Introduction to the Isabelle Proof Assistant

Clemens Ballarin
Gerwin Klein
Tutorial Schedule

- Session I
  - Basics
- Session II
  - Specification Tools
  - Readable Proofs
- Session III
  - More on Readable Proofs
  - Modules
- Session IV
  - Applications
  - Q & A session with Larry Paulson
Session I

Basics
System Architecture

Isabelle — Generic, interactive theorem prover
System Architecture

Isabelle — Generic, interactive theorem prover
Standard ML — Logic implemented as ADT
System Architecture

HOL, ZF — Object-logics
Isabelle — Generic, interactive theorem prover
Standard ML — Logic implemented as ADT
System Architecture

Proof General — User interface
HOL, ZF — Object-logics
Isabelle — Generic, interactive theorem prover
Standard ML — Logic implemented as ADT
System Architecture

User can access all layers!

- Proof General — User interface
- HOL, ZF — Object-logics
- Isabelle — Generic, interactive theorem prover
- Standard ML — Logic implemented as ADT
Documentation

Available from http://isabelle.in.tum.de
Available from http://isabelle.in.tum.de

- Learning Isabelle
Documentation

Available from http://isabelle.in.tum.de

- Learning Isabelle
  - Tutorial on Isabelle/HOL (LNCS 2283)
  - Tutorial on Isar
  - Tutorial on Locales
Documentation

Available from http://isabelle.in.tum.de

- Learning Isabelle
  - Tutorial on Isabelle/HOL (LNCS 2283)
  - Tutorial on Isar
  - Tutorial on Locales

- Reference Manuals
Available from http://isabelle.in.tum.de

- Learning Isabelle
  - Tutorial on Isabelle/HOL (LNCS 2283)
  - Tutorial on Isar
  - Tutorial on Locales

- Reference Manuals
  - Isabelle/Isar Reference Manual
  - Isabelle Reference Manual
  - Isabelle System Manual
Documentation

Available from http://isabelle.in.tum.de

- Learning Isabelle
  - Tutorial on Isabelle/HOL (LNCS 2283)
  - Tutorial on Isar
  - Tutorial on Locales

- Reference Manuals
  - Isabelle/Isar Reference Manual
  - Isabelle Reference Manual
  - Isabelle System Manual

- Reference Manuals for Object-Logics
Isabelle’s Meta-Logic

- Intuitionistic fragment of Church’s theory of simple types.
Isabelle’s Meta-Logic

- Intuitionistic fragment of Church’s theory of simple types.
- With type variables.
Isabelle’s Meta-Logic

- Intuitionistic fragment of Church’s theory of simple types.
- With type variables.
- Can be used to formalise your own object-logic.
Isabelle’s Meta-Logic

- Intuitionistic fragment of Church’s theory of simple types.
- With type variables.
- Can be used to formalise your own object-logic.
- Normally, use rich infrastructure of the object-logics HOL and ZF.
Isabelle’s Meta-Logic

- Intuitionistic fragment of Church’s theory of simple types.
- With type variables.
- Can be used to formalise your own object-logic.
- Normally, use rich infrastructure of the object-logics HOL and ZF.
- This presentation assumes HOL.
Types
Syntax:

\[ \tau ::= (\tau) \]

\[ | \ 'a | 'b | \ldots \]

Type variables
Syntax:

\[ \tau ::= (\tau) \]
\[ | \quad \text{type variables} \quad \]
\[ | \quad a \quad | \quad b \quad | \ldots \quad \]
\[ | \quad \tau \Rightarrow \tau \quad \text{total functions} \]
Syntax:

\[ \tau ::= (\tau) \]

| \[ \mid 'a \mid 'b \mid \ldots \] type variables
| \[ \mid \tau \rightarrow \tau \] total functions
| \[ \mid \text{bool} \mid \text{nat} \mid \ldots \] HOL base types
Syntax:

\[ \tau ::= (\tau) \]

| 'a | 'b | ... | \text{type variables} |
| \tau \Rightarrow \tau | \text{total functions} |
| bool | nat | ... | \text{HOL base types} |
| \tau \times \tau | \text{HOL pairs (ascii: *)} |
Syntax:

\[
\tau ::= (\tau) \\
  \mid 'a \mid 'b \mid \ldots \quad \text{type variables} \\
  \mid \tau \Rightarrow \tau \quad \text{total functions} \\
  \mid \text{bool} \mid \text{nat} \mid \ldots \quad \text{HOL base types} \\
  \mid \tau \times \tau \quad \text{HOL pairs (ascii: *)} \\
  \mid \tau \ \text{list} \quad \text{HOL lists}
\]
Syntax:

\[ \tau ::= (\tau) \]
\[ \tau \Rightarrow \tau \]
\[ \texttt{bool} | \texttt{nat} | \ldots \]
\[ \tau \times \tau \]
\[ \tau \texttt{list} \]
\[ \ldots \]

- type variables
- total functions
- HOL base types
- HOL pairs (ascii: * )
- HOL lists
- user-defined types
Syntax

Syntax:

\[ \tau ::= (\tau) \]
\[ \ | \ 'a \ | \ 'b \ | \ldots \quad \text{type variables} \]
\[ \ | \ \tau \Rightarrow \tau \quad \text{total functions} \]
\[ \ | \ \textit{bool} \ | \ \textit{nat} \ | \ldots \quad \text{HOL base types} \]
\[ \ | \ \tau \times \tau \quad \text{HOL pairs (ascii: \ *)} \]
\[ \ | \ \tau \ \textit{list} \quad \text{HOL lists} \]
\[ \ | \ \ldots \quad \text{user-defined types} \]

Parentheses: \[ T1 \Rightarrow T2 \Rightarrow T3 \equiv T1 \Rightarrow (T2 \Rightarrow T3) \]
Introducing new Types: typedef

typedecl name

Introduces new “opaque” type name without definition.


**Introducing new Types: typedecl**

**typedecl** *name*

Introduces new “opaque” type *name* without definition.

Example:

**typedecl** *addr*  —An abstract type of addresses.
Terms
Syntax: (curried version)

\[ \text{term} ::= (\text{term}) \]
Syntax: (curried version)

\[ \text{term} ::= (\text{term}) \]
\[ \text{constant or variable (identifier)} \]
Syntax

Syntax: (curried version)

\[ term ::= (term) \]

\[ \]

constant or variable (identifier)

function application

\[ \]

\[ \]

Examples:

\[ f \ (g \ x) \ y \ h \ (x. \ f \ (g \ x)) \]
Syntax: (curried version)

\[ \text{term} ::= (\text{term}) \]
\[ \quad | \quad a \quad \text{constant or variable (identifier)} \]
\[ \quad | \quad \text{term term} \quad \text{function application} \]
\[ \quad | \quad \lambda x. \text{term} \quad \text{function “abstraction”} \]
Syntax

Syntax: (curried version)

```
term ::= (term)
| a
| term term
| \lambda x. term
| ...
```

constant or variable (identifier)
function application
function “abstraction”
lots of syntactic sugar
Syntax: (curried version)

\[
\text{term} ::= (\text{term})
\]

constant or variable (identifier)

function application

function “abstraction”

lots of syntactic sugar

Examples: \( f (g \, x) \, y \quad h (\lambda x. f (g \, x)) \)
Syntax: (curried version)

\[
\text{term} ::= (\text{term}) \\
| \ a \quad \text{constant or variable (identifier)} \\
| \text{term} \ \text{term} \quad \text{function application} \\
| \lambda x. \ \text{term} \quad \text{function “abstraction”} \\
| \ldots \quad \text{lots of syntactic sugar}
\]

Examples: \[f (g \ x) \ y \quad h (\lambda x. \ f (g \ x))\]

Parentheses: \[f \ a_1 \ a_2 \ a_3 \equiv ((f \ a_1) \ a_2) \ a_3\]
Schematic variables

Three kinds of variables:

- **bound**: $\forall x. x = x$
- **free**: $x = x$
Three kinds of variables:

- **bound**: $\forall x. \ x = x$
- **free**: $x = x$
- **schematic**: $?x = ?x$ ("unknown")
Schematic variables

Three kinds of variables:

- **bound**: $\forall x. \ x = x$
- **free**: $x = x$
- **schematic**: $?x = ?x$ (“unknown”)

Logically: free = schematic
Schematic variables

Three kinds of variables:

- **bound:** $\forall x. \ x = x$
- **free:** $x = x$
- **schematic:** $?x = ?x$ ("unknown")

- Logically: free = schematic
- Operationally:
  - free variables are fixed
  - schematic variables are instantiated by substitutions and unification
Theorems
Connectives of the Meta-Logic

Implication $\iff (\implies)$
For separating premises and conclusion of theorems.
Connectives of the Meta-Logic

Implication $\implies (\Rightarrow)$
For separating premises and conclusion of theorems.

Equality $\equiv (\equiv)$
For definitions.
Connectives of the Meta-Logic

**Implication** $\implies (\implies \implies)$
For separating premises and conclusion of theorems.

**Equality** $\equiv (\equiv)$
For definitions.

**Universal quantifier** $\forall (\exists \exists)$
For parameters in goals.
Connectives of the Meta-Logic

Implication \[\implies (\Rightarrow)\]
For separating premises and conclusion of theorems.

Equality \[\equiv (\equiv)\]
For definitions.

Universal quantifier \[\forall (\forall)\]
For parameters in goals.

Do not use inside object-logic formulae.
Notation

\[ \langle A_1; \ldots ; A_n \rangle \models B \]

abbreviates

\[ A_1 \models \ldots \models A_n \models B \]
Notation

\[ [ A_1 ; \ldots ; A_n ] \implies B \]

abbreviates

\[ A_1 \implies \ldots \implies A_n \implies B \]

; \quad \approx \quad \text{"and"}
Introducing New Theorems

- As axioms.
Introducing New Theorems

- As axioms.
- Through definitions.
Introducing New Theorems

- As axioms.
- Through definitions.
- Through proofs.
Introducing New Theorems

- As axioms.
- Through definitions.
- Through proofs.

Axioms should mainly be used when specifying object-logics.
Definition (non-recursive)

Declaration:

\textbf{consts}
\begin{align*}
    & sq :: nat \Rightarrow nat \\
\end{align*}

Definition:

\textbf{defs}
\begin{align*}
    & sq\_def: sq \ n \equiv n*n \\
\end{align*}
Definition (non-recursive)

Declaration:

\textbf{consts}

\begin{align*}
    sq & :: nat \rightarrow nat
\end{align*}

Definition:

\textbf{defs}

\begin{align*}
    sq\_def & : sq\ n \equiv n^2
\end{align*}

Declaration + definition:

\textbf{constdefs}

\begin{align*}
    sq & :: nat \rightarrow nat \\
    sq\ n & \equiv n^2
\end{align*}
Proofs

General schema:

lemma name: <goal>
apply <method>
apply <method>
::
done
Proofs

General schema:

lemma \( name \) : \(<goal>\)
apply \(<method>\)
apply \(<method>\)
·
done

- Sequential application of methods until all \texttt{subgoals} are solved.
The proof state

1. \( \bigwedge x_1 \ldots x_p. \left[ A_1; \ldots ; A_n \right] \rightarrow B \)
2. \( \bigwedge y_1 \ldots y_q. \left[ C_1; \ldots ; C_n \right] \rightarrow D \)
The proof state

1. \( \land x_1 \ldots x_p \cdot [A_1; \ldots ; A_n] \implies B \)
2. \( \land y_1 \ldots y_q \cdot [C_1; \ldots ; C_n] \implies D \)

- \( x_1 \ldots x_p \): Parameters
- \( A_1 \ldots A_n \): Local assumptions
- \( B \): Actual (sub)goal
Isabelle Theories
Theory = Source file

Syntax:

```plaintext
theory \textit{MyTh} = \textit{ImpTh}_1 + \ldots + \textit{ImpTh}_n:\n(declarations, definitions, theorems, proofs, ...)*
end
```

- \textit{MyTh}: name of theory. Must live in file \textit{MyTh}.thy
- \textit{ImpTh}_i: name of imported theories. Import transitive.
Theory = Source file

Syntax:

theory *MyTh* = *ImpTh_1* + ... + *ImpTh_n*:
(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* = Main:
X-Symbols

Input of funny symbols in Proof General

- via menu ("X-Symbol")
- via ascii encoding (similar to \LaTeX): \&and>, \&<or>, ...
- via abbreviation: \&/, \&/, -->, ...

<table>
<thead>
<tr>
<th>x-symbol</th>
<th>\forall</th>
<th>\exists</th>
<th>\lambda</th>
<th>\neg</th>
<th>\land</th>
<th>\lor</th>
<th>\rightarrow</th>
<th>\Rightarrow</th>
</tr>
</thead>
<tbody>
<tr>
<td>ascii (1)</td>
<td>&amp;forall&gt;</td>
<td>&amp;&lt;exists&gt;</td>
<td>&amp;&lt;lambda&gt;</td>
<td>&amp;&lt;not&gt;</td>
<td>&amp;/</td>
<td>&amp;/</td>
<td>--&gt;</td>
<td>=&gt;</td>
</tr>
<tr>
<td>ascii (2)</td>
<td>ALL</td>
<td>EX</td>
<td>%</td>
<td>~</td>
<td>&amp;</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(1) is converted to x-symbol, (2) stays ascii.
Demo: Isabelle theories
Natural Deduction
Rules

\[
\begin{align*}
\text{conjI} & \quad A \land B \\
\text{disjI} & \quad A \lor B \quad A \lor B \\
\text{impl} & \quad A \rightarrow B \\
\end{align*}
\]

\[
\begin{align*}
\text{conjE} & \quad A \land B \\
\text{disjE} & \quad A \lor B \\
\text{impE} & \quad A \rightarrow B
\end{align*}
\]
Rules

- **conjI**
  \[
  \frac{A \quad B}{A \land B}
  \]

- **disjI1/2**
  \[
  \frac{A}{A \lor B} \quad \frac{B}{A \lor B}
  \]

- **impl**
  \[
  \frac{A \implies B}{A \implies B}
  \]

- **conjE**
  \[
  \frac{A \land B}{C}
  \]

- **disjE**
  \[
  \frac{A \lor B}{C}
  \]

- **impE**
  \[
  \frac{A \implies B}{C}
  \]
Rules

\[
\frac{A \land B}{A \land B} \quad \text{conjl}
\]

\[
\frac{A \lor B}{A \lor B} \quad \frac{B}{A \lor B} \quad \text{disjl1/2}
\]

\[
\frac{A \Rightarrow B}{A \Rightarrow B} \quad \text{impl}
\]

\[
\frac{A \land B}{C} \quad \text{conjE}
\]

\[
\frac{\neg A \lor \neg B}{C} \quad \text{disjE}
\]

\[
\frac{A \Rightarrow B}{A \Rightarrow B} \quad \frac{B \Rightarrow C}{C} \quad \text{impE}
\]

\[
\frac{A \land B \quad [A;B]}{C} \quad \text{conjE}
\]

\[
\frac{A \lor B \quad A \Rightarrow C \quad B \Rightarrow C}{C} \quad \text{disjE}
\]

\[
\frac{A \Rightarrow B \quad A \quad B \Rightarrow C}{C} \quad \text{impE}
\]
Proof by assumption

apply assumption

proves

1. \[
[ B_1; \ldots ; B_m ] \rightarrow C
\]

by unifying \( C \) with one of the \( B_i \)
Proof by assumption

apply assumption

proves

1. \([ B_1; \ldots ; B_m ] \rightarrow C\)

by unifying \(C\) with one of the \(B_i\) (backtracking!)
Intro rules decompose formulae to the right of $\rightarrow$.

apply\,(rule\, <intro-rule>)
How to prove it by natural deduction

- **Intro** rules decompose formulae to the right of $\rightarrow$.

  apply\((rule \ <intro\text{-rule}>\))

Applying rule \([ A_1; \ldots ; A_n ] \rightarrow A\) to subgoal $C$:

- Unify $A$ and $C$
How to prove it by natural deduction

- **Intro** rules decompose formulae to the right of $\implies$.

  \begin{align*}
  & \text{apply}(\text{rule } <\text{intro-rule}>) \\
  & \text{Applying rule } [ A_1 ; \ldots ; A_n ] \implies A \text{ to subgoal } C: \\
  & \quad \text{Unify } A \text{ and } C \\
  & \quad \text{Replace } C \text{ with } n \text{ new subgoals } A_1 \ldots A_n
  \end{align*}
How to prove it by natural deduction

- **Intro** rules decompose formulae to the right of \( \rightarrow \).

  \[ \text{apply(rule intro-rule)} \]

  Applying rule \([ A_1; \ldots ; A_n ] \rightarrow A\) to subgoal \( C \):
  - Unify \( A \) and \( C \)
  - Replace \( C \) with \( n \) new subgoals \( A_1 \ldots A_n \)

- **Elim** rules decompose formulae on the left of \( \rightarrow \).

  \[ \text{apply(erule elim-rule)} \]
How to prove it by natural deduction

- **Intro** rules decompose formulae to the right of $\rightarrow$.

  apply\((\text{rule } <\text{intro-rule}>))$

  Applying rule $[ A_1; \ldots ; A_n ] \rightarrow A$ to subgoal $C$:
  - Unify $A$ and $C$
  - Replace $C$ with $n$ new subgoals $A_1 \ldots A_n$

- **Elim** rules decompose formulae on the left of $\rightarrow$.

  apply\((\text{erule } <\text{elim-rule}>))$

  Like $\text{rule}$ but also
  - unifies first premise of rule with an assumption
  - eliminates that assumption
Demo: natural deduction
Safe and unsafe rules

Safe rules preserve provability
Safe and unsafe rules

**Safe rules** preserve provability

  - conjI,
  - impI,
  - conjE,
  - disjE,
  - notI,
  - iffI,
  - refl,
  - ccontr,
  - classical

Apply safe rules before unsafe ones
Safe and unsafe rules

Safe rules preserve provability
   conjI, impI, conjE, disjE,
   notI, iffI, refl, ccontr, classical

Unsafe rules can turn provable goal into unprovable goal
Safe and unsafe rules

**Safe rules** preserve provability
- `conjI`, `impI`, `conjE`, `disjE`,
- `notI`, `iffI`, `refl`, `ccontr`, `classical`

**Unsafe rules** can turn provable goal into unprovable goal
- `disjI1`, `disjI2`, `impE`,
- `iffD1`, `iffD2`, `notE`
Safe and unsafe rules

Safe rules preserve provability
conjI, impI, conjE, disjE,
notI, iffI, refl, ccontr, classical

Unsafe rules can turn provable goal into unprovable goal
disjI1, disjI2, impE,
iffD1, iffD2, notE

Apply safe rules before unsafe ones
Predicate Logic: $\forall$ and $\exists$
Scope

- Scope of parameters: whole subgoal
- Scope of $\forall$, $\exists$, \ldots: ends with ; or $\implies$
Scope

- Scope of parameters: whole subgoal
- Scope of $\forall, \exists, \ldots$: ends with ; or $\rightarrow$

$$\forall x \forall y. \left[ \forall y. P y \rightarrow Q z y; Q x y \right] \rightarrow \exists x. Q x y$$
Scope

- Scope of parameters: whole subgoal
- Scope of $\forall, \exists, \ldots$: ends with $;$ or $\Rightarrow$

\[
\land x \ y. [ \land y. P \ y \rightarrow Q \ z \ y; \ Q \ x \ y ] \Rightarrow \exists x. Q \ x \ y
\]

means

\[
\land x \ y. [ (\forall y_1. P \ y_1 \rightarrow Q \ z \ y_1); \ Q \ x \ y ] \Rightarrow (\exists x_1. Q \ x_1 \ y)
\]
Natural deduction for quantifiers

\[ \forall x. P x \quad \text{allI} \]

\[ \exists x. P x \quad \text{exI} \]

\[ \forall x. P x \quad \text{allE} \]

\[ \exists x. P x \quad \text{exE} \]
Natural deduction for quantifiers

\[ \forall x. P x \quad \forall x. P x \quad \text{allI} \]

\[ \exists x. P x \quad \exists x. P x \quad \text{exI} \]

\[ \exists x. P x \quad \forall x. P x \quad \iff R \quad \text{exE} \]

\[ \forall x. P x \quad R \quad \text{allE} \]

\[ \iff \]

\[ \text{introduce new parameters (}_V x_\text{).} \]

\[ \text{introduce new unknowns (}_?x_\text{).} \]
Natural deduction for quantifiers

\[ \forall x. P x \quad \exists x. P x \]

\[ \frac{\forall x. P x}{\forall x. P x} \text{ allI} \]

\[ \frac{\exists x. P x}{\exists x. P x} \text{ exI} \]

\[ \frac{\forall x. P x \quad P ?x}{R} \text{ allE} \]

\[ \frac{\exists x. P x \quad \forall x. P x}{R} \text{ exE} \]
Natural deduction for quantifiers

\[
\begin{align*}
\forall x. P x & \quad \forall x. P x & \quad \text{allI} \\
\forall x. P x & \quad P ?x & \quad \Rightarrow & \quad R & \quad \text{allE} \\
\exists x. P x & \quad \exists x. P x & \quad \text{exI} \\
\exists x. P x & \quad \forall x. P x & \quad \Rightarrow & \quad R & \quad \text{exE}
\end{align*}
\]

- allI and exE introduce new parameters (\(\forall x\)).
- allE and exI introduce new unknowns (\(?x\)).
**Instantiating rules**

\[\text{apply}(\text{rule_tac } x = "\text{term}" \text{ in } \text{rule})\]

Like \textit{rule}, but \(x\) in \textit{rule} is instantiated by \textit{term} before application.
Instantiating rules

apply(rule_tac x = "term" in rule)

Like rule, but ?x in rule is instantiated by term before application.

Similar: erule_tac
**Instantiating rules**

\[
\text{apply}(\text{rule_tac } x = "\text{term}" \text{ in } \text{rule})
\]

Like `rule`, but `?x` in `rule` is instantiated by `term` before application.

Similar: `erule_tac`

\[
! \quad x \text{ is in } \text{rule}, \text{ not in the goal} \quad !
\]
Safe and unsafe rules

Safe  allI, exE
Unsafe  allE, exI
Safe and unsafe rules

Safe  allI, exE
Unsafe  allE, exI

Create parameters first, unknowns later
Forward proofs: frule and drule

\texttt{apply(frule \textit{rulename})}

Forward rule: \[ A_1 \implies A \]
Subgoal: \[ 1. \quad [B_1; \ldots; B_n] \implies C \]
Forward proofs: frule and drule

apply(frule rulename)

Forward rule: \( A_1 \implies A \)
Subgoal: \( 1. [ B_1; \ldots ; B_n ] \implies C \)
Unifies: one \( B_i \) with \( A_1 \)
New subgoal: \( 1. [ B_1; \ldots ; B_n ; A ] \implies C \)
Forward proofs: frule and drule

\[ \text{forward proof: } \quad \text{frule rulename} \]

Forward rule: \[ A_1 \Rightarrow A \]
Subgoal: \[ 1. [ B_1; \ldots ; B_n ] \Rightarrow C \]
Unifies: one \( B_i \) with \( A_1 \)
New subgoal: \[ 1. [ B_1; \ldots ; B_n; A ] \Rightarrow C \]

\[ \text{apply(drule rulename)} \]

Like \textit{frule} but also deletes \( B_i \)
Demo: quantifier proofs
Practical Session I

In the cool morning
A man simplifies, a goal
A theorem is born.

— Don Syme