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 3, 2013

Getting Started with Isabelle

- Choice
  - Use Isabelle on EWS
  - Install on your machine
  - Both
- On EWS
  - Assuming you are running an X client, log in to EWS:
    `ssh -Y <netid>@remlnx.ews.illinois.edu`
    - `-Y` used to forward X packets securely
  - To start Isabelle with `emacs` and ProofGeneral
    `/class/cs477/bin/isabelle emacs`
  - To start Isabelle with jedit
    `/class/cs477/bin/isabelle jedit`
  - Will assume `emacs` and ProofGeneral here

My First Theory File

File name: `my_theory.thy`
Contents:

```
theory My_theory
imports Main
begin

thm impI

lemma trivial: "A  A"
apply (rule impI)
apply assumption
done (* of lemma *)

thm trivial

end (* of theory file *)
```


Overview of Isabelle/HOL

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

Formulae (first Approximation)

- Syntax (in decreasing priority):

$$\begin{array}{rcl|l} \mathit{form} & ::= & (\mathit{form}) & \mathit{term} = \mathit{term} \\ & \mid & \neg\mathit{form} & \mathit{form} \wedge \mathit{form} \\ & \mid & \mathit{form} \vee \mathit{form} & \mathit{form} \longrightarrow \mathit{form} \\ & \mid & \forall x.\ \mathit{form} & \exists x.\ \mathit{form} \end{array}$$

and some others

- Scope of quantifiers: as far tot he 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
```

First ... theorem statement
(...) are *proof methods*

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!

Isabelle Syntax

- Distinct from HOL syntax
- Contains HOL syntax within it
- Also the same as HOL - need to not confuse them

Theory = Module

Syntax:

theory *MyTh*
imports $ImpTh_1$ ... $ImpTh_n$
begin
declarations, definitions, theorems, proofs, ...
end

- *MyTh*: name of theory being built. Must live in file *MyTh*.thy.
- $ImpTh_i$: name of *imported* theories. Importing is transitive.

Meta-logic: Basic Constructs

Implication: $\Longrightarrow$ (==>)
For separating premises and conclusion of theorems / rules

Equality: $\equiv$ (==)
For definitions

Universal Quantifier: $\bigwedge$ (!!)
Usually inserted and removed by Isabelle automatically

Do not use *inside* HOL formulae

Rule/Goal Notation

$$[| A_1; \ldots ; A_n |] \Longrightarrow B$$

abbreviates

$$A_1 \Longrightarrow \ldots \Longrightarrow A_n \Longrightarrow B$$

and means the rule (or potential rule):

$$\frac{A_1; \ldots ; A_n}{B}$$

; $\approx$ "and"

Note: A theorem is a rule; a rule is a theorem.

The Proof/Goal State

1. $\bigwedge x_1 \ldots x_m.\ [|\, A_1 ; \ldots ; A_n \,|] \Longrightarrow B$

$x_1 \ldots x_m$	Local constants (fixed variables)
$A_1 \ldots A_n$	Local assumptions
B	Actual (sub)goal

Proof Basics

- Isabelle uses *Natural Deduction* proofs
  - Uses (modified) *sequent* encoding
- Rule notation:

Rule	Sequent Encoding
$\dfrac{A_1 \ldots A_n}{A}$	$[\![A_1, \ldots, A_n]\!] \Longrightarrow A$
$\dfrac{A_1 \ldots \ \begin{array}{c} B \\ \vdots \\ A_i \end{array} \ \ldots A_n}{A}$	$[\![A_1, \ldots, B \Longrightarrow A_i, \ldots, A_n]\!] \Longrightarrow A$

Natural Deduction

For each logical operator $\oplus$, have two kinds of rules:

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

$$\frac{?}{A \oplus B}$$

Elimination: What can I prove using $A \oplus B$?

$$\frac{\ldots A \oplus B \ldots}{?}$$

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 we know A_1 and we want to prove A
it suffices to prove $A_2 \ldots A_n$

Natural Deduction for Propositional Logic

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

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

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

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

Natural Deduction for Propositional Logic

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

$$\frac{A = B \quad B}{A}\,\texttt{iffD2}$$

More Rules

$$\frac{\mathtt{A} \wedge \mathtt{B}}{\mathtt{A}}\ \text{conjunct1} \qquad \frac{\mathtt{A} \wedge \mathtt{B}}{\mathtt{B}}\ \text{conjunct2}$$

$$\frac{\mathtt{A} \longrightarrow \mathtt{B} \quad \mathtt{A}}{\mathtt{B}}\ \text{mp}$$

Compare to elimination rules:

$$\frac{\mathtt{A} \wedge \mathtt{B} \quad [\![\mathtt{A}; \mathtt{B}]\!] \Longrightarrow \mathtt{C}}{\mathtt{C}}\ \text{conjE} \qquad \frac{\mathtt{A} \longrightarrow \mathtt{B} \quad \mathtt{A} \quad \mathtt{B} \Longrightarrow \mathtt{C}}{\mathtt{C}}\ \text{impE}$$

"Classical" Rules

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

- `ccontr` and `classical` are not derivable from the Natural Deduction rules.
- They make the logic *"classical"*, i.e. *"non-constructive* or *"non-intuitionistic"*.

Proof by Assumption

$$\frac{\mathtt{A}_1 \ldots \mathtt{A}_i \ldots \mathtt{A}_n}{\mathtt{A}_i}$$

- Proof method: `assumption`
- Use:

  `apply assumption`
- Proves:

  $[\![\mathtt{A}_1; \ldots; \mathtt{A}_n]\!] \Longrightarrow \mathtt{A}$

  by unifying A with one of the A_i

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: $A_1' \ \ldots \ A_n'$

Backwards reduction, like in Prolog

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

subgoal: `1.` $\mathtt{A} \wedge \mathtt{B}$

Result: `1. A2. B`

Rule Application: More Complete Idea

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

- Unify A and C with (meta)-substitution σ
- Specialize goal to $\sigma(C)$
- Replace C with n new subgoals: $\sigma(A_1) \ \ldots \ \sigma(A_n)$

Note: schematic variables in C treated as existential variables

Does there exist value for $?X$ in C that makes C true?

(Still not the whole story)

`rule` Application

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. $[\![\sigma(B_1); \ldots; \sigma(B_m)]\!] \Longrightarrow \sigma(A_1)$

$\vdots$

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

Proves: $[\![\sigma(B_1); \ldots; \sigma(B_m)]\!] \Longrightarrow \sigma(C)$

Command: `apply (rule` <*rulename*>`)`

Applying Elimination Rules

`apply (erule <elim-rule>)`

Like `rule` but also

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

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. $[\![X; Y]\!] \Longrightarrow [\![A; B]\!] \Longrightarrow Z$

Same as: 1.$[\![X; Y; A; B]\!] \Longrightarrow Z$