Interactive Formal Verification
5: Logic in Isabelle

Tjark Weber
(Slides: Lawrence C Paulson)
Computer Laboratory
University of Cambridge
Logical Frameworks
Logical Frameworks

• A formalism to represent other formalisms
Logical Frameworks

- A formalism to represent other formalisms
- Support for *natural deduction*
Logical Frameworks

- A formalism to represent other formalisms
- Support for *natural deduction*
- A common basis for implementations
Logical Frameworks

- A formalism to represent other formalisms
- Support for *natural deduction*
- A common basis for implementations
- Type theories are commonly used, but Isabelle uses a simple meta-logic whose main primitives are
  - $\Rightarrow$ (implication)
  - $\forall$ (universal quantification)
Isabelle’s Family of Logics

- ZF
- LCF

- FOL
- IFOL
- CTT

- HOL
- HOLCF
- LK

- Modal logics

Pure Isabelle
Isabelle’s Family of Logics

Pure Isabelle

ZF   LCF

FOL

IFOL

CTT   HOL

HOLCF

LK

Modal logics
Natural Deduction in Isabelle
Natural Deduction in Isabelle

\[
\frac{P \quad Q}{P \land Q} \quad \quad P \Rightarrow (Q \Rightarrow P \land Q)
\]
Natural Deduction in Isabelle

\[
\frac{P}{P \land Q} \quad \frac{Q}{P \land Q}
\]

\[
P \Rightarrow (Q \Rightarrow P \land Q)
\]

\[
\frac{P \land Q}{P}
\]

\[
P \land Q \Rightarrow P
\]
Natural Deduction in Isabelle

\[
\begin{align*}
\frac{P}{P \land Q} & \quad P \Rightarrow (Q \Rightarrow P \land Q) \\
\frac{P \land Q}{P} & \quad P \land Q \Rightarrow P \\
\frac{P \land Q}{Q} & \quad P \land Q \Rightarrow Q
\end{align*}
\]
Natural Deduction in Isabelle

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

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

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

\[ \frac{P \rightarrow Q \quad P}{Q} \quad (P \rightarrow Q \Rightarrow (P \Rightarrow Q)) \]
Meta-implication
Meta-implication

• The symbol $\Rightarrow$ (or $\implies$) expresses the relationship between premise and conclusion
Meta-implication

• The symbol $\Rightarrow$ (or $\Longrightarrow$) expresses the relationship between premise and conclusion

• ...and between subgoal and goal.
Meta-implication

- The symbol $\Rightarrow$ (or $\Longrightarrow$) expresses the relationship between premise and conclusion.
- ... and between subgoal and goal.
- It is distinct from $\rightarrow$, which is not part of Isabelle's underlying logical framework.
Meta-implication

• The symbol $\Rightarrow$ (or $==\Rightarrow$) expresses the relationship between premise and conclusion
• ... and between subgoal and goal.
• It is distinct from $\rightarrow$, which is not part of Isabelle’s underlying logical framework.
• $P \Rightarrow (Q \Rightarrow R)$ is abbreviated as $\llbracket P ; Q \rrbracket \Rightarrow R$
A Trivial Proof

proof (prove): step 0

goal (1 subgoal):
1. (P; P → Q) → P ∧ Q
A Trivial Proof

reduce the goal using the given rule
Proof by Assumption

holds trivially, by assumption
Proof by Assumption

lemma "P → P → Q → P ∧ Q"
apply (rule conjI)
  apply assumption
apply (rule mp)
  apply assumption
  apply assumption
  apply assumption
done

proof (prove): step 2

goal (1 subgoal):
  1. [P; P → Q] → Q
Unknowns in Subgoals

```plaintext
lemma "P \implies P \implies Q \implies P \land Q"
apply (rule conjI)
apply assumption
apply (rule mp)
apply assumption
apply assumption
done

proof (prove): step 3

goal (2 subgoals):
1. [P; P \rightarrow Q] \implies ?P3 \rightarrow Q
2. [P; P \rightarrow Q] \implies ?P3
```

```
*goals*
Top 1 (Isar Proofstate Utoks Abbrev;)
tool-bar next
```
Unknowns in Subgoals

We need some instance of [rule mp].

Proof (prove): step 3

Goal (2 subgoals):
1. \([P; P \rightarrow Q] \Rightarrow ?P3 \rightarrow Q\)
2. \([P; P \rightarrow Q] \Rightarrow ?P3\)
Unknowns in Subgoals

We need some instance of mp!

formula placeholder
Unknowns and Unification

```
lemma "\( P \rightarrow P \rightarrow Q \rightarrow P \land Q \)"
apply (rule conjI)
  apply assumption
apply (rule mp)
  apply assumption
apply assumption
done
```

```
proof (prove): step 4

goal (1 subgoal):
  1. \([P; P \rightarrow Q] \rightarrow P\)
```
Unknowns and Unification

lemma "P \implies P \implies Q \implies P \land Q"
apply (rule conjI)
apply assumption
apply (rule mp)
apply assumption
apply assumption
done

proof (prove): step 4

goal (1 subgoal):
1. \([P; P \implies Q] \implies P\)

?P3 has been replaced by P
Discharging Assumptions
Discharging Assumptions

\[
\begin{align*}
&\quad [P] \\
&\quad \vdots \\
&\quad Q \\
&P \rightarrow Q \\
\hline
&\quad (P \Rightarrow Q) \Rightarrow P \rightarrow Q
\end{align*}
\]
Discharging Assumptions

\[
\begin{align*}
&\vdash P \\
&\vdots \\
&Q \\
&P \rightarrow Q
\end{align*}
\]

\[
(P \Rightarrow Q) \Rightarrow P \rightarrow Q
\]

\[
\begin{align*}
&P \lor Q \\
\vdots &P \\
\vdots &Q \\
&P \Rightarrow R \\
&Q \Rightarrow R
\end{align*}
\]

\[
\begin{array}{c}
\vdash P \lor Q; P \Rightarrow R; Q \Rightarrow R
\end{array}
\Rightarrow
\]

\[
\begin{array}{c}
R
\end{array}
\]
A Proof using Assumptions

```
lemma "P ∨ P → P"
apply (rule impl)
apply (erule disjE)
apply assumption+
done

proof (prove): step 0

goal (1 subgoal):
1. P ∨ P → P
```
A Proof using Assumptions

Subgoal is an implication, no assumptions
After Implies-Introduction

proof (prove): step 1

goal (1 subgoal):
1. $P \lor P \implies P$
After Implies-Introduction

Prove P using $P \lor P$
After Implies-Introduction

Prove $P$ using $P \lor P$

Assumption will be used, then deleted
Disjunction Elimination

proof (prove): step 2

goal (2 subgoals):
1. \( P \implies P \)
2. \( P \implies P \)
Disjunction Elimination

```
lemma "P ∨ P → P"
apply (rule impl)
apply (erule disjE)
apply assumption+
done
```

erule is good with elimination rules

proof (prove): step 2

goal (2 subgoals):
1. P → P
2. P → P
Disjunction Elimination

An instance of $P \lor Q$ has been found.

erule is good with elimination rules

proof (prove): step 2

goal (2 subgoals):
1. $P \Rightarrow P$
2. $P \Rightarrow P$
The Final Step

```
lemma "P v P --> P"
apply (rule impl)
apply (erule disjE)
apply assumption

done
```

```
proof (prove): step 3

goal:
No subgoals!
```
The Final Step

+ applies a method one or more times
Quantifiers
Quantifiers

\[
\frac{P(t)}{\exists x. P(x)} \quad P(x) \Rightarrow \exists x. P(x)
\]
Quantifiers

\[
\frac{P(t)}{\exists x. P(x)} \quad P(x) \Rightarrow \exists x. P(x)
\]

\[
\exists x. P(x) \quad Q
\]

\[
\Rightarrow \quad Q
\]

\[
[\exists x. P(x); \ \Lambda x. P(x) \Rightarrow Q] \Rightarrow Q
\]
Quantifiers

\[
\frac{P(t)}{\exists x. P(x)}
\]

\[
P(x) \Rightarrow \exists x. P(x)
\]

[∃x. P(x); \ ∀x. P(x) ⇒ Q] ⇒ Q

meta-universal quantifier states the variable condition
A Tiny Quantifier Proof

lemma "(\exists x. P (f x) \land Q x) \implies \exists x. P x"
apply (erule exE)
apply (erule conjE)
apply (rule exI)
apply assumption
done

proof (prove): step 0

goal (1 subgoal):
1. \exists x. P (f x) \land Q x \implies \exists x. P x
A Tiny Quantifier Proof

Find, use, delete an existential assumption
Conjunction Elimination

Lemma: 

\[(\exists x. \, P(f(x)) \land Q(x)) \Rightarrow \exists x. \, P(x)\]

Apply (erule exE)
Apply (erule conjE)
Apply (rule exI)
Apply assumption
Done

Proof (prove): step 1

Goal (1 subgoal):
1. \(\forall x. \, P(f(x)) \land Q(x) \Rightarrow \exists x. \, P(x)\)
Conjunction Elimination

The $x$ that is claimed to exist
Conjunction Elimination

Find, use, delete a conjunctive assumption

The $x$ that is claimed to exist
Now for $\exists$-Introduction

proof (prove): step 2

goal (1 subgoal):
  1. $\forall x. \[(P(f(x) \land Q(x)) \Rightarrow \exists x. P(x)]$
Now for \( \exists \)-Introduction

Two assumptions instead of one

```
lemma "(\(\exists x. P(f x) \land Q x\)) \Rightarrow \exists x. P x"
apply (erule exE)
apply (erule conjE)
apply (rule exI)
apply assumption
done
```

proof (prove): step 2

goal (1 subgoal):
1. \(\forall x. [P(f x); Q x] \Rightarrow \exists x. P x\)
Now for $\exists$-Introduction

Two assumptions instead of one

Apply the rule $\text{exI}$
An Unknown for the Witness

lemma "(\exists x. P (f x) \land Q x) \implies \exists x. P x"
apply (erule exE)
apply (erule conjE)
apply (rule exI)
apply assumption
done

proof (prove): step 3

goal (1 subgoal):
1. \(\forall x. [P (f x); Q x] \implies P (?x4 x)\)
An Unknown for the Witness

Proof by assumption will unify these two terms.
Done!

lemma "(\exists x. P (f x) \land Q x) \implies \exists x. P x"
apply (erule exE)
apply (erule conjE)
apply (rule exI)
apply assumption

proof (prove): step 4

goal:
No subgoals!