Mapping of ND proof templates to Isabelle formalization

Alexander Steen

April 25, 2016

1 ND rules and their Isabelle names

Summary of discussed natural deduction rules with their Isabelle name:

$$\frac{A \quad B}{A \wedge B}\ conjI \qquad \frac{A \wedge B}{A}\ conjunct1 \qquad \frac{A \wedge B}{B}\ conjunct2$$

$$\frac{A}{A \vee B}\ disjI1 \qquad \frac{B}{A \vee B}\ disjI2 \qquad \frac{A \vee B \quad \begin{matrix}[A]\\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B]\\ \vdots \\ C\end{matrix}}{C}\ disjE$$

$$\frac{\begin{matrix}[A]\\ \vdots \\ B\end{matrix}}{A \longrightarrow B}\ impI \qquad \frac{A \longrightarrow B \quad A}{B}\ mp \qquad \frac{\begin{matrix}[A]\\ \vdots \\ \bot\end{matrix}}{\neg A}\ notI \qquad \frac{\neg A \quad A}{B}\ notE$$

$$\frac{\begin{matrix}[\neg A]\\ \vdots \\ \bot\end{matrix}}{A}\ ccontr \qquad \frac{\neg\neg A}{A}\ notnotD \qquad \frac{}{\neg A \vee A}\ excluded\_middle$$

In Isabelle syntax

conjI $?P \Longrightarrow ?Q \Longrightarrow ?P \wedge ?Q$

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

conjunct2 $?P \wedge ?Q \Longrightarrow ?Q$

disjI1 $?P \Longrightarrow ?P \vee ?Q$

disjI2 $?Q \Longrightarrow ?P \vee ?Q$

disjE $?P \vee ?Q \Longrightarrow (?P \Longrightarrow ?R) \Longrightarrow (?Q \Longrightarrow ?R) \Longrightarrow ?R$

impI $(?P \Longrightarrow ?Q) \Longrightarrow ?P \longrightarrow ?Q$

mp $?P \longrightarrow ?Q \Longrightarrow ?P \Longrightarrow ?Q$

notI $(?P \Longrightarrow False) \Longrightarrow \neg ?P$

notE $\neg ?P \Longrightarrow ?P \Longrightarrow ?R$

ccontr $(\neg ?P \Longrightarrow False) \Longrightarrow ?P$

notnotD $\neg\neg ?P \Longrightarrow ?P$

excluded_middle $\neg ?P \vee ?P$

2 General hints and keywords

2.1 General

thm Output a fact. Can be added anywhere and does not influence anything around it. Handy for checking which facts are currently known to Isabelle.

```
thm notI this
```

Outputs the fact notI (negation introduction) and the fact that is referred to by **this**. Multiple facts are separated by blanks.

{,} The curly braces open a new block, i.e. a sub-proof.

- The minus sign denotes the identity rule. Can be used at various places:
(1) Iterate facts (maybe with a new label)

```
lemma
  assumes "P"
  shows "..."
 proof -
  ...
  from assms have "P" by -
  moreover have ...
  ...
 qed
```

(2) top-level introduction rule of proof

```
lemma
  ...
 proof -
  ...
 qed
```

vs.

```
lemma
  ...
 proof (rule disjI1)
  ...
 qed
```

note Gives labels to blocks (and more?)

```
{
  assume "P"
  from ... have "Q" by ...
} note a = this
```

gives the fact $P \Longrightarrow Q$ the label a.

2.2 Within proofs

have Add new fact to the collection of known facts:

```
from a b c have "P" by ...
```

from Refer to a (list of) fact(s) that is used a source for the current fact construction

this Refer to the last fact (e.g. the fact that has been introduced last)

```
from ... have a: P by ...
from a have ... by ...
```

is equivalent to

```
from ... have P by ...
from this have ... by ...
```

with facts is short for `from facts this`, i.e.

```
from ... have a: P by ...
from somefact a have ... by ...
```

is equivalent to

```
from ... have P by ...
with somefact have ... by ...
```

then Short for `from this`. The above listing can be simplified to

```
from ... have P by ...
then have ... by ...
```

hence Short for `then have`. The above listing can be simplified to

```
from ... have P by ...
hence ... by ...
```

moreover, ultimately Start collecting facts for **have**ing a fact from all these collected facts without explicit naming, e.g.

```
from ... have "P" by (rule conjunct1)
moreover from ... have "Q" by (rule conjunct1)
ultimately have "P ∧ Q" by (rule conjI)
```

show Used to state that we can proof a goal (by application of some rules):

```
from a b c show "P" by ...
```

thus Directly refer to `this` for a show-command:

```
from ... have a: P by ...
from a show ... by ...
```

is equivalent to

```
from ... have P by ...
thus ... by ...
```

Example proof using some of the above keywords for $\vdash A \vee \neg A$

```
theorem
  shows "A ∨ ¬A"
 proof -
  {
    assume a: "¬(A ∨ ¬A)"
    {
      assume "A"
      then have "A ∨ ¬A" by (rule disjI1)
      with a have "False" by (rule notE)
    }
    hence "¬A" by (rule notI)
    hence "A ∨ ¬A" by (rule disjI2)
    with a have "False" by (rule notE)
  }
  hence "¬¬(A ∨ ¬A)" by (rule notI)
  thus "A ∨ ¬A" by (rule notnotD)
 qed
```

3 ND proof templates

For use within proofs to create new facts (with **have**):

conjI Rule: $\dfrac{A \quad B}{A \wedge B}\ conjI$

```
from ... have "A" by ...
moreover from ... have "B" by ...
ultimately have "A ∧ B" by (rule conjI)
```

---

conjunct1 Rule: $\dfrac{A \wedge B}{A}\ conjunct1$

```
from ... have "A ∧ B" by ...
hence "A" by (rule conjunct1)
```

---

conjunct2 Rule: $\dfrac{A \wedge B}{B}\ conjunct2$

```
from ... have "A ∧ B" by ...
hence "B" by (rule conjunct2)
```

---

disjI1 Rule: $\dfrac{A}{A \vee B}\ disjI1$

```
from ... have "A" by ...
hence "A ∨ B" by (rule disjI1)
```

---

disjI2 Rule: $\dfrac{B}{A \lor B}\ \mathit{disjI2}$

```
from ... have "B" by ...
hence "A ∨ B" by (rule disjI2)
```

---

disjE Rule: $\dfrac{A \lor B \quad \begin{matrix}[A] \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B] \\ \vdots \\ C\end{matrix}}{C}\ \mathit{disjE}$

```
from ... have "A ∨ B" by ...
moreover {
  assume "A"
  ...
  from ... have "C" by ...
}
moreover {
  assume "B"
  ...
  from ... have "C" by ...
}
ultimately have "C" by (rule disjE)
```

---

impI Rule: $\dfrac{\begin{matrix}[A] \\ \vdots \\ B\end{matrix}}{A \longrightarrow B}\ \mathit{impI}$

```
{
  assume "A"
  ...
  from ... have "B" by ...
}
hence "A ⟶ B" by (rule impI)
```

---

mp Rule: $\dfrac{A \longrightarrow B \quad A}{B}\ \mathit{mp}$

```
from ... have "A ⟶ B" by ...
moreover from ... have "A" by ...
ultimately have "B" by (rule mp)
```

---

notI Rule: $\dfrac{\begin{matrix}[A] \\ \vdots \\ \bot\end{matrix}}{\neg A}\ \mathit{notI}$

```
{
  assume "A"
```

```
    ...
    from ... have "False" by ...
  }
  hence "¬A" by (rule notI)
```

---

notE Rule: $\dfrac{\neg A \quad A}{B}$ *notE*

```
  from ... have "¬A" by ...
  moreover from ... have "A" by ...
  ultimately have "B" by (rule notE)
```

---

ccontr Rule: $\dfrac{\begin{matrix}[\neg A] \\ \vdots \\ \bot\end{matrix}}{A}$ *ccontr*

```
  {
    assume "¬A"
    ...
    from ... have "False" by ...
  }
  hence "A" by (rule ccontr)
```

---

notnotD Rule: $\dfrac{\neg\neg A}{A}$ *notnotD*

```
  from ... have "¬¬A" by ...
  hence "A" by (rule notnotD)
```

---

excluded_middle Rule: $\dfrac{}{\neg A \vee A}$ *excluded_middle*

```
  have "A ∨ ¬A" by (rule excluded_middle)
```