

Experiments in Verification

SS 2010

Christian Sternagel (VO)¹

Computational Logic
Institute of Computer Science
University of Innsbruck

26 March 2010

¹christian.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
- ▶ \implies : implication
- ▶ \equiv : equality

Example

$$\bigwedge x y. x \equiv y \implies y \equiv x$$

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 $\llbracket A_1 ; \dots ; A_n \rrbracket \implies B$ instead of $A_1 \implies \dots \implies A_n \implies B$
- ▶ **assumes** A **shows** B is turned into $A \implies B$ after a proof

Natural Deduction

Inference Rules

- ▶ $\frac{A_1 \quad \dots \quad A_n}{B} \langle name \rangle$
- ▶ **premises** A_1, \dots, A_n
- ▶ **conclusion** B

In Isabelle

theorem $\langle name \rangle$: **assumes** A_1 and ... and A_n **shows** B

resulting in

$$\llbracket ?A_1 ; \dots ; ?A_n \rrbracket \implies ?B$$

Example

Conjunction Rules and an Easy Proof

$\frac{\phi \quad \psi}{\phi \wedge \psi} \wedge_i$	1	$p \wedge q$	premise
	2	r	premise
$\frac{\phi \wedge \psi}{\phi} \wedge_{e_1}$	3	q	$\wedge_{e_2} 1$
	4	p	$\wedge_{e_1} 1$
$\frac{\phi \wedge \psi}{\psi} \wedge_{e_2}$	5	$q \wedge r$	$\wedge_i 3, 2$
	6	$p \wedge (q \wedge r)$	$\wedge_i 4, 5$

The Same Rules in Isabelle

$\text{conjI: } \llbracket ?P; ?Q \rrbracket \Longrightarrow ?P \wedge ?Q$
 $\text{conjunct1: } ?P \wedge ?Q \Longrightarrow ?P$
 $\text{conjunct2: } ?P \wedge ?Q \Longrightarrow ?Q$

The Method rule

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

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

$$\frac{\phi \quad \psi}{\phi \wedge \psi} (\wedge i)$$

$$\frac{\phi_i}{\phi_1 \vee \phi_2} (\vee i)$$

$$\frac{\boxed{\begin{array}{c} \phi \\ \vdots \\ \psi \end{array}}}{\phi \rightarrow \psi} (\rightarrow i)$$

$$\frac{\boxed{\begin{array}{c} \phi \\ \vdots \\ \perp \end{array}}}{\neg \phi} (\neg i)$$

$$\frac{\phi_1 \wedge \phi_2}{\phi_i} (\wedge e_i)$$

$$\frac{\phi \vee \psi \quad \boxed{\begin{array}{c} \phi \\ \vdots \\ \chi \end{array}} \quad \boxed{\begin{array}{c} \psi \\ \vdots \\ \chi \end{array}}}{\chi} (\vee e)$$

$$\frac{\phi \rightarrow \psi \quad \phi}{\psi} (\rightarrow e)$$

$$\frac{\neg \phi \quad \phi}{\psi} (\neg e)$$

Some Derived Rules

Double Negation Introduction

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

Proof.

1	ϕ	premise
2	$\neg \phi$	assumption
3	\perp	$\neg e$ 2, 1
4	$\neg \neg \phi$	$\neg i$ 2-3

□

Some Derived Rules (cont'd)

Law Of The Excluded Middle

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

Proof.

Exercise □

Some Derived Rules (cont'd)

Double Negation Elimination

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

Proof.

1	$\neg\neg\phi$	premise
2	$\phi \vee \neg\phi$	lem
3	ϕ	assumption
4	$\neg\phi$	assumption
5	ϕ	$\neg\text{e } 1, 4$
6	ϕ	$\vee\text{e } 2, 3, 4\text{--}5$

□

Some Derived Rules (cont'd)

Proof By Contradiction

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

Proof.

1	$\neg\phi$ assumption
⋮	\vdots
n	\perp
n + 1	$\neg\neg\phi$ $\neg i$ 1-n
n + 2	ϕ $\neg\neg e$ n + 1



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)

$$\frac{\phi \wedge \psi \quad \boxed{\begin{array}{c} \phi \\ \psi \\ \vdots \\ \chi \end{array}}}{\chi} \text{ } (\wedge e)$$

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

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

Isabelle Idiom for Meta Universal Quantification

fix x_0 ... **show** " $?P(x_0)$ " $\langle proof \rangle$

results in

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

Existential Quantification

Introduction and Elimination Rules

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

Isabelle Idiom For \exists -Elimination

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

results in

$?P(y)$

An Example Proof

lemma

assumes ex: " $\exists x. \forall y. P \ x \ y$ "

shows " $\forall y. \exists x. P \ x \ y$ "

proof

fix y

from ex **obtain** x **where** " $\forall y. P \ x \ y$ " **by** (rule exE)

hence " $P \ x \ y$ " **by** (rule spec)

thus " $\exists x. P \ x \ y$ " **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>