Experiments in Verification

SS 2010

Christian Sternagel (VO)[1]

Computational Logic
Institute of Computer Science
University of Innsbruck

26 March 2010

[1] christian.sternagel@uibk.ac.at

Simplification On One Slide

- basic methods: `simp`, `simp_all`
- `simp`-modifiers: `add:` ⟨*thms*⟩, `del:` ⟨*thms*⟩, `only:` ⟨*thms*⟩, `(no_asm)`, `(no_asm_simp)`, `(no_asm_use)`
- modifying the simpset: **`declare`** ⟨*thm*⟩`[simp]`, **`declare`** ⟨*thm*⟩`[simp del]`
- unfolding specific `simp`-rules: **`unfolding`** ⟨*thms*⟩

This Time

Session 1
formal verification, Isabelle/HOL basics, functional programming in HOL

Session 2
simplification, function definitions, induction, calculational reasoning

Session 3
natural deduction, propositional logic, predicate logic

Session 4
sets, relations, inductively defined sets, advanced topics

Isabelle's Meta-Logic

Description

minimal intuitionistic higher-order logic

Connectives

- $\bigwedge$: universal quantifier
- $\Longrightarrow$: implication
- $\equiv$: equality

Example

$$\bigwedge x\ y.\ x \equiv y \Longrightarrow y \equiv x$$

Some Remarks

Schematic Variables

free variables and (meta) universally quantified variables (at the outermost level) are both turned into schematic variables after a proof

Meta-Equality

in almost any case, equality (=) may be used instead of meta-equality ($\equiv$)

Meta-Implication

- nested implications associate to the right and
- may be abbreviated by $[\![A_1\,;\,\ldots\,;A_n]\!] \Longrightarrow B$ instead of $A_1 \Longrightarrow \ldots \Longrightarrow A_n \Longrightarrow B$
- **assumes** A **shows** B is turned into $A \Longrightarrow B$ after a proof

Natural Deduction

Inference Rules

- $\dfrac{A_1 \qquad \ldots \qquad A_n}{B}\,\langle \mathit{name} \rangle$
- premises $A_1, \ldots, A_n$
- conclusion B

In Isabelle

$$\textbf{theorem}\ \langle \mathit{name} \rangle\texttt{:}\ \textbf{assumes}\ A_1\ \texttt{and}\ \ldots\ \texttt{and}\ A_n\ \textbf{shows}\ B$$

resulting in

$$[\![?A_1;\ldots;?A_n]\!] \Longrightarrow ?B$$

Example

Conjunction Rules and an Easy Proof

$$\frac{\phi \qquad \psi}{\phi \land \psi}\ \land\mathsf{i}$$

$$\frac{\phi \land \psi}{\phi}\ \land\mathsf{e}_1$$

$$\frac{\phi \land \psi}{\psi}\ \land\mathsf{e}_2$$

1	$p \land q$	premise
2	r	premise
3	q	$\land\mathsf{e}_2$ 1
4	p	$\land\mathsf{e}_1$ 1
5	$q \land r$	$\land\mathsf{i}$ 3, 2
6	$p \land (q \land r)$	$\land\mathsf{i}$ 4, 5

The Same Rules in Isabelle

$\texttt{conjI:}\ [\![?P; ?Q]\!] \Longrightarrow\ ?P \land\ ?Q$

$\texttt{conjunct1:}\ ?P \land\ ?Q \Longrightarrow\ ?P$

$\texttt{conjunct2:}\ ?P \land\ ?Q \Longrightarrow\ ?Q$

The Method `rule`

- synopsis: `rule` $\langle \mathit{name} \rangle$
- applies to a goal provided it is the instance of the conclusion of $\langle \mathit{name} \rangle$
- solves the goal if there are current facts that are instances of the premises of $\langle \mathit{name} \rangle$
- the number and order of those facts has to be exactly the same as for the premises of $\langle \mathit{name} \rangle$

The Above Proof in Isabelle

State What You Want To Prove

```
lemma
  assumes pq: "p ∧ q" and "r"
  shows "p ∧ (q ∧ r)" (is ?goal)
```

Prove It

```
proof -
  from pq have "q" by (rule conjunct2)
  from pq have "p" by (rule conjunct1)
  moreover
  from `q` and `r` have "q ∧ r" by (rule conjI)
  ultimately
  show ?goal by (rule conjI)
qed
```

Some Notes

- referring to facts is possible via name (if one was defined), e.g., **`from`** `pq ...`
- or by explicitly writing the fact between backticks (this is then called a literal fact), e.g., **`from`** `` `q` ... ``
- for every term (between double quotes) an abbreviation can be introduced using an is-pattern, e.g., "$p \wedge (q \wedge r)$" `(is ?goal)`
- **`moreover`** is used to collect a list of facts
- afterwards the list is used by **`ultimately`**

Introduction/Elimination Rules

Idea

For every logical connective there are several rules for introducing it and for eliminating it.

Natural Deduction - Propositional Logic

$$\frac{\phi \qquad \psi}{\phi \wedge \psi}\,(\wedge\mathrm{i}) \qquad \frac{\phi_i}{\phi_1 \vee \phi_2}\,(\vee\mathrm{i}_i) \qquad \frac{\boxed{\begin{array}{c}\phi\\ \vdots\\ \psi\end{array}}}{\phi \to \psi}\,(\to\mathrm{i}) \qquad \frac{\boxed{\begin{array}{c}\phi\\ \vdots\\ \bot\end{array}}}{\neg\phi}\,(\neg\mathrm{i})$$

$$\frac{\phi_1 \wedge \phi_2}{\phi_i}\,(\wedge\mathrm{e}_i) \qquad \frac{\phi \vee \psi \qquad \boxed{\begin{array}{c}\phi\\ \vdots\\ \chi\end{array}} \qquad \boxed{\begin{array}{c}\psi\\ \vdots\\ \chi\end{array}}}{\chi}\,(\vee\mathrm{e}) \qquad \frac{\phi \to \psi \qquad \phi}{\psi}\,(\to\mathrm{e}) \qquad \frac{\neg\phi \qquad \phi}{\psi}\,(\neg\mathrm{e})$$

Some Derived Rules

Double Negation Introduction

$$\frac{\phi}{\neg\neg\phi}\ (\neg\neg\text{i})$$

Proof.

1	ϕ	premise
2	$\neg\phi$	assumption
3	$\bot$	$\neg$e 2, 1
4	$\neg\neg\phi$	$\neg$i 2–3

□

Some Derived Rules (cont'd)

Law Of The Excluded Middle

$$\frac{}{\phi \vee \neg\phi}\ (\mathsf{lem})$$

Proof.
Exercise □

Some Derived Rules (cont'd)

Double Negation Elimination

$$\frac{\neg\neg\phi}{\phi}\ (\neg\neg\mathsf{e})$$

Proof.

1	$\neg\neg\phi$	premise
2	$\phi \vee \neg\phi$	lem
3	ϕ	assumption
4	$\neg\phi$	assumption
5	ϕ	$\neg$e 1, 4
6	ϕ	$\vee$e 2, 3, 4–5

□

Some Derived Rules (cont'd)

Proof By Contradiction

$$\frac{\boxed{\begin{array}{c}\neg\phi\\ \vdots\\ \bot\end{array}}}{\phi}\ (\mathrm{pbc})$$

Proof.

1	$\neg\phi$	assumption
$\vdots$	$\vdots$	
n	$\bot$	
$n+1$	$\neg\neg\phi$	$\neg$i 1–n
$n+2$	ϕ	$\neg\neg$e $n+1$

$\square$

A Word On Destruction Rules

Loosing Information

- usually rules like $\wedge e_1$ are known as elimination rules
- in Isabelle they are called destruction rules
- using such rules destroys information
- thus it can turn a goal unprovable
- use destruction rules with care

Example (Conjunction Elimination)

$$\dfrac{\phi \wedge \psi \qquad \boxed{\begin{array}{c}\phi\\ \psi\\ \vdots\\ \chi\end{array}}}{\chi}\;(\wedge\mathsf{e})$$

Raw Proof Blocks

In-Place Proofs

- enclose between { and }
- does not work on current goal but introduces new facts
- any '**assume**'s are premises of the resulting fact
- the last '**have**' is the conclusion of the resulting fact
- like boxes in the 'pen 'n' paper' natural deduction rules

Universal Quantification

Introduction and Elimination Rules

$$\frac{\boxed{\begin{array}{c} x_0 \\ \vdots \\ \phi(x_0) \end{array}}}{\forall x.\ \phi(x)}\ (\forall\mathrm{i}) \qquad \frac{\forall x.\ \phi(x)}{\phi(t)}\ (\forall\mathrm{e})$$

Isabelle Idiom for Meta Universal Quantification

$$\texttt{\textbf{fix}}\ x_0\ \ldots\ \texttt{\textbf{show}}\ \texttt{"}?P(x_0)\texttt{"}\ \langle \mathit{proof} \rangle$$

results in

$$\bigwedge x.\ ?P(x)$$

Existential Quantification

Introduction and Elimination Rules

$$\frac{\phi(t)}{\exists x.\ \phi(x)}\ (\exists i) \qquad \frac{\exists x.\ \phi(x) \qquad \boxed{\begin{array}{c} x_0 \ \ \phi(x_0) \\ \vdots \\ \psi \end{array}}}{\psi}\ (\exists e)$$

Isabelle Idiom For ∃-Elimination

"$\exists x.\ ?P(x)$" **then** **obtain** y **where** "$?P(y)$" $\langle proof \rangle$

results in

$$?P(y)$$

An Example Proof

```
lemma
  assumes ex: "∃x. ∀y. P x y"
    shows "∀y. ∃x. P x y"
proof
  fix y
  from ex obtain x where "∀y. P x y" by (rule exE)
  hence "P x y" by (rule spec)
  thus "∃x. P x y" by (rule exI)
qed
```

Exercises

http://isabelle.in.tum.de/exercises/logic/elimination/ex.pdf
http://isabelle.in.tum.de/exercises/logic/propositional/ex.pdf
http://isabelle.in.tum.de/exercises/logic/predicate/ex.pdf