

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

- Λ : universal quantifier
- $\blacktriangleright \implies$: implication
- $\blacktriangleright \equiv: equality$

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

Natural Deduction

Inference Rules

•
$$\frac{A_1 \dots A_n}{B} \langle name \rangle$$

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

Example

Conjunction Rules and an Easy Proof al

$\phi \psi$			
$\frac{1}{\phi \wedge \psi} \wedge i$	1	$p \wedge q$	premise
T, T	2	r	premise
$\phi \wedge \psi$,	3	q	$\wedge e_2 \ 1$
$\frac{-\phi \wedge \psi}{\phi} \wedge e_1$	4	p	$\wedge e_1 \ 1$
	5	$m{q}\wedgem{r}$	∧i 3, 2
$\phi \wedge \psi \wedge \mathbf{e}_2$	6	$p \wedge (q \wedge r)$	∧i 4, 5
ψ , ψ			

The Same Rules in Isabelle

7

The Method rule

- ► synopsis: rule (*name*)
- ▶ applies to a goal provided it is the instance of the conclusion of ⟨name⟩
- ► solves the goal if there are current facts that are instances of the premises of (name)
- ► the number and order of those facts has to be exactly the same as for the premises of (name)

The Above Proof in Isabelle

```
State What You Want To Prove
 lemma
   assumes pq: "p \land q" and "r"
   shows "p \land (q \land 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 \wedge r" by (rule conjI)
   ultimately
   show ?goal by (rule conjI)
qed
```

Some Notes

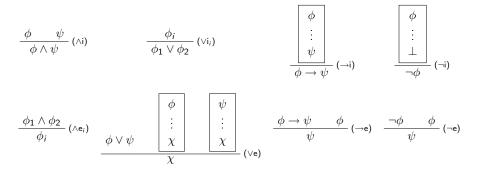
- referring to facts is possible via name (if one was defined), e.g., from pq ...
- or by explicitly writing the fact between backticks (this is then called a literal fact), e.g., from 'q' ...
- ▶ for every term (between double quotes) an abbreviation can be introduced using an is-pattern, e.g., "p ∧ (q ∧ 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



Some Derived Rules

Double Negation Introduction

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

Proof.

1	ϕ	premise
2	$\neg \phi$	assumption
3		¬e 2, 1
4	$\neg \neg \phi$	¬i 2−3

Session 3 - Experiments in Verification

Some Derived Rules (cont'd)

Law Of The Excluded Middle

$$\overline{\phi \lor \neg \phi}$$
 (lem)

Proof. Exercise

Some Derived Rules (cont'd)

Double Negation Elimination

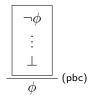


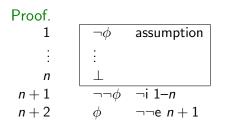
Proof.

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

Some Derived Rules (cont'd)

Proof By Contradiction





A Word On Destruction Rules

Loosing Information

- usually rules like $\land e_1$ 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)

$$\begin{array}{c|c} \phi \\ \psi \\ \vdots \\ \chi \end{array} \\ \hline \chi \end{array} (\wedge e)$$

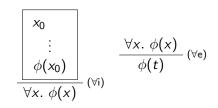
Raw Proof Blocks

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



Isabelle Idiom for Meta Universal Quantification

fix
$$x_0 \dots$$
 show "? $P(x_0)$ " $\langle proof \rangle$
 $\bigwedge x. ?P(x)$

results in

Existential Quantification

Introduction and Elimination Rules

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

()

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)
ged
```

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