Mapping of ND proof templates to Isabelle formalization

Alexander Steen
April 25, 2016

1 ND rules and their Isabelle names

<table>
<thead>
<tr>
<th>Rule</th>
<th>Isabelle Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \frac{A \quad B}{A \land B} ) conjI</td>
<td>\textit{conjI}</td>
</tr>
<tr>
<td>( \frac{A}{A} )</td>
<td>\textit{conjunct1}</td>
</tr>
<tr>
<td>( \frac{A}{B} )</td>
<td>\textit{conjunct2}</td>
</tr>
<tr>
<td>( \frac{A}{A \lor B} ) disjI1</td>
<td>\textit{disjI1}</td>
</tr>
<tr>
<td>( \frac{B}{A \lor B} ) disjI2</td>
<td>\textit{disjI2}</td>
</tr>
<tr>
<td>( \frac{A \land B}{C} ) disjE</td>
<td>\textit{disjE}</td>
</tr>
<tr>
<td>( \frac{A \rightarrow B}{A} ) impI</td>
<td>\textit{impI}</td>
</tr>
<tr>
<td>( \frac{A \rightarrow B}{A} ) mp</td>
<td>\textit{mp}</td>
</tr>
<tr>
<td>( \frac{A}{\neg A} ) notI</td>
<td>\textit{notI}</td>
</tr>
<tr>
<td>( \frac{\neg A}{A} ) contr</td>
<td>\textit{contr}</td>
</tr>
<tr>
<td>( \frac{\neg \neg A}{A} ) notnotD</td>
<td>\textit{notnotD}</td>
</tr>
<tr>
<td>( \frac{\neg A \lor A}{A} ) excluded_middle</td>
<td>\textit{excluded_middle}</td>
</tr>
</tbody>
</table>

In Isabelle syntax

cnjI \( \frac{P \Rightarrow Q}{P \land Q} \)

conjunct1 \( \frac{P \land Q}{P} \)

conjunct2 \( \frac{P \land Q}{Q} \)

disjI1 \( \frac{P \Rightarrow P \lor Q}{Q} \)

disjI2 \( \frac{Q \Rightarrow P \lor Q}{P} \)

disjE \( \frac{P \lor Q \Rightarrow (P \Rightarrow R) \Rightarrow (Q \Rightarrow R) \Rightarrow R}{R} \)

imp1 \( \frac{P \Rightarrow Q \Rightarrow P \Rightarrow Q}{Q} \)

mp \( \frac{P \Rightarrow Q \Rightarrow P}{Q} \)

notI \( \frac{P \Rightarrow \text{False}}{\neg P} \)

notE \( \frac{\neg P \Rightarrow Q}{P \Rightarrow Q} \)
ccontr: \( \neg P \implies False \implies P \)

notnotD: \( \neg \neg P \implies P \)

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.

\begin{verbatim}
  thm notI this
\end{verbatim}

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)
  \begin{verbatim}
  lemma
    assumes "P"
    shows "..."
  proof -
    ...
    from assms have "P" by -
    moreover have ...
    ...
  qed
  \end{verbatim}
  (2) top-level introduction rule of proof
  \begin{verbatim}
  lemma
    ...
    proof -
    ...
  qed
  vs.
  lemma
    ...
    proof (rule disjI1)
    ...
  qed
  \end{verbatim}

note: Gives labels to blocks (and more?)

\begin{verbatim}
  { assume "P"
    from ... have "Q" by ...
  } note a = this
\end{verbatim}
gives the fact $P \implies Q$ the label a.

2.2 Within proofs

have   Add new fact to the collection of known facts:

\[
\text{from } a \ b \ c \ \text{have } "P" \ \text{by } ...
\]

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

\[
\text{from } \ldots \ \text{have } a: \ P \ \text{by } ...
\]
\[
\text{from } a \ \text{have } \ldots \ \text{by } ...
\]

is equivalent to

\[
\text{from } \ldots \ \text{have } P \ \text{by } ...
\]
\[
\text{from } \text{this} \ \text{have } \ldots \ \text{by } ...
\]

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

\[
\text{from } \ldots \ \text{have } a: \ P \ \text{by } ...
\]
\[
\text{from } \text{somefact} \ a \ \text{have } \ldots \ \text{by } ...
\]

is equivalent to

\[
\text{from } \ldots \ \text{have } P \ \text{by } ...
\]
\[
\text{with } \text{somefact} \ \text{have } \ldots \ \text{by } ...
\]

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

\[
\text{from } \ldots \ \text{have } P \ \text{by } ...
\]
\[
\text{then } \text{have } \ldots \ \text{by } ...
\]

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

\[
\text{from } \ldots \ \text{have } P \ \text{by } ...
\]
\[
\text{hence } \ldots \ \text{by } ...
\]

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

\[
\text{from } \ldots \ \text{have } "P" \ \text{by (rule conjunct1)}
\]
\[
\text{moreover from } \ldots \ \text{have } "Q" \ \text{by (rule conjunct1)}
\]
\[
\text{ultimately have } "P \land Q" \ \text{by (rule conjI)}
\]

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

\[
\text{from } a \ b \ c \ \text{show } "P" \ \text{by } ...
\]

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 $\vdash A \lor \neg A$

\textbf{theorem}

shows "$A \lor \neg A$"

\textbf{proof} -

\{ 
 assume a: "$\neg (A \lor \neg A)$"
\{
 assume "A"
 then have "$A \lor \neg A$" by (rule disjI1)
 with a have "False" by (rule notE)
\}
 hence "$\neg A$" by (rule notI)
 hence "$A \lor \neg A$" by (rule disjI2)
 with a have "False" by (rule notE)
\}
 hence "$\neg (A \lor \neg A)$" by (rule notI)
 thus "$A \lor \neg A$" by (rule notnotD)
qed

\section{ND proof templates}

For use within proofs to create new facts (with \textbf{have}):

\textbf{conjI} Rule: $\frac{A \quad B}{A \land B}$ \textit{conjI}

from ... have "A" by ...
moreover from ... have "B" by ...
ultimately have "A \land B" by (rule conjI)

\textbf{conjunct1} Rule: $\frac{A \land B}{A}$ \textit{conjunct1}

from ... have "A \land B" by ...
hence "A" by (rule conjunct1)

\textbf{conjunct2} Rule: $\frac{A \land B}{B}$ \textit{conjunct2}

from ... have "A \land B" by ...
hence "B" by (rule conjunct2)

\textbf{disjI1} Rule: $\frac{A}{A \lor B}$ \textit{disjI1}
from ... have "A" by ...
  hence "A ∨ B" by (rule disjI1)

\text{disjI2 Rule: } \frac{B}{A ∨ B} \quad \text{disjI2}

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

\text{disjE Rule: } \frac{[A] \quad [B]}{A ∨ B \quad \neg A \quad \neg B \quad \neg A ∨ \neg B} \quad \text{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)

\text{implI Rule: } \frac{[A] \quad : \quad : \quad [B]}{A \rightarrow B \quad \text{implI}}

{ 
  assume "A"
  ...
  from ... have "B" by ...
}
hence "A → B" by (rule implI)

\text{mp Rule: } \frac{A → B \quad A}{B} \quad \text{mp}

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

\text{notI Rule: } \frac{[A]}{\neg A \quad \text{notI}}

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

\[ \text{notE Rule: } \frac{\neg A}{B} \quad \text{notE} \]

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

\[ [\neg A] \]

\[ \text{ccontr Rule: } \frac{}{\bot} \quad \text{ccontr} \]

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

\[ \text{notnotD Rule: } \frac{\neg\neg A}{A} \quad \text{notnotD} \]

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

\[ \text{excluded middle Rule: } \frac{\neg A \lor A}{A} \quad \text{excluded middle} \]

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