

Experiments in Verification SS 2009

Christian Sternagel (VO)¹

Computational Logic Institute of Computer Science University of Innsbruck

20 March 2009

 $^{1} {\tt christian.sternagel@uibk.ac.at}$

Session 3 - Experiments in Verification

Summary of Last Session

Simplification On One Slide

- ▶ basic methods: simp, simp_all
- ▶ simp-modifiers: add: $\langle thms \rangle$, del: $\langle thms \rangle$, only: $\langle thms \rangle$, (no_asm), (no_asm_simp), (no_asm_use)
- modifying the simpset: declare \langle thm \rangle [simp],
 declare \langle thm \rangle [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

CS (ICS@UIBK) EVE 3/21

Session 3 - Experiments in Verification

Natural Deduction

Isabelle's Meta-Logic

Description

minimal intuitionistic higher-order logic

Connectives

► \\: universal quantifier

▶ ⇒: implication

► ≡: 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 $\llbracket A_1; \ldots; A_n \rrbracket \Longrightarrow B$ instead of $A_1 \Longrightarrow \ldots \Longrightarrow A_n \Longrightarrow B$
- **assumes** A shows B is turned into $A \Longrightarrow B$ after a proof

CS (ICS@UIBK) EVE 5/2:

Session 3 - Experiments in Verification

Natural Deduction

Natural Deduction

Inference Rules

- ightharpoonup premises A_1, \ldots, A_n
- ► conclusion B

In Isabelle

theorem
$$\langle name \rangle : [A_1; ...; A_n] \Longrightarrow B$$

resulting in

$$\llbracket ?A_1; \ldots; ?A_n \rrbracket \Longrightarrow ?B$$

Example

Conjunction Rules and An Easy Proof

ϕ ψ			
$\frac{1}{\phi \wedge \psi} \wedge i$	1	$p \wedge q$	premise
7 / 7	2	r	premise
$\phi \wedge \psi$	3	q	$\wedge e_2 \ 1$
$\frac{\varphi \wedge \varphi}{\phi} \wedge e_1$	4	p	$\wedge e_1 \ 1$
	5	$q \wedge r$	∧i 3, 2
$\frac{\phi \wedge \psi}{} \wedge e_2$	6	$p \wedge (q \wedge r)$	∧i 4, 5
ψ		,	

The Same Rules in Isabelle

$$\begin{array}{ll} \texttt{conjI:} \ \llbracket ?P; ?Q \rrbracket \Longrightarrow ?P \land ?Q & \texttt{conjunct1:} \ ?P \land ?Q \Longrightarrow ?P \\ & \texttt{conjunct2:} \ ?P \land ?Q \Longrightarrow ?Q \end{array}$$

CS (ICS@UIBK) EVE 7/21

Session 3 - Experiments in Verification

Natural Deduction

The Method rule

- ► synopsis: rule ⟨name⟩
- \blacktriangleright applies to a goal provided it is the instance of the conclusion of $\langle \textit{name} \rangle$
- \blacktriangleright 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
```

CS (ICS@UIBK) EVE 9/2

Session 3 - Experiments in Verification

Natural Deduction

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., " $p \land (q \land r)$ " (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

$$\frac{\phi \quad \psi}{\phi \wedge \psi} \text{ (\wedgei$)} \qquad \frac{\phi_{i}}{\phi_{1} \vee \phi_{2}} \text{ (\veei$)} \qquad \frac{\phi}{\psi} \text{ (\negi$)} \qquad \frac{\phi}{\psi} \text{ (\negi$)} \qquad \frac{\phi}{\neg \phi} \text{$$

CS (ICS@UIBK) EVE 11/21

Session 3 - Experiments in Verification

Propositional Logi

Some Derived Rules

Double Negation Introduction

$$\frac{\phi}{\neg\neg\phi}$$
 (¬¬i)

Proof.

$$\begin{array}{cccc} 1 & \phi & \text{premise} \\ 2 & \neg \phi & \text{assumption} \\ 3 & \bot & \neg e \ 2, \ 1 \\ 4 & \neg \neg \phi & \neg i \ 2 – 3 \end{array}$$

Some Derived Rules (cont'd)

Law Of The Excluded Middle

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

Proof.

Exercise

CS (ICS@UIBK) EVE 13/21

Session 3 - Experiments in Verification

Propositional Logi

Some Derived Rules (cont'd)

Double Negation Elimination

$$\frac{\neg\neg\phi}{\phi}$$
 (¬¬e)

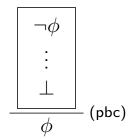
Proof.

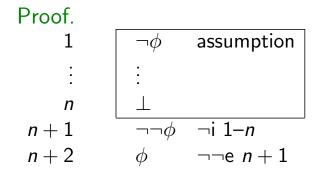
6

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

Some Derived Rules (cont'd)

Proof By Contradiction





CS (ICS@UIBK) EVE 15/21

Session 3 - Experiments in Verification

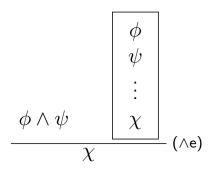
Propositional Logic

A Word On Destruction Rules

Loosing Information

- ightharpoonup 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)



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

CS (ICS@UIBK) EVE 17/2

Session 3 - Experiments in Verification

Predicate Logi

Universal Quantification

Introduction and Elimination Rules

$$\begin{array}{c|c}
x_0 \\
\vdots \\
\phi(x_0)
\end{array}$$

$$\frac{\forall x. \ \phi(x)}{\phi(t)} \ (\forall e)$$

$$\frac{\forall x. \ \phi(x)}{\phi(t)} \ (\forall e)$$

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

Isabelle Idiom For ∃-Elimination

```
"\exists x. \ ?P(x)" then obtain y where "?P(y)" \langle proof \rangle results in ?P(y)
```

CS (ICS@UIBK) EVE 19/21

Session 3 - Experiments in Verification

Predicate Logi

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

CS (ICS@UIBK) EVE 21/21