Recap

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

\[
\begin{align*}
\frac{P Q}{P \land Q} \quad \text{(conjI)} & \quad \frac{P}{P \lor Q} \quad \text{(disjI1)} & \quad \frac{Q}{P \lor Q} \quad \text{(disjI2)} \\
\end{align*}
\]

\[
\begin{align*}
\frac{P \land Q}{P} \quad \text{(conjunct1)} & \quad \frac{P \land Q}{Q} \quad \text{(conjunct2)} \\
\end{align*}
\]

\[
\begin{align*}
\frac{P \lor Q \quad [P] \quad [Q] \quad \vdots \quad \vdots \quad \vdots}{R \quad R} \quad \text{R (disjE)}
\end{align*}
\]

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

\[
\begin{array}{c}
\frac{[P]}{\vdots}
\end{array}
\]

**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.

\[
\frac{P \rightarrow Q}{P} \quad (\text{impI})
\]

\[
\frac{P \rightarrow Q \quad P}{\vdots} \quad (\text{mp})
\]

The “modus ponens” rule.

\[
\begin{array}{c}
\frac{[Q]}{\vdots}
\end{array}
\]

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

\[
\frac{P \rightarrow Q \quad P \quad R}{R} \quad (\text{impE})
\]

In general, derivation assumptions may occur multiple times, and only a subset of the occurrences need be discharged.
Rules for $\leftrightarrow$

$$
\begin{array}{c}
\begin{array}{c}
[Q] \\
\vdots \\
\vdots \\
P
\end{array} \\
\begin{array}{c}
\vdots \\
\vdots \\
Q
\end{array}
\end{array}
\Rightarrow
P \leftrightarrow Q \quad \text{(iffI)}
$$

$$
\begin{array}{c}
\begin{array}{c}
P \leftrightarrow Q \\
\vdots
\end{array} \\
Q
\end{array}
\Rightarrow
P \quad \text{(iffE1)}
$$

$$
\begin{array}{c}
\begin{array}{c}
P \leftrightarrow Q \\
\vdots
\end{array} \\
Q
\end{array}
\Rightarrow
P \quad \text{(iffE2)}
$$

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

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

N.B. \( \bot \) is written \text{False} in Isabelle.

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

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

\[((Sunny \lor Rainy) \land \neg Sunny) \rightarrow Rainy\]

which we previously knew only by semantic means.

\[
\frac{
\begin{align*}
\frac{
\frac{[S \lor R] \land \neg S}{[S \lor R]}_1
\end{align*}
\end{align*}
\begin{align*}
\frac{[S \lor R]_2
\end{align*}
\begin{align*}
\frac{\neg S}{R}
\end{align*}
\begin{align*}
\frac{\neg S}{[R]_2}
\end{align*}
\begin{align*}
\frac{R}{[S \lor R]_2}
\end{align*}
\begin{align*}
\frac{R}{R}
\end{align*}
\begin{align*}
\frac{((S \lor R) \land \neg S) \rightarrow R}{(S \lor R) \land \neg S \rightarrow R}
\end{align*}
\]

(1)

(2)

The subscripts \([\cdot]_1\) and \([\cdot]_2\) on the discharged assumptions refer to the rule instances where they are discharged.
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

\[ \neg P \]
\[ \vdots \]
\[ \vdash \]
\[ \neg P \lor P \] (excluded_middle)
\[ \therefore P \] (ccontr)

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:

\[ P_2 \]
\[ P_1 \quad : \quad : \quad \ldots \quad : \quad P_n \]
\[ \vdash \]
\[ Q \]

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 much more fiddly on paper, but easier to prove meta-theoretic properties for, and easier to represent on a computer.
Natural Deduction Sequents

\[
\begin{align*}
\frac{P \in \Gamma}{\Gamma \vdash P} \quad &\text{(assumption)} \\
\end{align*}
\]

New rule:

\[
\begin{align*}
\frac{\Gamma \vdash P \quad \Gamma \vdash Q}{\Gamma \vdash P \land Q} \quad &\text{(conjI)} \\
\frac{\Gamma \vdash P \land Q}{\Gamma \vdash P} \quad &\text{(conjunct1)} \\
\frac{\Gamma \vdash P \land Q}{\Gamma \vdash Q} \quad &\text{(conjunct2)} \\
\frac{\Gamma \vdash P}{\Gamma \vdash P \lor Q} \quad &\text{(disjI1)} \\
\frac{\Gamma \vdash Q}{\Gamma \vdash P \lor Q} \quad &\text{(disjI2)} \\
\end{align*}
\]

\[
\begin{align*}
\frac{\Gamma \vdash P \land Q}{\Gamma \vdash P} \quad &\text{(conjunct1)} \\
\frac{\Gamma \vdash P \land Q}{\Gamma \vdash Q} \quad &\text{(conjunct2)} \\
\frac{\Gamma \vdash P \lor Q}{\Gamma \vdash P} \quad &\text{(disjI1)} \\
\frac{\Gamma \vdash P \lor Q}{\Gamma \vdash Q} \quad &\text{(disjI2)} \\
\frac{\Gamma \vdash P \lor Q}{\Gamma \vdash P} \quad &\text{(disjI1)} \\
\frac{\Gamma \vdash P \lor Q}{\Gamma \vdash Q} \quad &\text{(disjI2)} \\
\frac{\Gamma \vdash A \rightarrow B}{\Gamma \vdash A} \quad &\text{(implI)} \\
\frac{\Gamma \vdash A \rightarrow B}{\Gamma \vdash B} \quad &\text{(mp)} \\
\frac{\Gamma \vdash P \land Q}{\Gamma \vdash P} \quad &\text{(conjunct1)} \\
\frac{\Gamma \vdash P \land Q}{\Gamma \vdash Q} \quad &\text{(conjunct2)} \\
\frac{\Gamma \vdash P \lor Q}{\Gamma \vdash P} \quad &\text{(disjI1)} \\
\frac{\Gamma \vdash P \lor Q}{\Gamma \vdash Q} \quad &\text{(disjI2)} \\
\frac{\Gamma \vdash A \rightarrow B}{\Gamma \vdash A} \quad &\text{(implI)} \\
\frac{\Gamma \vdash A \rightarrow B}{\Gamma \vdash B} \quad &\text{(mp)} \\
\frac{\Gamma \vdash P \land Q}{\Gamma \vdash P} \quad &\text{(conjunct1)} \\
\frac{\Gamma \vdash P \land Q}{\Gamma \vdash Q} \quad &\text{(conjunct2)} \\
\frac{\Gamma \vdash P \lor Q}{\Gamma \vdash P} \quad &\text{(disjI1)} \\
\frac{\Gamma \vdash P \lor Q}{\Gamma \vdash Q} \quad &\text{(disjI2)} \\
\frac{\Gamma \vdash A \rightarrow B}{\Gamma \vdash A} \quad &\text{(implI)} \\
\frac{\Gamma \vdash A \rightarrow B}{\Gamma \vdash B} \quad &\text{(mp)} \\
\end{align*}
\]

No introduction rule for \( \bot \)

\[
\begin{align*}
\frac{\Gamma, P \vdash \bot}{\Gamma \vdash \neg P} \quad &\text{(notI)} \\
\frac{\Gamma \vdash P \quad \Gamma \vdash \neg P}{\Gamma \vdash \bot} \quad &\text{(notE)} \\
\frac{\Gamma \vdash \bot}{\Gamma \vdash P} \quad &\text{(FalseE)} \\
\frac{\Gamma \vdash P}{\Gamma \vdash P \lor \neg P} \quad &\text{(excluded_middle)} \\
\end{align*}
\]
Natural Deduction in Isabelle/HOL

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

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

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

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

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

\[
\begin{array}{c}
\vdash \left( \begin{array}{c} [P] \\
\vdots \\
Q \\
\end{array} \right) \\
\hline
P \rightarrow Q \\
\end{array}
\]

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

A selection of natural deduction rules in Isabelle notation:

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

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

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

\[
\frac{P \lor Q \quad R \quad R}{R} \quad \quad (\text{disjE}) \quad \quad \left[ ?P \lor ?Q ; ?P \Rightarrow ?R ; ?Q \Rightarrow ?R \right] \Rightarrow ?R
\]
Doing proofs in Isabelle

A declaration like so enters proof mode:

```isabelle
theorem K: "A \rightarrow B \rightarrow A"
```

Isabelle responds:

```isabelle
proof (prove): step 0
```

1 subgoal:

1. \( A \rightarrow B \rightarrow A \)

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:

\[ [A; B] \implies A \]

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:

`apply assumption`
The rule Method

To apply an inference rule, we use rule.

Consider the theorem disjI1

\[ \neg P \implies \neg P \lor \neg Q \]

Using the command

apply (rule disjI1)

on the goal

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

yields the subgoal

\[ [A; B; C] \implies A \land B \]
Matching and Unification

In applying rule

\[ P \rightarrow P \lor Q \]

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 instantiation \( P \leftrightarrow A \land B\), \( Q \leftrightarrow D\) 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!
Getting Started with Isabelle

This document on the AR slides webpage explains

- How Isabelle interactive theorem prover is started up
- Basics of *Proof General* user interface for Isabelle
- Examples of propositional logic proofs in Isabelle ("Prop.thy")
Summary

- More natural deduction (H&R 1.2, 1.4)
  - The rules for →, ↔ and ¬
  - Rules for classical reasoning
  - Soundness and completeness properties
  - Sequent-style presentation
- Starting proving in Isabelle
- Next time:
  - More on using Isabelle to do proofs
  - N-style vs. L-style proof systems