Experiments in Verification

SS 2011

Christian Sternagel

Computational Logic
Institute of Computer Science
University of Innsbruck

April 1, 2011

Today's Topics

- Natural Deduction
- Propositional Logic
- Predicate Logic

Natural Deduction

Isabelle's Meta-Logic

- description: minimal intuitionistic higher-order logic
- connectives
  - $\bigwedge$: universal quantifier
  - $\Longrightarrow$: implication
  - $\equiv$: equality

Example

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

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

- $\dfrac{A_1 \quad \ldots \quad A_n}{B}\ \langle name \rangle$
- premises $A_1, \ldots, A_n$
- 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

$$\frac{\phi \quad \psi}{\phi \wedge \psi}\ \wedge\text{i} \qquad \frac{\phi \wedge \psi}{\phi}\ \wedge\text{e}_1 \qquad \frac{\phi \wedge \psi}{\psi}\ \wedge\text{e}_2$$

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

The Same Rules in Isabelle

`conjI:` $[\![?P; ?Q]\!] \Longrightarrow ?P \wedge ?Q$

`conjunct1:` $?P \wedge ?Q \Longrightarrow ?P$

`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

```
lemma
  assumes pq: "p ∧ q" and "r"
  shows "p ∧ (q ∧ r)" (is ?goal)
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 ∧ (q ∧ r)" (is ?goal)`
- `moreover` is used to collect a list of facts
- afterwards the list is used by `ultimately`

Propositional Logic

Idea of Introduction/Elimination Rules

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

Natural Deduction – Propositional Logic

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

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

Derived Rule – 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

Derived Rule – Law of the Excluded Middle

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

Proof

Exercise

Derived Rule – Double Negation Elimination

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

Proof

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

Derived Rule – Proof by Contradiction

$$\frac{\begin{array}{|c|}\hline \neg\phi \\ \vdots \\ \bot \\ \hline\end{array}}{\phi}\ (\text{pbc})$$

Proof

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

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

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

Raw Proof Blocks

- 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

Predicate Logic

Universal Quantification

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

Isabelle Idiom for Meta Universal Quantification

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

results in

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

Existential Quantification

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

Isabelle Idiom for ∃-Elimination

"∃x. ?P(x)" **then obtain** y **where** "?P(y)" ⟨*proof*⟩

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