Concrete Semantics
with Isabelle/HOL

Tobias Nipkow

Fakultät für Informatik
Technische Universität München

2017-3-8
Part I

Isabelle
Chapter 2

Programming and Proving
1. Overview of Isabelle/HOL

2. Type and function definitions

3. Induction Heuristics

4. Simplification
Implication associates to the right:

\[ A \implies B \implies C \quad \text{means} \quad A \implies (B \implies C) \]

Similarly for other arrows: \( \Rightarrow \), \( \rightarrow \)

\[ \frac{A_1 \ldots A_n}{B} \quad \text{means} \quad A_1 \implies \ldots \implies A_n \implies B \]
1. Overview of Isabelle/HOL

2. Type and function definitions

3. Induction Heuristics

4. Simplification
HOL = Higher-Order Logic
HOL = Functional Programming + Logic

HOL has
- datatypes
- recursive functions
- logical operators

HOL is a programming language!

Higher-order = functions are values, too!

HOL Formulas:
- For the moment: only \( \text{term} = \text{term} \), e.g. \( 1 + 2 = 4 \)
- Later: \( \land, \lor, \rightarrow, \forall, \ldots \)
Overview of Isabelle/HOL

Types and terms

Interface

By example: types bool, nat and list

Summary
Types

Basic syntax:

\[ \tau ::= \left( \tau \right) \mid \text{bool} \mid \text{nat} \mid \text{int} \mid \ldots \mid 'a \mid 'b \mid \ldots \mid \tau \Rightarrow \tau \mid \tau \times \tau \mid \tau \text{ list} \mid \tau \text{ set} \mid \ldots \]

base types

base types

type variables

functions

pairs (ascii: \( * \))

lists

sets

user-defined types

Convention: \( \tau_1 \Rightarrow \tau_2 \Rightarrow \tau_3 \equiv \tau_1 \Rightarrow (\tau_2 \Rightarrow \tau_3) \)
Terms can be formed as follows:

- **Function application:** \( f t \)
  is the call of function \( f \) with argument \( t \).
  If \( f \) has more arguments: \( f t_1 t_2 \ldots \)
  Examples: \( \sin \pi, \ \text{plus} \ x \ y \)

- **Function abstraction:** \( \lambda x. t \)
  is the function with parameter \( x \) and result \( t \),
  i.e. “\( x \mapsto t \)”.  
  Example: \( \lambda x. \text{plus} \ x \ x \)
Terms

Basic syntax:

\[ t ::= (t) \]
\[ \mid a \quad \text{constant or variable (identifier)} \]
\[ \mid t \, t \quad \text{function application} \]
\[ \mid \lambda x. \, t \quad \text{function abstraction} \]
\[ \mid \ldots \quad \text{lots of syntactic sugar} \]

Examples:

\[ f \,(g \, x) \, y \]
\[ h \,(\lambda x. \, f \,(g \, x)) \]

Convention:

\[ f \, t_1 \, t_2 \, t_3 \equiv ((f \, t_1) \, t_2) \, t_3 \]

This language of terms is known as the \( \lambda \)-calculus.
The computation rule of the $\lambda$-calculus is the replacement of formal by actual parameters:

$$(\lambda x. \ t) \ u \ = \ t[u/x]$$

where $t[u/x]$ is “$t$ with $u$ substituted for $x$.”

Example: $$(\lambda x. \ x + 5) \ 3 \ = \ 3 + 5$$

- The step from $(\lambda x. \ t) \ u$ to $t[u/x]$ is called \textit{\textbf{\textbeta}}-\textit{reduction}.
- Isabelle performs $\beta$-reduction automatically.
Terms must be well-typed
(the argument of every function call must be of the right type)

Notation:
\( t :: \tau \) means “\( t \) is a well-typed term of type \( \tau \).”

\[
\frac{t :: \tau_1 \Rightarrow \tau_2 \quad u :: \tau_1}{t \ u :: \tau_2}
\]
Type inference

Isabelle automatically computes the type of each variable in a term. This is called *type inference*.

In the presence of *overloaded* functions (functions with multiple types) this is not always possible.

User can help with *type annotations* inside the term. Example: $f \, (x::nat)$
Currying

Thou shalt Curry your functions

- Curried: \( f :: \tau_1 \Rightarrow \tau_2 \Rightarrow \tau \)
- Tupled: \( f' :: \tau_1 \times \tau_2 \Rightarrow \tau \)

Advantage:

Currying allows *partial application*

\[ f \ a_1 \quad \text{where} \quad a_1 :: \tau_1 \]
Predefined syntactic sugar

- **Infix:** +, −, *, #, @, ...
- **Mixfix:** if _ then _ else _, case _ of, ...

Prefix binds more strongly than infix:

\[
!f \ x + y \equiv (f \ x) + y \neq f (x + y)
\]

Enclose if and case in parentheses:

\[
!(if \ _ \ then \ _ \ else \ _)
\]
Theory = Isabelle Module

Syntax: theory $MyTh$
imports $T_1 \ldots T_n$
begin
(definitions, theorems, proofs, ...)*
end

$MyTh$: name of theory. Must live in file $MyTh$.thy

$T_i$: names of imported theories. Import transitive.

Usually: imports Main
Concrete syntax

In .thy files:
Types, terms and formulas need to be inclosed in "

Except for single identifiers

" normally not shown on slides
Overview of Isabelle/HOL

Types and terms

Interface

By example: types \textit{bool}, \textit{nat} and \textit{list}

Summary
isabelle jedit

- Based on *jEdit* editor
- Processes Isabelle text automatically when editing `.thy` files (like modern Java IDEs)
Overview_Demo.thy
1 Overview of Isabelle/HOL

Types and terms

Interface

By example: types \textit{bool}, \textit{nat} and \textit{list}

Summary
Type `bool`

**datatype**  
`bool = True | False`

Predefined functions:  
\[\wedge, \vee, \rightarrow, \ldots : bool \Rightarrow bool \Rightarrow bool\]

A formula is a term of type `bool`

if-and-only-if: `=`
Type \( \text{nat} \)

\textbf{datatype} \quad \text{nat} \; = \; 0 \mid \text{Suc nat}

Values of type \( \text{nat} \): \( 0, \; \text{Suc 0}, \; \text{Suc(Suc 0)}, \ldots \)

Predefined functions: \( +, \; \ast, \ldots \; :: \; \text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat} \)

\! Numbers and arithmetic operations are overloaded:
\( 0,1,2,\ldots \; :: \; \text{'a}, \quad + \; :: \; \text{'a} \Rightarrow \text{'a} \Rightarrow \text{'a} \)

You need type annotations: \( 1 :: \text{nat}, \; x + (y :: \text{nat}) \)

unless the context is unambiguous: \( \text{Suc z} \)
Nat_Demo.thy
An informal proof

Lemma \( \text{add}\ m\ 0 = m \)

Proof by induction on \( m \).

- Case 0 (the base case):
  \( \text{add}\ 0\ 0 = 0 \) holds by definition of \( \text{add} \).

- Case \( \text{Suc}\ m \) (the induction step):
  We assume \( \text{add}\ m\ 0 = m \),
  the induction hypothesis (IH).
  We need to show \( \text{add}\ (\text{Suc}\ m)\ 0 = \text{Suc}\ m \).
  The proof is as follows:
  \[
  \text{add}\ (\text{Suc}\ m)\ 0 = \text{Suc}\ (\text{add}\ m\ 0) \quad \text{by def. of \( \text{add} \)}
  = \text{Suc}\ m \quad \text{by IH}
  \]
Type 'a list

Lists of elements of type 'a

datatype 'a list = Nil | Cons 'a ('a list)

Some lists: Nil, Cons 1 Nil, Cons 1 (Cons 2 Nil), ...

Syntactic sugar:
- [] = Nil: empty list
- x # xs = Cons x xs:
  list with first element x ("head") and rest xs ("tail")
- [x₁, ..., xₙ] = x₁ # ... xₙ # []
Structural Induction for lists

To prove that $P(xs)$ for all lists $xs$, prove

- $P([])$ and
- for arbitrary but fixed $x$ and $xs$, $P(xs)$ implies $P(x\#xs)$.

\[
P([]) \land \forall x \; xs. \; P(xs) \implies P(x\#xs)
\]

\[
\therefore \quad P(xs)
\]
List_Demo.thy
An informal proof

**Lemma** $\text{app}\ (\text{app}\ xs\ ys)\ zs = \text{app}\ xs\ (\text{app}\ ys\ zs)$

**Proof** by induction on $xs$.

- **Case Nil**: $\text{app}\ (\text{app}\ \text{Nil}\ ys)\ zs = \text{app}\ ys\ zs = \text{app}\ \text{Nil}\ (\text{app}\ ys\ zs)$ holds by definition of $\text{app}$.

- **Case Cons x xs**: We assume $\text{app}\ (\text{app}\ xs\ ys)\ zs = \text{app}\ xs\ (\text{app}\ ys\ zs)$ (IH), and we need to show $\text{app}\ (\text{app}\ (\text{Cons}\ x\ xs)\ ys)\ zs = \text{app}\ (\text{Cons}\ x\ xs)\ (\text{app}\ ys\ zs)$.

  The proof is as follows:
  \[
  \begin{align*}
  &\text{app}\ (\text{app}\ (\text{Cons}\ x\ xs)\ ys)\ zs \\
  &= \text{Cons}\ x\ (\text{app}\ (\text{app}\ xs\ ys)\ zs) \quad \text{by definition of } \text{app} \\
  &= \text{Cons}\ x\ (\text{app}\ xs\ (\text{app}\ ys\ zs)) \quad \text{by IH} \\
  &= \text{app}\ (\text{Cons}\ x\ xs)\ (\text{app}\ ys\ zs) \quad \text{by definition of } \text{app}
  \end{align*}
  \]
Large library: HOL/List.thy

Included in Main.

Don’t reinvent, reuse!

Predefined: $xs @ ys$ (append), $length$, and $map$

$$map\ f\ [x_1, \ldots, x_n] = [f\ x_1, \ldots, f\ x_n]$$

fun $map :: ('a => 'b) => 'a\ list => 'b\ list$ where

$map\ f\ [] = [] |$

$map\ f\ (x \#\ xs) = f\ x \#\ map\ f\ xs$

Note: $map$ takes $function$ as argument.
1 Overview of Isabelle/HOL

Types and terms

Interface

By example: types \texttt{bool}, \texttt{nat} and \texttt{list}

Summary
- **datatype** defines (possibly) recursive data types.

- **fun** defines (possibly) recursive functions by pattern-matching over datatype constructors.
Proof methods

- *induction* performs structural induction on some variable (if the type of the variable is a datatype).

- *auto* solves as many subgoals as it can, mainly by simplification (symbolic evaluation):

  “=” is used only from left to right!
Proofs

General schema:

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

If the lemma is suitable as a simplification rule:

```plaintext
lemma name[simp]: "..."
```
Top down proofs

Command

\texttt{sorry}

“completes” any proof.

Allows top down development:

\textit{Assume lemma first, prove it later.}
The proof state

1. $\land x_1 \ldots x_p \cdot A \implies B$

$x_1 \ldots x_p$ fixed local variables
$A$ local assumption(s)
$B$ actual (sub)goal
Multiple assumptions

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

abbreviates

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

; \quad \approx \quad "\text{and}"
1 Overview of Isabelle/HOL

2 Type and function definitions

3 Induction Heuristics

4 Simplification
2 Type and function definitions
   Type definitions
   Function definitions
Type synonyms

\texttt{type\_synonym} \hspace{1em} \textit{name} = \tau

Introduces a \textit{synonym} \textit{name} for type $\tau$

Examples

\texttt{type\_synonym} \hspace{1em} \textit{string} = \textit{char list}

\texttt{type\_synonym} \hspace{1em} (\textit{\textquoteleft}a,\textit{\textquoteleft}b)\textit{foo} = \textit{\textquoteleft}a list \times \textit{\textquoteleft}b list

Type synonyms are expanded after parsing and are not present in internal representation and output
**datatype — the general case**

\[
\text{datatype } (\alpha_1, \ldots, \alpha_n)t = \begin{array}{c}
C_1 \tau_{1,1} \cdots \tau_{1,n_1} \\
\vdots \\
C_k \tau_{k,1} \cdots \tau_{k,n_k}
\end{array}
\]

- **Types:** $C_i :: \tau_{i,1} \Rightarrow \cdots \Rightarrow \tau_{i,n_i} \Rightarrow (\alpha_1, \ldots, \alpha_n)t$
- **Distinctness:** $C_i \ldots \neq C_j \ldots$ if $i \neq j$
- **Injectivity:** $(C_i \ x_1 \ldots x_{n_i} = C_i \ y_1 \ldots y_{n_i}) = (x_1 = y_1 \land \cdots \land x_{n_i} = y_{n_i})$

Distinctness and injectivity are applied automatically
Induction must be applied explicitly
Case expressions

Datatype values can be taken apart with \textit{case}:

\[
\text{(case } xs \text{ of } [] \Rightarrow \ldots \mid y \# ys \Rightarrow \ldots y \ldots ys \ldots)\]

Wildcards: 

\[
\text{(case } m \text{ of } 0 \Rightarrow \text{Suc } 0 \mid \text{Suc } _{} \Rightarrow 0)\]

Nested patterns:

\[
\text{(case } xs \text{ of } [0] \Rightarrow 0 \mid [\text{Suc } n] \Rightarrow n \mid _{} \Rightarrow 2)\]

Complicated patterns mean complicated proofs!

Need ( ) in context
Tree_Demo.thy
The *option* type

datatype 'a option = None | Some 'a

If 'a has values \(a_1, a_2, \ldots\)
then 'a option has values None, Some \(a_1\), Some \(a_2\), \ldots

Typical application:

fun lookup :: ('a × 'b) list ⇒ 'a ⇒ 'b option where

\[
\begin{align*}
\text{lookup} \; [] \; x &= \text{None} \\
\text{lookup} \; ((a,b) \# \; ps) \; x &= \\
&\quad (\text{if } a = x \text{ then Some } b \text{ else lookup } ps \; x)
\end{align*}
\]
2 Type and function definitions
   Type definitions
     Function definitions
Non-recursive definitions

Example

definition sq :: nat ⇒ nat where sq n = n*n

No pattern matching, just f x₁ ... xₙ = ...
The danger of nontermination

How about $f \ x = f \ x + 1$?

! All functions in HOL must be total!
Key features of fun

- Pattern-matching over datatype constructors
- Order of equations matters
- Termination must be provable automatically by size measures
- Proves customized induction schema
Example: separation

\textbf{fun} \hspace{1em} \textit{sep} :: \textquote{'}a \Rightarrow \textquote{'}a \text{ list} \Rightarrow \textquote{'}a \text{ list} \ \textbf{where}

\begin{align*}
\text{sep} \hspace{1em} a \hspace{1em} (x \# y \# zs) &= x \# a \# \text{sep} \hspace{1em} a \hspace{1em} (y \# zs) \ | \\
\text{sep} \hspace{1em} a \hspace{1em} xs &= xs
\end{align*}
fun ack :: nat ⇒ nat ⇒ nat where
ack 0 n = Suc n |
ack (Suc m) 0 = ack m (Suc 0) |
ack (Suc m) (Suc n) = ack m (ack (Suc m) n)

Terminates because the arguments decrease lexicographically with each recursive call:
- (Suc m, 0) > (m, Suc 0)
- (Suc m, Suc n) > (Suc m, n)
- (Suc m, Suc n) > (m, _)
• A restrictive version of **fun**
• Means *primitive recursive*
• Most functions are primitive recursive
• Frequently found in Isabelle theories

The essence of primitive recursion:

\[
\begin{align*}
  f(0) &= \ldots \quad \text{no recursion} \\
  f(Suc\ n) &= \ldots f(n) \ldots \\
  g([]) &= \ldots \quad \text{no recursion} \\
  g(x\#xs) &= \ldots g(xs) \ldots
\end{align*}
\]
1 Overview of Isabelle/HOL

2 Type and function definitions

3 Induction Heuristics

4 Simplification
Basic induction heuristics

Theorems about recursive functions are proved by induction

Induction on argument number $i$ of $f$
if $f$ is defined by recursion on argument number $i$
A tail recursive reverse

Our initial reverse:

fun rev :: 'a list ⇒ 'a list where
  rev [] = [] |
  rev (x#xs) = rev xs @ [x]

A tail recursive version:

fun itrev :: 'a list ⇒ 'a list ⇒ 'a list where
  itrev [] ys = ys |
  itrev (x#xs) ys =

lemma itrev xs [] = rev xs
Induction_Demo.thy

Generalisation
Generalisation

- Replace constants by variables
- Generalize free variables
  - by *arbitrary* in induction proof
  - (or by universal quantifier in formula)
So far, all proofs were by structural induction because all functions were primitive recursive.

In each induction step, 1 constructor is added. In each recursive call, 1 constructor is removed.

Now: induction for complex recursion patterns.
Computation Induction

Example

```plaintext
fun div2 :: nat ⇒ nat where
  div2 0 = 0       |
  div2 (Suc 0) = 0  |
  div2 (Suc(Suc n)) = Suc(div2 n)
```

〜 induction rule div2.induct:

\[
\begin{align*}
P(0) & \quad P(Suc\ 0) \quad \land \ n. \ P(n) \implies P(Suc(Suc\ n)) \\
\end{align*}
\]

\[P(m)\]
Computation Induction

If \( f :: \tau \Rightarrow \tau' \) is defined by \textbf{fun}, a special induction schema is provided to prove \( P(x) \) for all \( x :: \tau \):

\[
\text{for each defining equation}
\]

\[ f(e) = \ldots f(r_1) \ldots f(r_k) \ldots \]

prove \( P(e) \) assuming \( P(r_1), \ldots, P(r_k) \).

Induction follows course of (terminating!) computation

Motto: properties of \( f \) are best proved by rule \( f.induct \)
How to apply $f.induct$

If $f :: \tau_1 \Rightarrow \cdots \Rightarrow \tau_n \Rightarrow \tau'$:

$\text{(induction } a_1 \ldots a_n \text{ rule: } f.induct)$

Heuristic:

- there should be a call $f a_1 \ldots a_n$ in your goal
- ideally the $a_i$ should be variables.
Induction_Demo.thy

Computation Induction
1. Overview of Isabelle/HOL

2. Type and function definitions

3. Induction Heuristics

4. Simplification
Simplification means . . .

Using equations \( l = r \) from left to right

As long as possible

Terminology: equation \( \rightsquigarrow \) simplification rule

Simplification = (Term) Rewriting
An example

Equations:

\[ 0 + n = n \] (1)

\[ (Suc \ m) + n = Suc \ (m + n) \] (2)

\[ (Suc \ m \leq Suc \ n) = (m \leq n) \] (3)

\[ (0 \leq m) = True \] (4)

Rewriting:

\[ 0 + Suc \ 0 \leq Suc \ 0 + x \] (1) \[ = \]

\[ Suc \ 0 \leq Suc \ 0 + x \] (2) \[ = \]

\[ Suc \ 0 \leq Suc \ (0 + x) \] (3) \[ = \]

\[ 0 \leq 0 + x \] (4) \[ = \]

True
Conditional rewriting

Simplification rules can be conditional:

\[ [ P_1; \ldots; P_k ] \implies l = r \]

is applicable only if all \( P_i \) can be proved first, again by simplification.

Example

\[ p(0) = True \]

\[ p(x) \implies f(x) = g(x) \]

We can simplify \( f(0) \) to \( g(0) \) but we cannot simplify \( f(1) \) because \( p(1) \) is not provable.
Termination

Simplification may not terminate. Isabelle uses simp-rules (almost) blindly from left to right.

Example: \( f(x) = g(x) \), \( g(x) = f(x) \)

\[ [P_1; \ldots; P_k] \implies l = r \]

is suitable as a simp-rule only if \( l \) is “bigger” than \( r \) and each \( P_i \)

\[
\begin{align*}
n < m & \implies (n < Suc m) = True \quad \text{YES} \\
Suc n < m & \implies (n < m) = True \quad \text{NO}
\end{align*}
\]
Proof method *simp*

**Goal:** 1. \([P_1; \ldots; P_m] \Rightarrow C\)

**apply**(*simp add: eq_1 \ldots eq_n*)

Simplify \(P_1 \ldots P_m\) and \(C\) using
- lemmas with attribute *simp*
- rules from *fun* and *datatype*
- additional lemmas *eq_1 \ldots eq_n*
- assumptions \(P_1 \ldots P_m\)

**Variations:**
- \((simp \ldots del: \ldots)\) removes *simp*-lemmas
- *add* and *del* are optional
auto versus simp

- `auto` acts on all subgoals
- `simp` acts only on subgoal 1
- `auto` applies `simp` and more
- `auto` can also be modified:
  
  ```
  (auto simp add: ... simp del: ...) 
  ```
Rewriting with definitions

Definitions (**definition**) must be used **explicitly**:

\[
(simp \ add: \ f\_def \ldots)
\]

\(f\) is the function whose definition is to be unfolded.
Case splitting with $\texttt{simp}$

Automatic:

$$P(\text{if } A \text{ then } s \text{ else } t) = (A \rightarrow P(s)) \land (\neg A \rightarrow P(t))$$

By hand:

$$P(\text{case } e \text{ of } 0 \Rightarrow a \mid \text{Suc } n \Rightarrow b) = (e = 0 \rightarrow P(a)) \land (\forall n. \ e = \text{Suc } n \rightarrow P(b))$$

Proof method: ($\texttt{simp split: nat.split}$)

Or $\texttt{auto}$. Similar for any datatype $t$: $\texttt{t.split}$
Simp_Demo.thy
Chapter 3

Case Study: IMP Expressions
Case Study: IMP Expressions
Case Study: IMP Expressions
This section introduces

*arithmetic and boolean expressions*

of our imperative language IMP.

IMP *commands* are introduced later.
5 Case Study: IMP Expressions

Arithmetic Expressions

Boolean Expressions

Stack Machine and Compilation
Concrete and abstract syntax

Concrete syntax: strings, eg "a+5*b"

Abstract syntax: trees, eg

Parser: function from strings to trees

Linear view of trees: terms, eg $Plus\ a\ (Times\ 5\ b)$

Abstract syntax trees/terms are datatype values!
Concrete syntax is defined by a context-free grammar, e.g.

$$a ::= n \mid x \mid (a) \mid a + a \mid a * a \mid \ldots$$

where $n$ can be any natural number and $x$ any variable.

We focus on abstract syntax which we introduce via datatypes.
Datatype $aexp$

Variable names are strings, values are integers:

**type_synonym** $vname = string$

**datatype** $aexp = N\ int \mid V\ vname \mid Plus\ aexp\ aexp$

<table>
<thead>
<tr>
<th>Concrete</th>
<th>Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>$N\ 5$</td>
</tr>
<tr>
<td>x</td>
<td>$V\ &quot;x&quot;$</td>
</tr>
<tr>
<td>x+y</td>
<td>$Plus\ (V\ &quot;x&quot;)\ (V\ &quot;y&quot;)$</td>
</tr>
<tr>
<td>2+(z+3)</td>
<td>$Plus\ (N\ 2)\ (Plus\ (V\ &quot;z&quot;)\ (N\ 3))$</td>
</tr>
</tbody>
</table>
Warning

This is syntax, not (yet) semantics!

\[ N \ 0 \neq \ Plus \ (N \ 0) \ (N \ 0) \]
The (program) state

What is the value of \( x+1 \)?

- The value of an expression depends on the value of its variables.
- The value of all variables is recorded in the state.
- The state is a function from variable names to values:

```plaintext
type_synonym val = int
type_synonym state = vname ⇒ val
```
Function update notation

If \( f :: \tau_1 \Rightarrow \tau_2 \) and \( a :: \tau_1 \) and \( b :: \tau_2 \) then

\[
f(a := b)
\]

is the function that behaves like \( f \) except that it returns \( b \) for argument \( a \).

\[
f(a := b) = (\lambda x. \text{if } x = a \text{ then } b \text{ else } f \ x)
\]
How to write down a state

Some states:

- \( \lambda x. 0 \)
- \( (\lambda x. 0)("a" := 3) \)
- \( ((\lambda x. 0)("a" := 5))("x" := 3) \)

Nicer notation:

\(<"a" := 5, "x" := 3, "y" := 7>\)

Maps everything to 0, but "a" to 5, "x" to 3, etc.
AExp.thy
5 Case Study: IMP Expressions

Arithmetic Expressions

Boolean Expressions

Stack Machine and Compilation
Case Study: IMP Expressions

Arithmetic Expressions

Boolean Expressions

Stack Machine and Compilation
ASM.thy
This was easy. Because evaluation of expressions always terminates. But execution of programs may *not* terminate. Hence we cannot define it by a total recursive function.

We need more logical machinery to define program execution and reason about it.
Chapter 4

Logic and Proof
Beyond Equality
6 Logical Formulas

7 Proof Automation

8 Single Step Proofs

9 Inductive Definitions
6 Logical Formulas

7 Proof Automation

8 Single Step Proofs

9 Inductive Definitions
Syntax (in decreasing precedence):

\[
\text{form} ::= (\text{form}) \mid \text{term} = \text{term} \mid \neg \text{form} \\
\mid \text{form} \land \text{form} \mid \text{form} \lor \text{form} \mid \text{form} \rightarrow \text{form} \\
\mid \forall x. \text{form} \mid \exists x. \text{form}
\]

Examples:

\[
\neg A \land B \lor C \equiv ((\neg A) \land B) \lor C
\]

\[
s = t \land C \equiv (s = t) \land C
\]

\[
A \land B = B \land A \equiv A \land (B = B) \land A
\]

\[
\forall x. P x \land Q x \equiv \forall x. (P x \land Q x)
\]

Input syntax: \(\leftrightarrow\) (same precedence as \(\rightarrow\))
Variable binding convention:

\[ \forall x \; y. \; P \; x \; y \; \equiv \; \forall x. \; \forall y. \; P \; x \; y \]

Similarly for \( \exists \) and \( \lambda \).
Warning

Quantifiers have low precedence and need to be parenthesized (if in some context)

\[ P \land \forall x. \ Q \ x \ \sim \ P \land (\forall x. \ Q \ x) \]
Mathematical symbols

... and their ascii representations:

\( \forall \) \(<forall>\) ALL
\( \exists \) \(<exists>\) EX
\( \lambda \) \(<\text{lambda}>\) %
\( \rightarrow \) -->
\( \leftrightarrow \) <->
\( \land \) \&
\( \lor \) |
\( \neg \) \(<\text{not}>\) ~
\( \neq \) \(<\text{noteq}>\) ~=
Sets over type 'a

'a set

- \{\}, \{e_1, \ldots, e_n\}
- e \in A, \ A \subseteq B
- A \cup B, \ A \cap B, \ A - B, \ - A
- ...

\[ \in \ \langle \text{in} \rangle \quad : \]
\[ \subseteq \ \langle \text{subseteq}\rangle \quad \leq \]
\[ \cup \ \langle \text{union}\rangle \quad \text{Un} \]
\[ \cap \ \langle \text{inter}\rangle \quad \text{Int} \]
Set comprehension

• \( \{ x. \ P \} \) where \( x \) is a variable
• But not \( \{ t. \ P \} \) where \( t \) is a proper term
• Instead: \( \{ t \mid x \ y \ z. \ P \} \)
  is short for \( \{ v. \ \exists x \ y \ z. \ v = t \land P \} \)
  where \( x, \ y, \ z \) are the free variables in \( t \)
6 Logical Formulas

7 Proof Automation

8 Single Step Proofs

9 Inductive Definitions
simp and auto

simp: rewriting and a bit of arithmetic
auto: rewriting and a bit of arithmetic, logic and sets

- Show you where they got stuck
- highly incomplete
- Extensible with new simp-rules

Exception: auto acts on all subgoals
fastforce

- rewriting, logic, sets, relations and a bit of arithmetic.
- **incomplete** but better than *auto*.
- Succeeds or fails
- Extensible with new *simp*-rules
• A complete proof search procedure for FOL . . .
• . . . but (almost) without “=”
• Covers logic, sets and relations
• Succeeds or fails
• Extensible with new deduction rules
Automating arithmetic

\textit{arith:}

- proves linear formulas (no “$\ast$”)
- complete for quantifier-free \textit{real} arithmetic
- complete for first-order theory of \textit{nat} and \textit{int} (Presburger arithmetic)
Sledgehammer
Architecture:

Goal & filtered library

Isabelle

↓

external ATPs\(^1\)

↑

Proof

Characteristics:

- Sometimes it works,
- sometimes it doesn’t.

Do you feel lucky?

\(^1\)Automatic Theorem Provers
by $(\text{proof-method})$

\approx

\text{apply} (\text{proof-method})

done
Auto_Proof_Demo.thy
6 Logical Formulas

7 Proof Automation

8 Single Step Proofs

9 Inductive Definitions
Step-by-step proofs can be necessary if automation fails and you have to explore where and why it failed by taking the goal apart.
What are these ?-variables?

After you have finished a proof, Isabelle turns all free variables $V$ in the theorem into ?$V$.

Example: theorem conjI: \[ ?P; ?Q \implies ?P \land ?Q \]

These ?-variables can later be instantiated:

- By hand:
  \[ \text{conjI[of "a=b" "False"]} \sim \]
  \[ \[ a = b; False \] \implies a = b \land False \]

- By unification:
  unifying ?$P \land ?Q$ with $a=b \land False$
  sets ?$P$ to $a=b$ and ?$Q$ to False.
Rule application

Example: rule: \[[?P; ?Q]\] \(\implies\) ?P \(\land\) ?Q
subgoal:  1. . . . \(\implies\) A \(\land\) B

Result:  1. . . . \(\implies\) A
        2. . . . \(\implies\) B

The general case: applying rule \[[ A_1; . . . ; A_n \]] \(\implies\) A
to subgoal . . . \(\implies\) C:
- Unify A and C
- Replace C with \(n\) new subgoals \(A_1 . . . A_n\)

apply(rule xyz)

“Backchaining”
Typical backwards rules

\[ \frac{?P \quad ?Q}{?P \land ?Q} \quad \text{conjI} \]

\[ \frac{?P \iff ?Q}{?P \implies ?Q} \quad \text{impI} \]

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

\[ \frac{?P \iff ?Q \quad ?Q \iff ?P}{?P = ?Q} \quad \text{iffI} \]

They are known as **introduction rules** because they *introduce* a particular connective.
Automating intro rules

If $r$ is a theorem $[ A_1; \ldots; A_n ] \Rightarrow A$ then

$(\text{blast intro}: r)$

allows blast to backchain on $r$ during proof search.

Example:

theorem $\text{le_trans} : [ ?x \leq ?y; ?y \leq ?z ] \Rightarrow ?x \leq ?z$

goal 1. $[ a \leq b; b \leq c; c \leq d ] \Rightarrow a \leq d$

proof apply($\text{blast intro}: \text{le_trans}$)

Also works for auto and fastforce

Can greatly increase the search space!
Forward proof: OF

If \( r \) is a theorem \( A \rightarrow B \) and \( s \) is a theorem that unifies with \( A \) then

\[ r[OF s] \]

is the theorem obtained by proving \( A \) with \( s \).

Example: theorem refl: \( ?t = ?t \)

\[
\text{conjI}[OF \text{refl[of "a"))]}
\]

\[ \sim \]

\[ ?Q \rightarrow a = a \land ?Q \]
The general case:

If \( r \) is a theorem \([ A_1; \ldots; A_n \] \( \implies A \) and \( r_1, \ldots, r_m \ (m \leq n) \) are theorems then

\[
r[OF r_1 \ldots r_m]
\]

is the theorem obtained by proving \( A_1 \ldots A_m \) with \( r_1 \ldots r_m \).

Example: theorem refl: \( \exists t = \exists t \)

\[
\text{conjI[OF refl[of "a"] refl[of "b"]]} \\
\sim \sim \\
a = a \land b = b
\]
From now on: ? mostly suppressed on slides
Single_Step_Demo.thy
is part of the Isabelle framework. It structures theorems and proof states: \[ [ A_1; \ldots; A_n ] \Rightarrow A \]

is part of HOL and can occur inside the logical formulas \( A_i \) and \( A \).

Phrase theorems like this \[ [ A_1; \ldots; A_n ] \Rightarrow A \]
not like this \( A_1 \land \ldots \land A_n \Rightarrow A \)
6 Logical Formulas

7 Proof Automation

8 Single Step Proofs

9 Inductive Definitions
Example: even numbers

Informally:

- 0 is even
- If \( n \) is even, so is \( n + 2 \)
- These are the only even numbers

In Isabelle/HOL:

```isabelle
inductive ev :: nat ⇒ bool
where
  ev 0 | ev n ⇒ ev (n + 2)
```
An easy proof:  $ev\ 4$

$ev\ 0 \implies ev\ 2 \implies ev\ 4$
Consider

```haskell
fun evn :: nat ⇒ bool where
evn 0 = True |
evn (Suc 0) = False |
evn (Suc (Suc n)) = evn n
```

A trickier proof:  \( \text{ev } m \implies \text{evn } m \)

By induction on the structure of the derivation of \( \text{ev } m \)

Two cases:  \( \text{ev } m \) is proved by

- rule  \( \text{ev } 0 \)
  \[ \implies m = 0 \implies \text{evn } m = \text{True} \]
- rule  \( \text{ev } n \implies \text{ev } (n+2) \)
  \[ \implies m = n+2 \text{ and } \text{evn } n \text{ (IH)} \]
  \[ \implies \text{evn } m = \text{evn } (n+2) = \text{evn } n = \text{True} \]
Rule induction for $ev$

To prove

$$ev\ n \implies P\ n$$

by *rule induction* on $ev\ n$ we must prove

- $P\ 0$
- $P\ n \implies P(n+2)$

Rule $ev.induct$:

$$
\frac{
  ev\ n \quad P\ 0 \quad \land n. \ [ ev\ n;\ P\ n ] \\
}{P\ n}
\implies P(n+2)
$$
Format of inductive definitions

\[ \text{inductive } I :: \tau \Rightarrow \text{bool} \text{ where} \]
\[ \left[ I \ a_1; \ldots; I \ a_n \right] \Rightarrow I \ a \]

Note:

- \( I \) may have multiple arguments.
- Each rule may also contain \textit{side conditions} not involving \( I \).
Rule induction in general

To prove

\[ I \, x \Rightarrow P \, x \]

by *rule induction* on \( I \, x \)

we must prove for every rule

\[ \left[ I \, a_1; \ldots ; I \, a_n \right] \Rightarrow I \, a \]

that \( P \) is preserved:

\[ \left[ I \, a_1; \, P \, a_1; \ldots ; I \, a_n; \, P \, a_n \right] \Rightarrow P \, a \]
Rule induction is absolutely central to (operational) semantics and the rest of this lecture course.
Inductive_Demo.thy
**Inductively defined sets**

\[
\text{inductive_set } I ::= \tau \text{ set where } \\
\left[ a_1 \in I; \ldots ; a_n \in I \right] \implies a \in I
\]

Difference to \textit{inductive}:
- arguments of \( I \) are tupled, not curried
- \( I \) can later be used with set theoretic operators, eg \( I \cup \ldots \)
Chapter 5

Isar: A Language for Structured Proofs
Isar by example

Proof patterns

Streamlining Proofs

Proof by Cases and Induction
Apply scripts

• unreadable
• hard to maintain
• do not scale

No structure!
Apply scripts versus Isar proofs

Apply script = assembly language program
Isar proof = structured program with assertions

But: **apply** still useful for proof exploration
proof
  assume \( \text{formula}_0 \)
  have \( \text{formula}_1 \) by simp
  :
  have \( \text{formula}_n \) by blast
  show \( \text{formula}_{n+1} \) by \ldots
qed

proves \( \text{formula}_0 \implies \text{formula}_{n+1} \)
Isar core syntax

\[
\text{proof} = \text{proof} \ [\text{method}] \ \text{step}^* \ \text{qed}
\]

\[
\text{by method}
\]

\[
\text{method} = (\text{simp} \ldots) \mid (\text{blast} \ldots) \mid (\text{induction} \ldots) \mid \ldots
\]

\[
\text{step} = \text{fix variables} \ (\wedge)
\]

\[
\mid \ \text{assume } \text{prop} \ (\implies)
\]

\[
\mid \ [\text{from } \text{fact}^+] \ (\text{have } \mid \text{show}) \ \text{prop} \ \text{proof}
\]

\[
\text{prop} = [\text{name:}] \ "\text{formula}"
\]

\[
\text{fact} = \text{name} | \ldots
\]
10 Isar by example

11 Proof patterns

12 Streamlining Proofs

13 Proof by Cases and Induction
Example: Cantor’s theorem

lemma  ¬ surj(f :: 'a ⇒ 'a set)
proof  default proof: assume surj, show False
   assume a: surj f
   from a have b: ∀ A. ∃ a. A = f a
      by (simp add: surj_def)
   from b have c: ∃ a. {x. x ∉ f x} = f a
      by blast
   from c show False
      by blast
qed
Isar_Demo.thy

Cantor and abbreviations
**Abbreviations**

\[\text{this} = \text{the previous proposition proved or assumed}\]
\[\text{then} = \text{from this}\]
\[\text{thus} = \text{then show}\]
\[\text{hence} = \text{then have}\]
using and with

\((\text{have}|\text{show}) \text{ prop using facts} = \) 
\(\text{from facts } (\text{have}|\text{show}) \text{ prop with facts} = \) 
\(\text{from facts this} \)
Structured lemma statement

**Lemma**

**Fixes** \( f :: 'a \Rightarrow 'a \text{ set} \)

**Assumes** \( s : \text{surj } f \)

**Shows** \( \text{False} \)

**Proof** — no automatic proof step

**Have** \( \exists a. \{ x. x \not\in f x \} = f a \) **Using** \( s \)

**By** (auto simp: surj_def)

**Thus** \( \text{False} \) **By** blast

**Qed**

Proves \( \text{surj } f \implies \text{False} \)

but \( \text{surj } f \) becomes local fact \( s \) in proof.
The essence of structured proofs

Assumptions and intermediate facts can be named and referred to explicitly and selectively
Structured lemma statements

- **fixes** $x :: \tau_1$ and $y :: \tau_2$ ...
- **assumes** $a: P$ and $b: Q$ ...
- **shows** $R$

- **fixes** and **assumes** sections optional
- **shows** optional if no **fixes** and **assumes**
Isar by example

Proof patterns

Streamlining Proofs

Proof by Cases and Induction
Case distinction

show $R$
proof cases
  assume $P$
  :$
  show \ K \ \ldots$
next
  assume $\neg P$
  :$
  show \ R \ \ldots$
qed

have $P \lor Q \ \ldots$
then show $R$
proof
  assume $P$
  :$
  show \ R \ \ldots$
next
  assume $Q$
  :$
  show \ R \ \ldots$
qed
Contradiction

show \( \neg P \)
proof
  assume \( P \)
  :
  show \( False \) . . .
qed

show \( P \)
proof \((rule\ ccontr)\)
  assume \( \neg P \)
  :
  show \( False \) . . .
qed
show $P \iff Q$

proof

assume $P$

: 

show $Q$ \ldots

next

assume $Q$

: 

: 

show $P$ \ldots

qed
\( \forall \) and \( \exists \) introduction

show \( \forall x. \ P(x) \)
proof
  fix \( x \) local fixed variable
  show \( P(x) \) ...
qed

show \( \exists x. \ P(x) \)
proof
  show \( P(\text{witness}) \) ...
qed
\exists \text{ elimination: obtain }

have \ \exists x. \ P(x) \\
then \textbf{obtain} \ x \text{ where } p: \ P(x) \text{ by blast} \\
: \ x \text{ fixed local variable}

Works for one or more \ x
lemma ¬ surj(f :: 'a ⇒ 'a set)
proof
  assume surj f
  hence ∃ a. {x. x ∉ f x} = f a by (auto simp: surj_def)
  then obtain a where {x. x ∉ f x} = f a by blast
  hence a ∉ f a ←→ a ∈ f a by blast
  thus False by blast
qed
Set equality and subset

show \( A = B \)
proof
  show \( A \subseteq B \) . . .
next
  show \( B \subseteq A \) . . .
qed

show \( A \subseteq B \)
proof
  fix \( x \)
  assume \( x \in A \)
  :
  show \( x \in B \) . . .
qed
Isar_Demo.thy

Exercise
10 Isar by example

11 Proof patterns

12 Streamlining Proofs

13 Proof by Cases and Induction
Streamlining Proofs

Pattern Matching and Quotations

Top down proof development

moreover

Raw proof blocks
Example: pattern matching

\[
\text{show } \quad formula_1 \longleftrightarrow formula_2 \quad (\text{is } \ ?L \longleftrightarrow \ ?R) \\
\text{proof} \\
\quad \text{assume } \ ?L \\
\quad : \\
\quad \text{show } \ ?R \ \ldots \\
\text{next} \\
\quad \text{assume } \ ?R \\
\quad : \\
\quad \text{show } \ ?L \ \ldots \\
\text{qed}
\]
show $\text{formula } (is \ ?\text{thesis})$
proof -
  
  show $?\text{thesis} \ldots$
qed

Every show implicitly defines $?\text{thesis}$
Introducing local abbreviations in proofs:

```simply-typed
let ?t = "some-big-term"
:
have "... ?t ..."
```
Quoting facts by value

By name:

```agda
have x0: "x > 0" ...
:
from x0 ...
```

By value:

```agda
have "x > 0" ...
:
from 'x>0' ...
```

↑ ↑

back quotes
Isar-demo.thy

Pattern matching and quotations
Streamlining Proofs

Pattern Matching and Quotations

Top down proof development

moreover

Raw proof blocks
Example

**Lemma**

\[(\exists \ ys \ zs. \ xs = ys \ @ \ zs \land length \ ys = length \ zs) \lor (\exists \ ys \ zs. \ xs = ys \ @ \ zs \land length \ ys = length \ zs + 1)\]

**Proof**

???
Isar_Demo.thy

Top down proof development
When automation fails

Split proof up into smaller steps.

Or explore by `apply`:

- `have ... using ...`
- `apply -` to make incoming facts part of proof state
- `apply auto` or whatever
- `apply ...`

At the end:

- `done`
- Better: *convert to structured proof*
Streamlining Proofs

Pattern Matching and Quotations
Top down proof development

moreover

Raw proof blocks
moreover—ultimately

have $P_1$ . . .
moreover
have $P_2$ . . .
moreover
:  
moreover
have $P_n$ . . .
ultimately
have $P$ . . .

have $\text{lab}_1$: $P_1$ . . .
have $\text{lab}_2$: $P_2$ . . .
:  
have $\text{lab}_n$: $P_n$ . . .
from $\text{lab}_1$ $\text{lab}_2$ . . .
have $P$ . . .

\[ \approx \]

With names
12 Streamlining Proofs

Pattern Matching and Quotations

Top down proof development

moreover

Raw proof blocks
{ \textbf{fix} \; x_1 \ldots x_n \\
\textbf{assume} \; A_1 \ldots A_m \\
\vdots \\
\textbf{have} \; B 
}\ \\
\text{proves} \; [ \; A_1; \ldots ; A_m \; ] \implies B \\
\text{where all } x_i \text{ have been replaced by } \pi x_i.
Isar_Demo.thy

moreover and {  }
Proof state and Isar text

In general: \textbf{proof method}

Applies \textit{method} and generates subgoal(s):

\[
\forall x_1 \ldots x_n [ A_1; \ldots ; A_m ] \implies B
\]

How to prove each subgoal:

\textbf{fix} \ x_1 \ldots x_n
\textbf{assume} \ A_1 \ldots A_m
\textbf{show} \ B

Separated by \textbf{next}
10 Isar by example

11 Proof patterns

12 Streamlining Proofs

13 Proof by Cases and Induction
Isar_Induction_Demo.thy

Proof by cases
Datatype case analysis

\textbf{datatype} \quad t \; = \; C_1 \; \vec{\tau} \; \mid \; \ldots

\begin{proof}
\begin{cases}
\text{case} \ (C_1 \ x_1 \ \ldots \ x_k) \\
\ldots \ x_j \ \ldots
\end{cases}
\end{proof}

next

\vdots

\textbf{qed}

where

\begin{align*}
\text{case} \ (C_i \ x_1 \ \ldots \ x_k) & \equiv \\
\text{fix} \ x_1 \ \ldots \ x_k & \\
\text{assume} \ C_i: \ & \underbrace{\text{term} = (C_i \ x_1 \ \ldots \ x_k)}_{\text{formula}}
\end{align*}
Isar_Induction_Demo.thy

Structural induction for $\textit{nat}$
Structural induction for \textit{nat}

\begin{verbatim}
show \(P(n)\)
proof \(\text{(induction } n)\)
  case 0
  \vdots
  show \(?case\)
next
  case \(\text{Suc } n\)
  \vdots
  \vdots
  show \(?case\)
qed
\end{verbatim}

\begin{verbatim}
\equiv \quad \text{let } ?case = P(0)
\equiv \quad \text{fix } n \text{ assume } \text{Suc: } P(n)
\quad \text{let } ?case = P(\text{Suc } n)
\end{verbatim}
Structural induction with $\Rightarrow$

show $A(n) \Rightarrow P(n)$

proof (induction $n$)

  case 0
  :
  show $?case$

next

  case (Suc $n$)
  :
  :
  show $?case$

qed
Named assumptions

In a proof of

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

by structural induction:
In the context of

\textbf{case} \( C \)

we have

\( C.IH \) the induction hypotheses

\( C.prems \) the premises \( A_i \)

\( C \quad C.IH + C.prems \)
A remark on style

- **case** $(\text{Suc } n)$ \ldots **show** \texttt{?case}
  is easy to write and maintain

- **fix** $n$ **assume** \texttt{formula} \ldots **show** \texttt{formula'}
  is easier to read:
  - all information is shown locally
  - no contextual references (e.g. \texttt{?case})
Proof by Cases and Induction

Rule Induction

Rule Inversion
Isar_Induction_Demo.thy

Rule induction
Rule induction

\textbf{inductive} \( I :: \tau \Rightarrow \sigma \Rightarrow \text{bool} \)
\textbf{where}
\begin{align*}
\text{rule}_1 & : \ldots \\
\vdots & \\
\text{rule}_n & : \ldots
\end{align*}

\textbf{show} \( I \ x \ y \Rightarrow P \ x \ y \)
\textbf{proof} \ (\text{induction rule: } I.\text{induct})
\begin{align*}
\text{case} & \text{ rule}_1 \\
\vdots & \\
\text{show} & \ ?\text{case} \\
\text{next} & \\
\vdots & \\
\text{next} & \\
\text{case} & \text{ rule}_n \\
\vdots & \\
\text{show} & \ ?\text{case} \\
\text{qed}
\end{align*}
Fixing your own variable names

\textbf{case } \langle rule_i \; x_1 \; \ldots \; x_k \rangle

Renames the first $k$ variables in $rule_i$ (from left to right) to $x_1 \; \ldots \; x_k$. 
Named assumptions

In a proof of

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

by rule induction on \( I \ldots \):

In the context of

\textbf{case} \( R \)

we have

\( R.\text{IH} \) the induction hypotheses

\( R.\text{hyps} \) the assumptions of rule \( R \)

\( R.\text{prems} \) the premises \( A_i \)

\( R \) \( R.\text{IH} + R.\text{hyps} + R.\text{prems} \)
Proof by Cases and Induction

Rule Induction

Rule Inversion
Rule inversion

\textbf{inductive} \textit{ev} :: \textit{nat} \Rightarrow \textit{bool} \textbf{ where}

\textit{ev0}: \quad \textit{ev} \ 0 \mid

\textit{evSS}: \quad \textit{ev} \ n \quad \Rightarrow \quad \textit{ev}(\textit{Suc}(\textit{Suc} \ n))

What can we deduce from \textit{ev} \ n? 
That it was proved by either \textit{ev0} or \textit{evSS}!

\textit{ev} \ n \quad \Rightarrow \quad n = 0 \lor (\exists \ k. \ n = \textit{Suc}(\textit{Suc} \ k) \land \textit{ev} \ k)

\textbf{Rule inversion} = \textbf{case distinction over rules}
Isar_Induction_Demo.thy

Rule inversion
Rule inversion template

from ‘ev n‘ have P
proof cases
  case ev0
  : show thesis ...
next
  case (evSS k)
  : show thesis ...
qed

Impossible cases disappear automatically