CS477 Formal Software Development Methods

Elsa L Gunter
2112 SC, UIUC
egunter@illinois.edu
http://courses.engr.illinois.edu/cs477

Slides based in part on previous lectures by Mahesh Vishwanathan, and by Gul Agha

February 1, 2013

Assumptions in Natural Deduction

- Problem: Keeping track of hypotheses and their discharge in Natural Deduction is *HARD!*
- Solution: Use *sequents* to track hypotheses

- A sequent is a pair of
  - A set of propositions (called assumptions, or hypotheses of sequent) and
  - A proposition (called conclusion of sequent)
- More generally (not here), allow set of hypotheses and set of conclusions

Nat. Ded. Introduction Sequent Rules

Γ is set of propositions (assumptions/hypotheses)

Hypothesis Introduction:

$$\frac{}{\Gamma \cup \{A\} \vdash A}\ \text{Hyp}$$

Truth Introduction:

$$\frac{}{\Gamma \vdash \mathbf{T}}\ \mathbf{T}\ \text{I}$$

And Introduction:

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \land B}\ \text{And I}$$

Or Introduction:

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \lor B}\ \text{Or}_L\ \text{I} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \lor B}\ \text{Or}_R\ \text{I}$$

Not Introduction:

$$\frac{\Gamma \cup \{A\} \vdash \mathbf{F}}{\Gamma \vdash \neg A}\ \text{Not I}$$

Implication Introduction:

$$\frac{\Gamma \cup \{A\} \vdash B}{\Gamma \vdash A \Rightarrow B}\ \text{Imp I}$$

Nat. Ded. Elimination Sequent Rules

Γ is set of propositions (assumptions/hypotheses)

Not Elimination:

$$\frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash C}\ \text{Not E}$$

Implication Elimination:

$$\frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A \quad \Gamma \cup \{B\} \vdash C}{\Gamma \vdash C}\ \text{Imp E}$$

And Elimination:

$$\frac{\Gamma \vdash A \wedge B \quad \Gamma \cup \{A\} \vdash C}{\Gamma \vdash C}\ \text{And}_L\ \text{E} \qquad \frac{\Gamma \vdash A \wedge B \quad \Gamma \cup \{B\} \vdash C}{\Gamma \vdash C}\ \text{And}_R\ \text{E}$$

False Elimination:

$$\frac{\Gamma \vdash \mathbf{F}}{\Gamma \vdash C}\ \mathbf{F}\ \text{E}$$

Or Elimination:

$$\frac{\Gamma \vdash A \vee B \quad \Gamma \cup \{A\} \vdash C \quad \Gamma \cup \{B\} \vdash C}{\Gamma \vdash C}\ \text{Or E}$$

Example Proof 4, Revisited

$$\overline{\{\ \} \vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}$$

Example Proof 4, Revisited

$\Gamma_1 = \{A \Rightarrow B\}$

$$\dfrac{\dfrac{}{\Gamma_1 \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}}{\{\ \} \vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}\ \text{Imp I}$$

Example Proof 4, Revisited

$\Gamma_1 = \{A \Rightarrow B\}$
$\Gamma_2 = \{A \Rightarrow B,\ B \Rightarrow C\}$

$$\dfrac{\dfrac{\dfrac{}{\Gamma_2 \vdash A \Rightarrow C}}{\Gamma_1 \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}\ \text{Imp I}}{\{\ \} \vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}\ \text{Imp I}$$

Example Proof 4, Revisited

$\Gamma_1 = \{A \Rightarrow B\}$
$\Gamma_2 = \{A \Rightarrow B,\ B \Rightarrow C\}$
$\Gamma_3 = \{A \Rightarrow B,\ B \Rightarrow C,\ A\}$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma_3 \vdash C}}{\Gamma_2 \vdash A \Rightarrow C}\text{Imp I}}{\Gamma_1 \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}\text{Imp I}}{\{\ \} \vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}\text{Imp I}$$

Example Proof 4, Revisited

$\Gamma_1 = \{A \Rightarrow B\}$
$\Gamma_2 = \{A \Rightarrow B,\ B \Rightarrow C\}$
$\Gamma_3 = \{A \Rightarrow B,\ B \Rightarrow C,\ A\}$
$\Gamma_4 = \{A \Rightarrow B,\ B \Rightarrow C,\ A,\ B\}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma_3 \vdash A \Rightarrow B} \quad \dfrac{}{\Gamma_3 \vdash A} \quad \dfrac{}{\Gamma_4 \vdash C}}{\Gamma_3 \vdash C}\ \text{Imp E}}{\Gamma_2 \vdash A \Rightarrow C}\ \text{Imp I}}{\Gamma_1 \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}\ \text{Imp I}}{\{\ \} \vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}\ \text{Imp I}$$

Example Proof 4, Revisited

$\Gamma_1 = \{A \Rightarrow B\}$
$\Gamma_2 = \{A \Rightarrow B,\ B \Rightarrow C\}$
$\Gamma_3 = \{A \Rightarrow B,\ B \Rightarrow C,\ A\}$
$\Gamma_4 = \{A \Rightarrow B,\ B \Rightarrow C,\ A,\ B\}$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma_3 \vdash A \Rightarrow B}\text{Hyp} \quad \dfrac{}{\Gamma_3 \vdash A} \quad \dfrac{}{\Gamma_4 \vdash C}}{\Gamma_3 \vdash C}\text{Imp E}}{\Gamma_2 \vdash A \Rightarrow C}\text{Imp I}}{\Gamma_1 \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}\text{Imp I}}{\{\ \} \vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}\text{Imp I}
$$

Example Proof 4, Revisited

$\Gamma_1 = \{A \Rightarrow B\}$
$\Gamma_2 = \{A \Rightarrow B,\ B \Rightarrow C\}$
$\Gamma_3 = \{A \Rightarrow B,\ B \Rightarrow C,\ A\}$
$\Gamma_4 = \{A \Rightarrow B,\ B \Rightarrow C,\ A,\ B\}$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\text{Hyp}}{\Gamma_3 \vdash A \Rightarrow B} \quad \dfrac{\text{Hyp}}{\Gamma_3 \vdash A} \quad \dfrac{}{\Gamma_4 \vdash C}}{\Gamma_3 \vdash C}\text{Imp E}}{\Gamma_2 \vdash A \Rightarrow C}\text{Imp I}}{\Gamma_1 \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}\text{Imp I}}{\{\ \} \vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}\text{Imp I}
$$

Example Proof 4, Revisited

$\Gamma_1 = \{A \Rightarrow B\}$
$\Gamma_2 = \{A \Rightarrow B,\ B \Rightarrow C\}$
$\Gamma_3 = \{A \Rightarrow B,\ B \Rightarrow C,\ A\}$
$\Gamma_4 = \{A \Rightarrow B,\ B \Rightarrow C,\ A,\ B\}$
$\Gamma_5 = \{A \Rightarrow B,\ B \Rightarrow C,\ A,\ B,\ \color{red}{C}\}$

$$
\cfrac{
  \cfrac{
    \cfrac{
      \cfrac{\text{Hyp}}{\Gamma_3 \vdash A \Rightarrow B}
      \quad
      \cfrac{\text{Hyp}}{\Gamma_3 \vdash A}
      \quad
      \cfrac{
        \cfrac{}{\Gamma_4 \vdash B \Rightarrow \color{red}{C}}
        \quad
        \cfrac{}{\Gamma_4 \vdash B}
        \quad
        \cfrac{}{\color{red}{\Gamma_5} \vdash C}
      }{\Gamma_4 \vdash C}\ \color{red}{\text{Imp E}}
    }{\Gamma_3 \vdash C}\ \text{Imp E}
  }{\Gamma_2 \vdash A \Rightarrow C}\ \text{Imp I}
}{
  \cfrac{\Gamma_1 \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}{\{\ \} \vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}\ \text{Imp I}
}\ \text{Imp I}
$$

Example Proof 4, Revisited

$\Gamma_1 = \{A \Rightarrow B\}$
$\Gamma_2 = \{A \Rightarrow B,\ B \Rightarrow C\}$
$\Gamma_3 = \{A \Rightarrow B,\ B \Rightarrow C,\ A\}$
$\Gamma_4 = \{A \Rightarrow B,\ B \Rightarrow C,\ A,\ B\}$
$\Gamma_5 = \{A \Rightarrow B,\ B \Rightarrow C,\ A,\ B,\ C\}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\text{Hyp}}{\Gamma_3 \vdash A \Rightarrow B} \quad \dfrac{\text{Hyp}}{\Gamma_3 \vdash A} \quad \dfrac{\dfrac{\text{Hyp}}{\Gamma_4 \vdash B \Rightarrow C} \quad \dfrac{}{\Gamma_4 \vdash B} \quad \dfrac{}{\Gamma_5 \vdash C}}{\Gamma_4 \vdash C}\,\text{Imp E}}{\Gamma_3 \vdash C}\,\text{Imp E}}{\Gamma_2 \vdash A \Rightarrow C}\,\text{Imp I}}{\Gamma_1 \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}\,\text{Imp I}}{\{\ \} \vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}\,\text{Imp I}$$

$\Gamma_1 = \{A \Rightarrow B\}$
$\Gamma_2 = \{A \Rightarrow B,\ B \Rightarrow C\}$
$\Gamma_3 = \{A \Rightarrow B,\ B \Rightarrow C,\ A\}$
$\Gamma_4 = \{A \Rightarrow B,\ B \Rightarrow C,\ A,\ B\}$
$\Gamma_5 = \{A \Rightarrow B,\ B \Rightarrow C,\ A,\ B,\ C\}$

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\text{Hyp}}{\Gamma_3 \vdash A \Rightarrow B} \quad \cfrac{\text{Hyp}}{\Gamma_3 \vdash A} \quad \cfrac{\cfrac{\text{Hyp}}{\Gamma_4 \vdash B \Rightarrow C} \quad \cfrac{\text{Hyp}}{\Gamma_4 \vdash B} \quad \cfrac{}{\Gamma_5 \vdash C}}{\Gamma_4 \vdash C}\,\text{Imp E}}{\Gamma_3 \vdash C}\,\text{Imp E}}{\Gamma_2 \vdash A \Rightarrow C}\,\text{Imp I}}{\Gamma_1 \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}\,\text{Imp I}}{\{\ \} \vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}\,\text{Imp I}$$

Example Proof 4, Revisited

$\Gamma_1 = \{A \Rightarrow B\}$
$\Gamma_2 = \{A \Rightarrow B,\ B \Rightarrow C\}$
$\Gamma_3 = \{A \Rightarrow B,\ B \Rightarrow C,\ A\}$
$\Gamma_4 = \{A \Rightarrow B,\ B \Rightarrow C,\ A,\ B\}$
$\Gamma_5 = \{A \Rightarrow B,\ B \Rightarrow C,\ A,\ B,\ C\}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\text{Hyp}}{\Gamma_3 \vdash A \Rightarrow B} \quad \dfrac{\text{Hyp}}{\Gamma_3 \vdash A} \quad \dfrac{\dfrac{\text{Hyp}}{\Gamma_4 \vdash B \Rightarrow C} \quad \dfrac{\text{Hyp}}{\Gamma_4 \vdash B} \quad \dfrac{\text{Hyp}}{\Gamma_5 \vdash C}}{\Gamma_4 \vdash C}\,\text{Imp E}}{\Gamma_3 \vdash C}\,\text{Imp E}}{\Gamma_2 \vdash A \Rightarrow C}\,\text{Imp I}}{\Gamma_1 \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}\,\text{Imp I}}{\{\ \} \vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}\,\text{Imp I}$$

Introduction to Isabelle/HOL

- Isabelle/HOL is an *interactive* theorem prover
- Proof guided by human
- Goal-directed reduction (LCF style)
- Core: type of type, term, theorem/inference rule as abstract types in SML
- Secure: every proof built from axioms, defintions, primitive rules of inference
- Programmable: derived rules and proof methods use secure core
- Layered interface (mostly don't need to see SML)

Some Useful Links

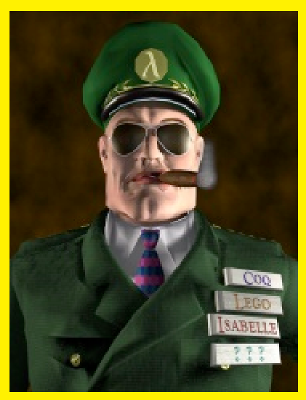
- Website for Isabelle:
  http://www.cl.cam.ac.uk/Research/HVG/Isabelle/
- Isabelle mailing list – to join, send mail to:
  isabelle-users@cl.cam.ac.uk
- Reference:
  http://www.cl.cam.ac.uk/Research/HVG/Isabelle/dist/Isabelle/doc/tutorial.pdf

System Architecture

*ProofGeneral**	(X)Emacs based interface
Isar	Isabelle proof scripting language
Isabelle/HOL	Isabelle instance for HOL
Isabelle	generic theorem prover
Standard ML	implementation language

* Also exists *jedit* interface

Proof General



An Isabelle Interface
by David Aspinall

Proof General

Customized version of (x)emacs:

- All of emacs (info: `Ctrl-h i`)
- Isabelle aware when editing `.thy` files
- (Optional) Can use mathematical symbols ("x-symbols")

Interaction:

- via mouse / buttons / pull-down menus
- or keyboard (for key bindings, see `Ctrl-h m`)

Proof General Input

Input of math symbols in ProofGeneral

- via "standard" ascii name: `&`, `|`, `-->`, ...
- via ascii encoding (similar to LaTeX):
  `\<and>`, `\<or>`, ...
- via menu ("X-Symbol")

Symbol Translations

x-symbol	$\forall$	$\exists$	λ	$\neg$	$\wedge$
ascii (1)	\<forall>	\<exists>	\<lambda>	\<not>	\<and>
ascii (2)	ALL	EX	%	~	&

x-symbol	$\vee$	$\longrightarrow$	$\Rightarrow$
ascii (1)	\<or>	\<longrightarrow>	\<Rightarrow>
ascii (2)	|	-->	=>

(1) is converted to x-symbol, (2) remains as ascii
See Appendix A of reference for more complete list

Demo 1

Time for a demo of types and terms
(and a simple lemma)

Overview of Isabelle/HOL

HOL

- HOL = Higher-Order Logic
- HOL = Types + Lambda Calculus + Logic
- HOL has
  - datatypes
  - recursive functions
  - logical operators ($\wedge$, $\vee$, $\longrightarrow$, $\forall$, $\exists$, $\ldots$)
- Contains propositional logic, first-order logic
- HOL is very similar to a functional programming language
- Higher-order = functions are values, too!

Formulae (Approximation)

- Syntax (in decreasing priority):

$$
\begin{array}{lclcl}
\mathit{form} & ::= & (\mathit{form}) & | & \mathit{term} = \mathit{term} \\
& | & \neg \mathit{form} & | & \mathit{form} \wedge \mathit{form} \\
& | & \mathit{form} \vee \mathit{form} & | & \mathit{form} \longrightarrow \mathit{form} \\
& | & \forall x.\ \mathit{form} & | & \exists x.\ \mathit{form} \\
& & \text{and some others} & &
\end{array}
$$

- Scope of quantifiers: as for to right as possible

Examples

- $\neg A \wedge B \vee C \equiv ((\neg A) \wedge B) \vee C$
- $A \wedge B = C \equiv A \wedge (B = C)$
- $\forall x.\ P\ x \wedge Q\ x \equiv \forall x.\ (P\ x \wedge Q\ x)$
- $\forall x. \exists y.\ P\ x\ y \wedge Q\ x \equiv \forall x. (\exists y.\ (P\ x\ y \wedge Q\ x))$

Proofs

General schema:

```
lemma name: " ..."
apply ( ...)
⋮
done
```

If the lemma is suitable as a simplification rule:

```
lemma name[simp]: " ..."
```

Adds lemma *name* to future simplifications

Top-down Proofs

`sorry`

"completes" any proof (by giving up, and accepting it)
Suitable for top-down development of theories:
Assume lemmas first, prove them later.

Only allowed for interactive proof!