



COMP 4161
NICTA Advanced Course

Advanced Topics in Software Verification

Gerwin Klein, June Andronick, Toby Murray, Rafal Kolanski

$\lambda \rightarrow$ and HOL

Slide 1



Last time...

- Simply typed lambda calculus: λ^{\rightarrow}
- Typing rules for λ^{\rightarrow} , type variables, type contexts
- β -reduction in λ^{\rightarrow} satisfies subject reduction
- β -reduction in λ^{\rightarrow} always terminates
- Types and terms in Isabelle

Slide 2



Content

- Intro & motivation, getting started [1]
- Foundations & Principles
 - Lambda Calculus, natural deduction [1,2]
 - Higher Order Logic [3^a]
 - Term rewriting [4]
- Proof & Specification Techniques
 - Isar [5]
 - Inductively defined sets, rule induction [6^b]
 - Datatypes, recursion, induction [7^c, 8]
 - Calculational reasoning, code generation [9]
 - Hoare logic, proofs about programs [10^d,11,12]

^aa1 due; ^ba2 due; ^csession break; ^da3 due

Slide 3



PREVIEW: PROOFS IN ISABELLE

Slide 4

Proofs in Isabelle



General schema:

```
lemma name: "<goal>"  
apply <method>  
apply <method>  
...  
done
```

→ Sequential application of methods until all **subgoals** are solved.

Slide 5

The Proof State



- $\bigwedge x_1 \dots x_p. [A_1; \dots; A_n] \Rightarrow B$
- $\bigwedge y_1 \dots y_q. [C_1; \dots; C_m] \Rightarrow D$

$x_1 \dots x_p$ Parameters
 $A_1 \dots A_n$ Local assumptions
 B Actual (sub)goal

Slide 6

Isabelle Theories



Syntax:

```
theory MyTh  
imports ImpTh1 ... ImpThn  
begin  
(declarations, definitions, theorems, proofs, ...)*  
end
```

- *MyTh*: name of theory. Must live in file *MyTh.thy*
- *ImpTh_i*: name of *imported* theories. Import transitive.

Unless you need something special:

```
theory MyTh imports Main begin ... end
```

Slide 7

Natural Deduction Rules



$$\frac{A \quad B}{A \wedge B} \text{ conjI} \qquad \frac{A \wedge B \quad [A; B] \Rightarrow C}{C} \text{ conjE}$$
$$\frac{A}{A \vee B} \quad \frac{B}{A \vee B} \text{ disjI1/2} \qquad \frac{A \vee B \quad A \Rightarrow C \quad B \Rightarrow C}{C} \text{ disjE}$$
$$\frac{A \Rightarrow B}{A \longrightarrow B} \text{ impl} \qquad \frac{A \longrightarrow B \quad A \quad B \Rightarrow C}{C} \text{ impE}$$

For each connective (\wedge, \vee , etc):
introduction and elimination rules

Slide 8

Proof by assumption



apply assumption

proves

1. $\llbracket B_1; \dots; B_m \rrbracket \implies C$

by unifying C with one of the B_i

There may be more than one matching B_i and multiple unifiers.

Backtracking!

Explicit backtracking command: **back**

Slide 9

Intro rules



Intro rules decompose formulae to the right of \implies .

apply (rule <intro-rule>)

Intro rule $\llbracket A_1; \dots; A_n \rrbracket \implies A$ means

→ To prove A it suffices to show $A_1 \dots A_n$

Applying rule $\llbracket A_1; \dots; A_n \rrbracket \implies A$ to subgoal C :

→ unify A and C

→ replace C with n new subgoals $A_1 \dots A_n$

Slide 10

Elim rules



Elim rules decompose formulae on the left of \implies .

apply (erule <elim-rule>)

Elim rule $\llbracket A_1; \dots; A_n \rrbracket \implies A$ means

→ If I know A_1 and want to prove A it suffices to show $A_2 \dots A_n$

Applying rule $\llbracket A_1; \dots; A_n \rrbracket \implies A$ to subgoal C :

Like **rule** but also

→ unifies first premise of rule with an assumption

→ eliminates that assumption

Slide 11

DEMO

Slide 12



MORE PROOF RULES

Slide 13

Iff, Negation, True and False



$$\frac{A \implies B \quad B \implies A}{A = B} \text{ iffI} \quad \frac{A = B \quad [A \longrightarrow B; B \longrightarrow A] \implies C}{C} \text{ iffE}$$

$$\frac{A = B}{A \implies B} \text{ iffD1}$$

$$\frac{A = B}{B \implies A} \text{ iffD2}$$

$$\frac{A \implies \text{False}}{\neg A} \text{ notI}$$

$$\frac{\neg A \quad A}{P} \text{ notE}$$

$$\frac{}{\text{True}} \text{ TrueI}$$

$$\frac{\text{False}}{P} \text{ FalseE}$$

Slide 14

Equality



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

$$\frac{s = t \quad P s}{P t} \text{ subst}$$

Rarely needed explicitly — used implicitly by term rewriting

Slide 15

Classical



$$\frac{}{P = \text{True} \vee P = \text{False}} \text{ True-False}$$

$$\frac{}{P \vee \neg P} \text{ excluded-middle}$$

$$\frac{\neg A \implies \text{False}}{A} \text{ ccontr} \quad \frac{\neg A \implies A}{A} \text{ classical}$$

- **excluded-middle**, **ccontr** and **classical** not derivable from the other rules.
- if we include True-False, they are derivable

They make the logic “classical”, “non-constructive”

Slide 16

Cases

$\overline{P \vee \neg P}$ excluded-middle

is a case distinction on type *bool*

Isabelle can do case distinctions on arbitrary terms:

`apply (case_tac term)`

Slide 17



Safe and not so safe

Safe rules preserve provability

conjI, impl, notI, iffI, refl, ccontr, classical, conjE, disjE

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

Unsafe rules can turn a provable goal into an unprovable one

disjI1, disjI2, impE, iffD1, iffD2, notE

$$\frac{A}{A \vee B} \text{ disjI1}$$

Apply safe rules before unsafe ones

Slide 18



What we have learned so far...

- natural deduction rules for $\wedge, \vee, \longrightarrow, \neg$, iff...
- proof by assumption, by intro rule, elim rule
- safe and unsafe rules

Slide 20



DEMO

Slide 19

