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

Isabelle's Meta-Logic

- description: minimal intuitionistic higher-order logic
- connectives

Isabelle's Meta-Logic

- description: minimal intuitionistic higher-order logic
- connectives
  - $\bigwedge$: universal quantifier

Isabelle's Meta-Logic

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

Isabelle's Meta-Logic

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

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

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 ($\equiv$)

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

- $$\frac{A_1 \qquad \ldots \qquad A_n}{B} \langle name \rangle$$

Natural Deduction

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

Natural Deduction

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

Natural Deduction

- $\dfrac{A_1 \qquad \dots \qquad A_n}{B}\,\langle name \rangle$
- 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

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

Example – Conjunction Rules and an Easy Proof

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

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

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

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

Example – Conjunction Rules and an Easy Proof

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

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

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

1	$p \wedge q$	premise
2	r	premise
3	q	$\wedge e_2$ 1
4	p	$\wedge e_1$ 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` ⟨*name*⟩

The Method `rule`

- synopsis: `rule` ⟨*name*⟩
- applies to a goal provided it is the instance of the conclusion of ⟨*name*⟩

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 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

```
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` ...

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` ...``

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` ...

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)

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

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`**

Propositional Logic

Idea of Introduction/Elimination Rules

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

Idea of Introduction/Elimination Rules

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

Natural Deduction – Propositional Logic

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

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

Derived Rule – Double Negation Introduction

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

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

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

Derived Rule – Law of the Excluded Middle

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

Proof

Exercise

Derived Rule – Double Negation Elimination

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

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

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

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

A Word on Destruction Rules – Loosing Information

- usually rules like $\wedge e_1$ are known as elimination rules

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

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

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

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

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 `}`

Raw Proof Blocks

- enclose between `{` and `}`
- does not work on current goal but introduces new facts

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

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

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

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

Universal Quantification

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

Isabelle Idiom for Meta Universal Quantification

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

results in

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

Existential Quantification

$$\frac{\phi(t)}{\exists x.\ \phi(x)}\ (\exists\mathrm{i})$$

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

Existential Quantification

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

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