convenient to introduce a 0-ary connective \( \bot \) to represent false. The connective \( \bot \) has the rules:

\[
\frac{\bot}{P} \quad \text{(FalseE)}
\]

no introduction rule for \( \bot \)

Note: \( \bot \) is written False in Isabelle.

\[
P
data 
\vdots
abla
\bot \quad \text{(notI)}
\]

\[
P \quad \neg P
\rightarrow \bot \quad \text{(notE)}
\]

Note: we could define \( \neg P \) to be \( P \rightarrow \bot \)

Note: In Isabelle, notE is different:

\[
P \quad \neg P
\rightarrow R \quad \text{(notE)}
\]

In this course, you can use either version in your proofs.
Proof

Recall the logic problems from lecture 2: we can now prove

\[(\text{Sunny } \lor \text{ Rainy}) \land \neg \text{Sunny} \rightarrow \text{Rainy}\]

which we previously knew only by semantic means.

The subscripts \([\cdot]_1 \) and \([\cdot]_2 \) on the assumptions refer to the rule instances (also with subscripts) where they are discharged. This makes the proof easier to follow.

Note: For a full proof, the names of all the ND rules being used should be given (i.e. not just \(\text{implI} \) and \(\text{disjE} \) as in the above).
Soundness and Completeness

**Theorem (Soundness)**

*If* $Q$ *is provable from assumptions* $P_1, \ldots, P_n$, *then* $P_1, \ldots, P_n \models Q$.

This follows because all our rules are *valid*.

Is the converse true?

Can’t prove Pierce’s law: $((A \rightarrow B) \rightarrow A) \rightarrow A$

Can prove it using the *law of excluded middle*: $P \lor \neg P$.

So far, our proof system is sound and complete for Intuitionistic Logic. Intuitionistic logic rejects the law of excluded middle.
Rules for classical reasoning

Either one suffices.

Theorem (Completeness)

If \( P_1, \ldots, P_n \models Q \), then \( Q \) is provable from the assumptions \( P_1, \ldots, P_n \).

Proof: more complicated, see H&R 1.4.4.
Sequents

We have been representing proofs with assumptions like so:

\[
\begin{align*}
& P_2 \\
& P_1 \vdots P_n \\
& \vdots \vdots \ldots \vdots \\
& Q
\end{align*}
\]

Another notation is sequent-style or Fitch-style:

\[
P_1, P_2, \ldots, P_n \vdash Q
\]

The assumptions are usually collectively referred to using \( \Gamma \):

\[
\Gamma \vdash Q
\]

This style is fiddlier on paper, but easier to prove meta-theoretic properties for, and easier to represent on a computer.
Natural Deduction Sequents

New rule:

\[
\frac{P \in \Gamma}{\Gamma \vdash P} \quad \text{(assumption)}
\]

\[
\frac{\Gamma \vdash P \quad \Gamma \vdash Q}{\Gamma \vdash P \land Q} \quad \text{(conjI)}
\]

\[
\frac{\Gamma \vdash P \land Q}{\Gamma \vdash P} \quad \text{(conjunct1)}
\]

\[
\frac{\Gamma \vdash P \land Q}{\Gamma \vdash Q} \quad \text{(conjunct2)}
\]

\[
\frac{\Gamma \vdash P}{\Gamma \vdash P \lor Q} \quad \text{(disjI1)}
\]

\[
\frac{\Gamma \vdash Q}{\Gamma \vdash P \lor Q} \quad \text{(disjI2)}
\]

\[
\frac{\Gamma \vdash P \lor Q}{\Gamma \vdash P \lor Q} \quad \frac{\Gamma, P \vdash R}{\Gamma \vdash R} \quad \frac{\Gamma, Q \vdash R}{\Gamma \vdash R} \quad \text{(disjE)}
\]

\[
\frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \quad \text{(implI)}
\]

\[
\frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \quad \text{(mp)}
\]

No introduction rule for \( \bot \)

\[
\frac{\Gamma, P \vdash \bot}{\Gamma \vdash \neg P} \quad \text{(notI)}
\]

\[
\frac{\Gamma \vdash P \quad \Gamma \vdash \neg P}{\Gamma \vdash \bot} \quad \text{(notE)}
\]

\[
\frac{\Gamma \vdash \bot}{\Gamma \vdash P} \quad \text{(FalseE)}
\]

\[
\frac{\Gamma \vdash P \lor \neg P}{\Gamma \vdash \bot} \quad \text{(excluded_middle)}
\]
Natural Deduction in Isabelle/HOL

Isabelle represents the sequent $P_1, P_2, \ldots, P_n \vdash Q$ with the following notation:

$$P_1 \rightarrow (P_2 \rightarrow \ldots \rightarrow (P_n \rightarrow Q) \ldots)$$

which is also written as: $[P_1; P_2; \ldots; P_n] \rightarrow Q$

Note: To enable the bracket notation for sequents in Isabelle, select: Plugins → Plugin Options in the Isabelle JEdit menu bar. Then select Isabelle → General and enter *brackets* in the Print Mode box.

The symbol $\rightarrow$ is *meta-implication*.

Meta-implication is used to represent the relationship between premises and conclusions of rules.

$$[P]$$
$$\vdots$$
$$Q$$

$P \rightarrow Q$ is written as $(?P \rightarrow ?Q) \rightarrow (?P \rightarrow ?Q)$
Natural Deduction Rules in Isabelle

A selection of natural deduction rules in Isabelle notation:

\[
\frac{P}{P \land Q} \quad \text{(conjI)}
\]

\[
\frac{P \land Q}{P} \quad \text{(conjunct1)}
\]

\[
\frac{P}{P \lor Q} \quad \text{(disjI1)}
\]

\[
\frac{[P]}{P \lor Q} \quad \text{[?P; ?Q] \implies ?P \land ?Q}
\]

\[
\frac{[P \land ?Q]}{?P} \quad \text{[?P \land ?Q] \implies ?P}
\]

\[
\frac{[?P]}{?P \lor ?Q} \quad \text{[?P] \implies ?P \lor ?Q}
\]

\[
\frac{P \lor Q}{R \quad R} \quad \text{(disjE)}
\]

\[
\frac{[?P \lor ?Q; ?P \implies ?R; ?Q \implies ?R]}{?R}
\]
Doing Proofs in Isabelle: Theory Set-up

Syntax: \begin{verbatim}
theory MyTh
imports T_1 ... T_n
begin
  (definitions, theorems, proofs, ...)*
end
\end{verbatim}

*MyTh*: name of theory. Must live in file *MyTh.thy*

*Ti*: names of imported theories. Import is transitive.

Often: \begin{verbatim}
imports Main
\end{verbatim}
Doing Proofs in Isabelle

A declaration like so enters proof mode:

```
theorem K: "A → B → A"
```

Isabelle responds:

```
proof (prove)
```

```
goal (1 subgoal):
  1. A → B → A
```

We now apply proof methods (tactics) that affect the subgoals. Either:

▶ generate new subgoal(s), breaking the problem down; or
▶ solve the subgoal

When there are no more subgoals, then the proof is complete.
The assumption Method

Given a subgoal of the form:

\[ [A; B] \rightarrow A \]

This subgoal is solvable because we want to prove \( A \) under the assumption that \( A \) is true.

We can solve this subgoal using the assumption method:

\texttt{apply} assumption
The rule Method

To apply an inference rule backward, we use rule.

Consider the theorem disjI1

\[ ?P \implies ?P \lor ?Q \]

Using the command

apply (rule disjI1)

on the goal

\[ [A; B; C] \implies (A \land B) \lor D \]

yields the subgoal

\[ [A; B; C] \implies A \land B \]

Using rule can be viewed as a way of breaking down the problem into subproblems.
Matching and Unification

In applying rule (with the ? in front of variables omitted)

\[ P \Rightarrow P \lor Q \]

to goal

\[ [A; B; C] \Rightarrow (A \land B) \lor D \]

The pattern \( P \lor Q \) is matched with the target \((A \land B) \lor D\) to yield the instantiations \( P \mapsto A \land B, \ Q \mapsto D\) which make the pattern and target the same. The following goal results

\[ [A; B; C] \Rightarrow A \land B \]

In general, if the goal conclusion contains schematic variables, the rule and goal conclusions are unified i.e. both are instantiated so as to make them the same.

More on unification later!
More natural deduction (H&R 1.2, 1.4)
- The rules for $\rightarrow$, $\leftrightarrow$ and $\neg$
- Rules for classical reasoning
- Soundness and completeness properties
- Sequent-style presentation

Starting with proofs in Isabelle

Next time:
- More on using Isabelle to do proofs
- N-style vs. L-style proof systems