Concrete Semantics
with Isabelle/HOL

Tobias Nipkow

Fakultät für Informatik
Technische Universität München

2019-10-14
Chapter 1

Introduction
1 Background

2 This Course
1 Background

2 This Course
Why Semantics?

Without semantics, we do not really know what our programs mean. We merely have a good intuition and a warm feeling. Like the state of mathematics in the 19th century — before set theory and logic entered the scene.
Intuition is important!

• You need a good intuition to get your work done efficiently.
• To understand the average accounting program, intuition suffices.
• To write a bug-free accounting program may require more than intuition!
• I assume you have the necessary intuition.
• This course is about “beyond intuition”.

Intuition is not sufficient!

Writing **correct** language processors (e.g. compilers, refactoring tools, ...) requires

- a deep understanding of language semantics,
- the ability to *reason* (= perform proofs) about the language and your processor.

**Example:**
What does the correctness of a type checker even mean? How is it proved?
Why Semantics??

We have a compiler — that is the ultimate semantics!!

- A compiler gives each individual program a semantics.
- It does not help with reasoning about the PL or individual programs.
- Because compilers are far too complicated.
- They provide the worst possible semantics.
- Moreover: compilers may differ!
The sad facts of life

- Most languages have one or more compilers.
- Most compilers have bugs.
- Few languages have a (separate, abstract) semantics.
- If they do, it will be informal (English).
Bugs

- Google “compiler bug”
- Google “hostile applet”
  Early versions of Java had various security holes. Some of them had to do with an incorrect bytecode verifier.

GI Dissertationspreis 2003:
Gerwin Klein: *Verified Java Bytecode Verification*
Standard ML (SML)

First real language with a mathematical semantics:
Milner, Tofte, Harper:
The Definition of Standard ML. 1990.

Robin Milner (1934–2010)
Turing Award 1991.

Main achievements:  LCF (theorem proving)
                   SML (functional programming)
                   CCS, pi (concurrency)
The sad fact of life

SML semantics hardly used:

- too difficult to read to answer simple questions quickly
- too much detail to allow reliable informal proof
- not processable beyond \LaTeX, not even executable
More sad facts of life

• Real programming languages are complex.
• Even if designed by academics, not industry.
• Complex designs are error-prone.
• Informal mathematical proofs of complex designs are also error-prone.
The solution

Machine-checked language semantics and proofs

• Semantics at least type-correct
• Maybe executable
• Proofs machine-checked

The tool:

Proof Assistant (PA)

or

Interactive Theorem Prover (ITP)
Proof Assistants

- You give the structure of the proof
- The PA checks the correctness of each step
- Can prove hard and huge theorems

Government health warnings:

Time consuming
Potentially addictive
Undermines your naive trust in informal proofs
This lecture course:

\[
\text{Formal} = \text{machine-checked} \\
\text{Verification} = \text{formal correctness proof}
\]

Traditionally:

\[
\text{Formal} = \text{mathematical}
\]
Two landmark verifications

C compiler
Competitive with gcc -01

Xavier Leroy
INRIA Paris
using Coq

Operating system microkernel (L4)

Gerwin Klein (& Co)
NICTA Sydney
using Isabelle
A happy fact of life

Programming language researchers are increasingly using PAs
Why verification pays off

Short term: *The software works!*

Long term:

Tracking effects of changes by rerunning proofs

Incremental changes of the software typically require only incremental changes of the proofs

Long term much more important than short term:

*Software Never Dies*
1 Background

2 This Course
What this course is *not* about

- Hot or trendy PLs
- Comparison of PLs or PL paradigms
- Compilers (although they will be one application)
What this course *is* about

- Techniques for the description and analysis of
  - PLs
  - PL tools
  - Programs
- Description techniques: *operational semantics*
- Proof techniques: *inductions*

 Both informally and formally (PA!)
Our PA: Isabelle/HOL

- Started 1986 by Paulson (U of Cambridge)
- Later development mainly by Nipkow & Co (TUM) and Wenzel
- The logic HOL is ordinary mathematics

Learning to use Isabelle/HOL is an integral part of the course

All exercises require the use of Isabelle/HOL
Why I am so passionate about the PA part

- It is the future
- It is the only way to deal with complex languages reliably
- I want students to learn how to write correct proofs
- I have seen too many proofs that look more like LSD trips than coherent mathematical arguments
Overview of course

- Introduction to Isabelle/HOL
- IMP (assignment and while loops) and its semantics
- A compiler for IMP
- Hoare logic for IMP
- Type systems for IMP
- Program analysis for IMP
The semantics part of the course is mostly traditional.
The use of a PA is leading edge.
A growing number of universities offer related course.
What you learn in this course goes far beyond PLs

It has applications in compilers, security, software engineering etc.

It is a new approach to informatics
Part I

Isabelle
Chapter 2

Programming and Proving
Overview of Isabelle/HOL

Type and function definitions

Induction Heuristics

Simplification
Notation

Implication associates to the right:

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

Similarly for other arrows: $\Rightarrow$, $\implies$

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

4 Type and function definitions

5 Induction Heuristics

6 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 \textit{bool}, \textit{nat} and \textit{list}

Summary
Types

Basic syntax:

\[ \tau ::= (\tau) \mid \text{base types} \mid \text{type variables} \mid \text{functions} \mid \text{pairs (ascii: *)} \mid \text{lists} \mid \text{sets} \mid \text{user-defined types} \]

\[ \text{Convention: } \tau_1 \Rightarrow \tau_2 \Rightarrow \tau_3 \equiv \tau_1 \Rightarrow (\tau_2 \Rightarrow \tau_3) \]
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:

\[ t ::= (t) \]
\[ \text{constant or variable (identifier)} \]
\[ t \hspace{1em} t \hspace{1em} \text{function application} \]
\[ \lambda x. \hspace{1em} t \hspace{1em} \text{function abstraction} \]
\[ \ldots \hspace{1em} \text{lots of syntactic sugar} \]

Examples:

\[ f \hspace{1em} (g \hspace{1em} x) \hspace{1em} y \]
\[ h \hspace{1em} (\lambda x. \hspace{1em} f \hspace{1em} (g \hspace{1em} x)) \]

Convention:

\[ f \hspace{1em} t_1 \hspace{1em} t_2 \hspace{1em} t_3 \equiv ((f \hspace{1em} t_1) \hspace{1em} t_2) \hspace{1em} t_3 \]

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 $\beta$-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*

\[ f \ a_1 \text{ where } a_1 :: \tau_1 \]
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 bool, nat and list

Summary
isabelle jedit

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

Types and terms

Interface

By example: types bool, nat and list

Summary
Type \textit{bool}

datatype \texttt{bool} = \texttt{True} \mid \texttt{False}

Predefined functions:
\&, \lor, \rightarrow, \ldots :: \texttt{bool} \Rightarrow \texttt{bool} \Rightarrow \texttt{bool}

A \textit{formula} is a term of type \textit{bool}

if-and-only-if: =
Type \textit{nat}

\textbf{datatype} \ \textit{nat} = 0 \mid \textit{Suc \ nat}

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

Predefined functions: $+, \ *, \ldots :: \textit{nat} \Rightarrow \textit{nat} \Rightarrow \textit{nat}$

\textbf{!} Numbers and arithmetic operations are overloaded:

0,1,2,... :: 'a, \quad + :: 'a \Rightarrow 'a \Rightarrow 'a

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

unless the context is unambiguous: \textit{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:
  \[
  \text{add } (\text{Suc } m) 0 = \text{Suc } (\text{add } m 0) \quad \text{by def. of add}
  \]
  \[
  = \text{Suc } m \quad \text{by IH}
  \]
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 $P(x#xs)$.

$$
\begin{align*}
P([]) & \land \forall x \in xs. \ P(xs) \implies P(x#xs) \\
\implies P(xs) \\
P(xs)
\end{align*}
$$
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 \( \text{Nil} \): \( \text{app} (\text{app} \; \text{Nil} \; ys) \; zs = \text{app} \; ys \; zs = \text{app} \; \text{Nil} \; (\text{app} \; ys \; zs) \) holds by definition of \( \text{app} \).

- Case \( \text{Cons} \; x \; xs \): 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:

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

Included in Main.

Don’t reinvent, reuse!

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

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

If the lemma is suitable as a simplification rule:
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. $\bigwedge x_1 \ldots x_p. \ A \implies B$

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

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

abbreviates

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

; \approx \text{“and”}
Overview of Isabelle/HOL

Type and function definitions

Induction Heuristics

Simplification
4 Type and function definitions

Type definitions

Function definitions
Type synonyms

\texttt{type\_synonym \ name = \ \tau}

Introduces a \textit{synonym \ name} for type \(\tau\)

Examples

\texttt{type\_synonym \ string = \ char \ list}

\texttt{type\_synonym \ ('a,'b)\ foo = \ 'a \ list \ \times \ \ 'b \ list}

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

\[
datatype \ \ (\alpha_1, \ldots, \alpha_n) t \quad = \quad C_1 \ \ \tau_{1,1} \ldots \tau_{1,n_1} \\
| \quad \ldots \\
| \quad C_k \ \ \tau_{k,1} \ldots \tau_{k,n_k}
\]

- **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:** 
  \[
  \begin{align*}
  (C_i \ x_1 \ldots x_{n_i} = C_i \ y_1 \ldots y_{n_i}) &= \\
  (x_1 = y_1 \land \cdots \land x_{n_i} = y_{n_i})
  \end{align*}
  \]

Distinctness and injectivity are applied automatically

Induction must be applied explicitly
Case expressions

Datatype values can be taken apart with `case`:

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

Wildcards: `_`

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

Nested patterns:

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

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, ...`
then `'a option` has values `None, Some a_1, Some a_2, ...`

Typical application:

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

lookup [] x = None |
lookup ((a, b) # ps) x =
  (if a = x then Some b else lookup ps x)
4 Type and function definitions
   Type definitions
   Function definitions
Non-recursive definitions

Example

**definition** $sq :: nat \Rightarrow nat$ where $sq \ n \ = \ n\ast n$

No pattern matching, just $f \ x_1 \ldots \ x_n \ = \ \ldots$
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

fun sep :: 'a ⇒ 'a list ⇒ 'a list where
sep a (x#y#zs) = x # a # sep a (y#zs) |
sep a xs = xs
Example: Ackermann

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 \textit{lexicographically} with each recursive call:

\begin{itemize}
  \item (Suc m, 0) > (m, Suc 0)
  \item (Suc m, Suc n) > (Suc m, n)
  \item (Suc m, Suc n) > (m, _) \end{itemize}
• A restrictive version of \texttt{fun}
• Means \textit{primitive recursive}
• Most functions are primitive recursive
• Frequently found in Isabelle theories

The essence of primitive recursion:

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

4 Type and function definitions

5 Induction Heuristics

6 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:

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

A tail recursive version:

```factorial
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

\[
\textbf{fun} \quad \text{div2} :: \text{nat} \Rightarrow \text{nat} \ \textbf{where} \\
\text{div2} \ 0 = 0 \quad | \\
\text{div2} \ (\text{Suc} \ 0) = 0 \quad | \\
\text{div2} \ (\text{Suc}(\text{Suc} \ n)) = \text{Suc}(\text{div2} \ n)
\]

\[\Rightarrow \text{induction rule div2.induct:}\]

\[
\frac{P(0) \quad P(\text{Suc} \ 0) \quad \land \ n. \ P(n) \implies P(\text{Suc}(\text{Suc} \ n))}{P(m)}
\]
Computation Induction

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

\begin{itemize}
  \item \textit{for each defining equation}
  \end{itemize}

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

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 \textit{f.induct}
How to apply \texttt{f.induct}

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

\[ (induction \ a_1 \ldots \ a_n \ rule: \ f.induct) \]

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
3 Overview of Isabelle/HOL

4 Type and function definitions

5 Induction Heuristics

6 Simplification
Simplification means . . .

Using equations $l = r$ from left to right
As long as possible

Terminology: equation $\leadsto$ simplification rule

Simplification $= (\text{Term})$ Rewriting
An example

Equations:

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

\[ (\text{Suc } m) + n = \text{Suc } (m + n) \quad (2) \]

\[ (\text{Suc } m \leq \text{Suc } n) = (m \leq n) \quad (3) \]

\[ (0 \leq m) = \text{True} \quad (4) \]

Rewriting:

\[ 0 + \text{Suc } 0 \leq \text{Suc } 0 + x \quad \overset{(1)}{=} \]

\[ \text{Suc } 0 \leq \text{Suc } 0 + x \quad \overset{(2)}{=} \]

\[ \text{Suc } 0 \leq \text{Suc } (0 + x) \quad \overset{(3)}{=} \]

\[ 0 \leq 0 + x \quad \overset{(4)}{=} \]

\[ \text{True} \]
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

\[
p(0) = \text{True}
\]
\[
p(x) \implies f(x) = g(x)
\]

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

Principle:

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

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

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

Goal: 1. $[P_1; \ldots; P_m] \implies C$

\textbf{apply}(simp add: eq_1 \ldots eq_n)

Simplify $P_1 \ldots P_m$ and $C$ using
- lemmas with attribute \textit{simp}
- rules from \textbf{fun} and \textbf{datatype}
- additional lemmas $eq_1 \ldots eq_n$
- assumptions $P_1 \ldots P_m$

Variations:
- $(simp \ldots del: \ldots)$ removes \textit{simp}-lemmas
- \textit{add} and \textit{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:
  \[(auto simp add: \ldots \ simp del: \ldots)\]
Rewriting with definitions

Definitions (definition) must be used explicitly:

\[(\text{simp add: } f\_\text{def} \ldots)\]

\(f\) is the function whose definition is to be unfolded.
Case splitting with \textit{simp/auto}

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: \textit{(simp split: nat.split)}

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

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

\textit{arithmetic and boolean expressions}

of our imperative language IMP.

IMP \textit{commands} are introduced later.
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

```
  +
 / \
\a/ /\b
 \/ 5/
```

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, eg

\[ a ::= n \mid x \mid (a) \mid a + a \mid a \ast a \mid \ldots \]

where \( n \) can be any natural number and \( x \) any variable.

We focus on abstract syntax which we introduce via datatypes.
Datatype \textit{aexp}

Variable names are strings, values are integers:

\begin{itemize}
  \item \textbf{type\_synonym} \textit{vname} = \textit{string}
  \item \textbf{datatype} \textit{aexp} = \textit{N int} \mid \textit{V vname} \mid \textit{Plus aexp aexp}
\end{itemize}

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

This is syntax, not (yet) semantics!

\[ N \ 0 \ \neq \ \text{Plus} \ (N \ 0) \ (N \ 0) \]
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 \textit{state}.
- The state is a function from variable names to values:

\begin{verbatim}
  type_synonym  val = int
  type_synonym  state = vname \Rightarrow val
\end{verbatim}
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
Case Study: IMP Expressions

Arithmetic Expressions

Boolean Expressions

Stack Machine and Compilation
BExp.thy
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.
8 Logical Formulas

9 Proof Automation

10 Single Step Proofs

11 Inductive Definitions
8 Logical Formulas

9 Proof Automation

10 Single Step Proofs

11 Inductive Definitions
Syntax (in decreasing precedence):

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

Examples:

\[
\begin{align*}
\neg A \land B \lor C & \equiv ((\neg A) \land B) \lor C \\
 s = t \land C & \equiv (s = t) \land C \\
 A \land B = B \land A & \equiv A \land (B = B) \land A \\
 \forall x. P x \land Q x & \equiv \forall x. (P x \land Q x)
\end{align*}
\]

Input syntax: \(\longleftrightarrow\) (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 \( \lambda \).
Quantifiers have low precedence and need to be parenthesized (if in some context)

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

... and their ascii representations:

∀ \texttt{\textbackslash {forall}} \quad \text{ALL}

∃ \texttt{\textbackslash {exists}} \quad \text{EX}

\lambda \quad \texttt{\textbackslash {lambda}} \quad \% 

\rightarrow \quad \text{-->}

\leftrightarrow \quad \text{<->}

\wedge \quad \texttt{\textbackslash {and}} \quad &

\vee \quad \texttt{\textbackslash {or}} \quad |

\neg \quad \texttt{\textbackslash {not}} \quad \sim

\neq \quad \texttt{\textbackslash {noteq}} \quad \sim=$
Sets over type `'a`

'a set

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

\(\in \, \text{'in'}\)
\(\subseteq \, \text{'subseteq'}\)
\(\cup \, \text{'union'}\)
\(\cap \, \text{'inter'}\)
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 \(t\)
8 Logical Formulas

9 Proof Automation

10 Single Step Proofs

11 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
• rewriting, logic, sets, relations and a bit of arithmetic.
• incomplete but better than auto.
• Succeeds or fails
• Extensible with new simp-rules
blast

- 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

\texttt{arith}:

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

Isabelle

Goal & filtered library

↓

Proof

eexternal ATPs

Characteristics:

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

Do you feel lucky?

\(^1\)Automatic Theorem Provers
by (proof-method)

≈

apply (proof-method)
done
Auto_Proof_Demo.thy
8 Logical Formulas
9 Proof Automation
10 Single Step Proofs
11 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`: \[
\begin{align*}
\begin{array}{ll}
\{ ?P; ?Q \} \\ 
\end{array} & \implies ?P \land ?Q
\end{align*}
\]

These ?-variables can later be instantiated:

- By hand:
  \[
  \text{conjI[of "a=b" "False"] } \rightsquigarrow \begin{array}{ll}
  \{ a = b; False \} \\ 
  \end{array} \implies a = b \land False
  \]

- 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. \ldots \implies A \land B

Result:  1. \ldots \implies A
        2. \ldots \implies B

The general case: applying rule \([ A_1; \ldots ; A_n ] \) \implies A to subgoal \ldots \implies C:

• Unify \( A \) and \( C \)
• Replace \( C \) with \( n \) new subgoals \( A_1 \ldots A_n \)

\texttt{apply}(\textit{rule xyz})

“Backchaining”
Typical backwards rules

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

\[ \frac{P \iff Q}{\neg P \iff \neg Q} \quad \text{implI} \]

\[ \frac{\text{\neg} x. \开采 P x}{\开采 x. \开采 P x} \quad \text{allI} \]

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

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

Also works for $\text{auto}$ and $\text{fastforce}$

Can greatly increase the search space!
Forward proof: OF

If $r$ is a theorem $A \implies B$ and $s$ is a theorem that unifies with $A$ then

$$r[\text{OF } s]$$

is the theorem obtained by proving $A$ with $s$.

Example: theorem refl: $\forall t \equiv \forall t$

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

$$\implies$$

$$\forall Q \implies a = a \land \forall Q$$
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 \texttt{refl}: \(?t = ?t\)

\[
\texttt{conjI[OF refl[of "a"] refl[of "b"]]} \\
\implies \\
a = a \land b = b
\]
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 \( A_1 \land \ldots \land A_n \rightarrow A \)
8 Logical Formulas

9 Proof Automation

10 Single Step Proofs

11 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

**fun evn :: nat ⇒ bool where**

\[ evn 0 = True \]
\[ evn (Suc 0) = False \]
\[ evn (Suc (Suc n)) = evn n \]

A trickier proof: \( ev m \implies evn m \)

By induction on the *structure* of the derivation of \( ev m \)

Two cases: \( ev m \) is proved by

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

To prove

$\text{ev } n \implies P \ n$

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

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

Rule $\text{ev.induct}$:

$$
\begin{array}{c}
\text{ev } n & P \ 0 & \wedge n. \ [ \text{ev } n; \ P \ n ] \implies P(n+2) \\
\hline
P \ n
\end{array}
$$
Format of inductive definitions

\textbf{inductive} \ \mathit{I} :: \ \tau \ \Rightarrow \ \text{bool} \ \text{where} \\
\left[ \mathit{I} \ \mathit{a}_1; \ \ldots; \ \mathit{I}\ a_n \ \right] \ \Rightarrow \ \mathit{I} \ \mathit{a}

\textbf{Note:}

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

To prove

\[ I \ x \ \implies \ P \ x \]

by rule induction on \( I \ x \)
we must prove for every rule

\[ \left[ I \ a_1; \ldots ; I \ a_n \right] \implies I \ a \]

that \( P \) is preserved:

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

\begin{verbatim}
inductive_set I :: \tau set where
  [ a_1 \in I; \ldots ; a_n \in I ] \Rightarrow a \in I
\end{verbatim}

Difference to \textbf{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
12 Isar by example

13 Proof patterns

14 Streamlining Proofs

15 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
A typical Isar proof

proof

  assume $formula_0$
  have $formula_1$ by simp
  
  
  have $formula_n$ by blast
  show $formula_{n+1}$ by \ldots

qed

proves $formula_0 \implies formula_{n+1}$
Isar core syntax

proof = proof [method] step* qed
| by method

method = (simp ...) | (blast ...) | (induction ...) | ...

step = fix variables (\land)
| assume prop (\equiv)
| [from fact^+] (have | show) prop proof

prop = [name:] "formula"

fact = name | ...
12 Isar by example

13 Proof patterns

14 Streamlining Proofs

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

lemma \( \neg \text{surj}(f :: 'a \Rightarrow 'a \ set) \)

proof  default proof: assume surj, show False

assume \( a: \text{surj } f \)

from \( a \) have \( b: \forall A. \exists a. A = f a \)
by (simp add: surj_def)

from \( b \) have \( c: \exists a. \{x. x \notin f x\} = f a \)
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

\[(\text{have} | \text{show}) \text{ prop using facts} = \text{from facts (have} | \text{show}) \text{ prop with facts} = \text{from facts this}\]
 lemma
  fixes $f :: 'a \Rightarrow 'a \text{ set}$
  assumes $s: \text{surj \, f}$
  shows $\text{False}$

proof — no automatic proof step
  have $\exists \, a. \, \{x. \, x \notin f \, x\} = f \, a$ using $s$
     by (auto simp: \text{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 $b: Q$ . . .
s 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 \( R \) \( \langle \text{proof} \rangle \)
next
   assume \( \neg P \)
    :
    show \( R \) \( \langle \text{proof} \rangle \)
qed

have \( P \lor Q \) \( \langle \text{proof} \rangle \)
then show \( R \)
proof
   assume \( P \)
    :
    show \( R \) \( \langle \text{proof} \rangle \)
next
   assume \( Q \)
    :
    show \( R \) \( \langle \text{proof} \rangle \)
qed
Contradiction

\textbf{show } \neg P

\textbf{proof}

\textbf{assume } P

\textbf{:}

\textbf{show } False \langle \text{proof} \rangle

\textbf{qed}

\textbf{show } P

\textbf{proof } (\textit{rule ccontr})

\textbf{assume } \neg P

\textbf{:}

\textbf{show } False \langle \text{proof} \rangle

\textbf{qed}
show $P \iff Q$

proof
  assume $P$
  :  
  show $Q \langle proof \rangle$

next
  assume $Q$
  :  
  :  
  show $P \langle proof \rangle$

qed
∀ and ∃ introduction

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

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

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

Works for one or more x
lemma \neg \text{surj}(f :: 'a \Rightarrow 'a \text{ set})

proof
  assume \text{surj } f
  hence \exists a. \{x. x \notin f\ x\} = f\ a \text{ by} (\text{auto simp: surj_def})
  then obtain a where \{x. x \notin f\ x\} = f\ a \text{ by blast}
  hence a \notin f\ a \iff a \in f\ a \text{ by blast}
  thus False \text{ by blast}

qed
Set equality and subset

\[
\begin{align*}
\text{show } & \quad A = B \\
\text{proof } & \\
\text{show } & \quad A \subseteq B \quad \langle \text{proof} \rangle \\
\text{next } & \\
\text{show } & \quad B \subseteq A \quad \langle \text{proof} \rangle \\
\text{qed} & \\
\text{show } & \quad A \subseteq B \\
\text{proof } & \\
\text{fix } & \quad x \\
\text{assume } & \quad x \in A \\
\therefore & \\
\text{show } & \quad x \in B \quad \langle \text{proof} \rangle \\
\text{qed} &
\end{align*}
\]
Isar_Demo.thy

Exercise
12 Isar by example

13 Proof patterns

14 Streamlining Proofs

15 Proof by Cases and Induction
Streamlining Proofs

Pattern Matching and Quotations

Top down proof development

moreover

Local lemmas
Example: pattern matching

\[
\text{show } formula_1 \leftrightarrow formula_2 \quad (\text{is } ?L \leftrightarrow ?R)
\]
proof
  \begin{align*}
  & \text{assume } ?L \\
  & \vdash \\
  & \text{show } ?R \langle \text{proof} \rangle \\
\end{align*}
next
  \begin{align*}
  & \text{assume } ?R \\
  & \vdash \\
  & \text{show } ?L \langle \text{proof} \rangle \\
\end{align*}
qed
show \textit{formula} \ (\textit{is} \ ?\textit{thesis})

proof -

::

  show ?thesis ⟨proof⟩

qed

\textbf{Every show implicitly defines} ?\textit{thesis}
Introducing local abbreviations in proofs:

let ?t = "some-big-term"

have "\ldots ?t \ldots "
Quoting facts by value

By name:

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

By value:

```
have "x > 0" 
:
from 'x>0' 
```
Isar_Demo.thy

Pattern matching and quotations
Streamlining Proofs

Pattern Matching and Quotations

Top down proof development

moreover

Local lemmas
Example

lemma

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

proof ???
Isar_Demo.thy

Top down proof development
When automation fails

Split proof up into smaller steps.

Or explore by apply:

have \ldots using \ldots
apply - to make incoming facts part of proof state
appl{\em auto} or whatever
apply \ldots

At the end:

- done
- Better: convert to structured proof
Streamlining Proofs

Pattern Matching and Quotations

Top down proof development

moreover

Local lemmas
moreover—ultimately

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

$\approx$

have $lab_1$: $P_1$ ...
have $lab_2$: $P_2$ ...
: 
have $lab_n$: $P_n$ ...
from $lab_1$ $lab_2$ ...
have $P$ ...

With names
Streamlining Proofs

Pattern Matching and Quotations
Top down proof development
moreover
Local lemmas
Local lemmas

have $B$ \textbf{if name:} $A_1 \ldots A_m$ \textbf{for} $x_1 \ldots x_n$

\langle proof \rangle

proves $\left[ A_1; \ldots ; A_m \right] \implies B$

where all $x_i$ have been replaced by $?x_i$. 
Proof state and Isar text

In general: \textbf{proof method}

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

\[
\forall x_1 \ldots x_n. \begin{array}{lcl}
\land A_1; \ldots ; A_m \end{array} \implies B
\]

How to prove each subgoal:

\begin{align*}
\text{fix } x_1 \ldots x_n \\
\text{assume } A_1 \ldots A_m \\
\vdash \\
\text{show } B
\end{align*}

Separated by \textbf{next}
Isar by example

Proof patterns

Streamlining Proofs

Proof by Cases and Induction
Isar_Induction_Demo.thy

Proof by cases
Datatype case analysis

datatype $t = C_1 \vec{\tau} \mid \ldots$

proof (cases "term")
  case $(C_1 x_1 \ldots x_k)$
  \ldots $x_j$ \ldots
  next
  :
  qed

where case $(C_i x_1 \ldots x_k)$ $\equiv$

fix $x_1 \ldots x_k$

assume $C_i$:

label $term = (C_i x_1 \ldots x_k)$

formula
Isar_Induction_Demo.thy

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

show $P(n)$

proof (induction $n$)
  case 0
  
  show $?case$

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

qed

$\equiv$  let $?case = P(0)$

$\equiv$  fix $n$ assume Suc: $P(n)$

let $?case = P(Suc n)$
Structural induction with $\Rightarrow$

\[
\text{show } A(n) \implies P(n)
\]
\[
\text{proof (induction } n) \\
\text{ case } 0 \equiv \text{ assume } 0: A(0) \\
\quad \text{let } ?case = P(0)
\]
\[
\text{next} \\
\text{ case } (\text{Suc } n) \equiv \text{ fix } n \\
\quad \text{assume } \text{Suc}: A(n) \implies P(n) \\
\quad \quad A(\text{Suc } n) \\
\quad \text{let } ?case = P(\text{Suc } n)
\]
\[
\text{show } ?case
\]
\text{qed}
Named assumptions

In a proof of

\[ A_1 \Rightarrow \ldots \Rightarrow A_n \Rightarrow B \]

by structural induction:

In the context of

**case** \( C \)

we have

**C.IH** the induction hypotheses

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

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

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

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

Rule Induction

Rule Inversion
Isar_Induction_Demo.thy

Rule induction
Rule induction

inductive $I :: \tau \Rightarrow \sigma \Rightarrow \text{bool}$
where
rule$_1$: ...
:
rule$_n$: ...

show $I \, x \, y \Longrightarrow P \, x \, y$
proof (induction rule: $I$\_induct)
  case rule$_1$
  ...
  show $?case$
next
  :
  :
next
  case rule$_n$
  ...
  show $?case$
qed
Fixing your own variable names

\[ \text{case } (\text{rule}_i \ x_1 \ldots \ x_k) \]

Renames the first \( k \) variables in \( \text{rule}_i \) (from left to right) to \( x_1 \ldots \ x_k \).
Named assumptions

In a proof of

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

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

In the context of \( \text{case } R \) we have

- \( R.IH \): the induction hypotheses
- \( R.hyps \): the assumptions of rule \( R \)
- \( R.prems \): the premises \( A_i \)

\[ R \quad R.IH + R.hyps + R.prems \]
Proof by Cases and Induction

Rule Induction

Rule Inversion
Rule inversion

inductive \( ev :: \text{nat} \Rightarrow \text{bool} \) where
\[ ev0: \ ev \ 0 \ |
\]
\[ evSS: \ ev \ n \Rightarrow ev(Suc(Suc \ n)) \]

What can we deduce from \( ev \ n \)?
That it was proved by either \( ev0 \) or \( evSS \)!

\[
\begin{align*}
\quad ev \ n & \Rightarrow n = 0 \lor (\exists k. \ n = Suc(Suc \ k) \land ev \ k)
\end{align*}
\]

Rule inversion = 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 (evSSS k)
    :
    show ?thesis ...
qed

Impossible cases disappear automatically