Notes on PVS logic

Logical Implication

The proposition, “A implies B,” is written

\[ A \Rightarrow B \]

Other ways of saying \( A \Rightarrow B \) include “If A then B,” “B if A,” “A suffices for B,” and “A only if B.” The last of these is confusing to some, but what it says is that A cannot be true when B is false. The meaning of logical implication is

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>A \Rightarrow B</th>
</tr>
</thead>
<tbody>
<tr>
<td>false</td>
<td>false</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>false</td>
<td>true</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>true</td>
<td>false</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>true</td>
<td>true</td>
<td>true</td>
<td></td>
</tr>
</tbody>
</table>

Thus, no matter whether the proposition \( X \) is true or false, by the table above,

\[
\begin{align*}
\text{false} & \Rightarrow X \\
X & \Rightarrow \text{true} \\
X & \Rightarrow X
\end{align*}
\]

are each true.

Implication is used in three ways in formal logic. So as not to confuse these uses, different notations are used.

1. **Logical implication,** \( A \Rightarrow B \).

2. **Logical consequence,** \( A \vdash B \). If one assumes \( A \) holds \textit{then} one can deduce that \( B \) holds. In other words, there is a \textit{proof} that starts with \( A \) and ends with \( B \).

3. **Inference.** A logic is a system of rules for reasoning. Typically, inference rules are valid ways of reducing a proof \textit{goal} to one or more simpler \textit{subgoals}.

\[
\frac{\text{subgoal}_1, \ldots, \text{subgoal}_n}{\text{goal}}
\]

means, “In order to prove \textit{goal}, it suffices to prove each of the \( n \) subgoals.”

**Example.** The fundamental rule of classical logic is \textit{modus ponens}: “If \( P \) is true and \( P \Rightarrow Q \) is true then it follows that \( Q \) is true.” We terms of pure logical implication this is

\[ (P \land (P \Rightarrow Q)) \Rightarrow Q \]
Since the right-hand ‘⇒’ describes a consequence of reasoning, one might instead write
\[ P \land (P \Rightarrow Q) \vdash Q \]
or even
\[ P, P \Rightarrow Q \vdash Q \]
since by convention, all propositions to the left of the ‘⊢’ are conjoined (and’d).
Implication is transitive. A propositional form of Aristotle’s Rule of Syllogism, expressed as an inference rule, would be
\[
\begin{array}{c}
P \vdash Q \\
Q \vdash R \\
\hline
P \vdash R
\end{array}
\]
“If you can prove \( Q \) from \( P \) and \( R \) from \( Q \) then you can prove \( R \) from \( P \).”

**Sequents**

The *sequent*
\[ a_1, \ldots, a_m \vdash c_1, \ldots, c_n \]
says, “One one of consequents \( c_i \) is provable from all of the antecedents \( c_1, \ldots, c_n \).
Other ways to write this are
\[
(a_1 \land \cdots \land a_m) \Rightarrow (c_1 \lor \cdots \lor c_n)
\]
We often want to single out just one or two of the antecedents and consequents.
Let \( \Gamma = \{a_1, \ldots, a_m\} \) and \( \Delta = \{d_1, \ldots, d_n\} \). So the sequent above is written
\[ \Gamma \vdash \Delta \]
Suppose we want to focus on one antecedent, \( a \in \Gamma \), and one consequent, \( c \in \Delta \).
We write
\[ \Gamma, a \vdash c, \Delta \]

**Sequent Logic**

As we have seen, inference rules are expressed in terms of sequents.

\[
\frac{\Gamma_1 \vdash \Delta_1 \cdots \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta} \quad \text{NAME}(R)
\]
Translation: Rule NAME: “If you want to prove $\Gamma \vdash \Delta$, it suffices to prove each of $\Gamma_1 \vdash \Delta_1$, $\ldots$, $\Gamma_n \vdash \Delta_n$, provided side condition $R$ is satisfied.

An example of a side condition is, “You can’t introduce a variable that is already in use.”

A completed proof in the sequent calculus is a

A proof in the sequent calculus is a tree, whose root is the original goal, and whose interior nodes represent the application of an inference rule.

\[
\begin{array}{cccc}
\vdots & \vdots & \vdots & \vdots \\
G_{2,1,1} & G_{2,1,2} & \vdots & \vdots \\
G_2 & \vdots & G_3 \\
G_1 & \vdots & \\
\end{array}
\]

Terminal Rules

There are three:

$\Gamma, false \vdash \Delta$ \hspace{1cm} $\Gamma \vdash true, \Delta$ \hspace{1cm} $\Gamma, A \vdash A, \Delta$

The first two are easy to understand. If one of the antecedents is false, then so is the conjunction of all the antecedents. So the left-most rule reduces to

$false \Rightarrow \bigwedge \Delta$

which is tautologically true. Similarly, if any of the consequents is true the disjunction of all the consequents is also true and the center rule reduces to

$\bigvee \Gamma \Rightarrow true$

Stated informally, the right-hand rule says, “If one of the propositions you assume is $P$, then $P$ is one of the things you may conclude.

Structural Rules

The structural say things like, “the order of antecedents and consequents doesn’t matter,” and “duplicating antecedents and consequents doesn’t matter.” An important structural rule is weakening,

$\Gamma_1 \vdash \Delta_1 \quad \Gamma_2 \vdash \Delta_2 \quad \Gamma_1 \subseteq \Gamma_2 \text{ and } \Delta_1 \subseteq \Delta_2$

That is, is all right to have extra antecedents and consequents.
Propositional Rules

Each of the propositional says how you can reduce a sequent by eliminating one of the logical connectives. This may result in more subgoals, but they are all smaller. The goals can’t become smaller and smaller indefinitely, so eventually all the logical operations can be eliminated.

\[
\begin{align*}
\Gamma \vdash A, \Delta & \quad \Gamma, A \vdash \Delta \\
\Gamma \vdash \neg A, \Delta & \\
\Gamma, A, B \vdash \Delta & \quad \Gamma \vdash A, B, \Delta \\
\Gamma, A \land B \vdash \Delta & \quad \Gamma \vdash A \lor B, \Delta \\
\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta & \quad \Gamma, A \vdash \Delta, \Delta \\
\Gamma \vdash A \land B, \Delta & \quad \Gamma, A \vdash \Delta, B \\
\Gamma, A \lor B \vdash \Delta & \\
\end{align*}
\]

The rules for implication and bi-implication follow because \( A \Rightarrow B \) is logically equivalent to \( \neg A \lor B \) and \( A \iff B \) is logically equivalent to \((A \Rightarrow B) \land (B \Rightarrow A)\).

The Cut Rule

\[
\begin{align*}
\Gamma, A \vdash \Delta & \quad \Gamma \vdash A, \Delta \\
\Gamma \vdash \Delta & \quad \text{cut}
\end{align*}
\]

The cut rule derives from the fact that one may always add a true proposition to the antecedent. Consider adding the tautologically true proposition \( \Gamma, (A \lor \neg A) \vdash \Delta \). An \( \lor \)-rule decomposes this into subgoals \( \Gamma, A \vdash \Delta \) and \( \Gamma, \neg A \vdash \Delta \). The \( \neg \)-rule changes the subgoals to \( \Gamma, A \vdash \Delta \) and \( \Gamma \vdash A, \Delta \).

Quantification

\( A \{N \leftarrow x\} \) denotes substituting \( N \) for \( x \) in \( A \), that is,

(a) Replacing all free occurrences of \( x \) with \( N \)

(b) ... possibly changing the variables in \( N \) to avoid free variable capture.

Let \( t \) be a value.
Let $a$ be a name that appears nowhere else in the sequent, a “Skolem constant”.

\[
\begin{align*}
\Gamma, A\{t \leftarrow x\} & \vdash \Delta \\
\Gamma, \forall x : A & \vdash \Delta \\
\Gamma & \vdash A\{t \leftarrow x\}, \Delta \\
\Gamma & \vdash \exists x : A, \Delta
\end{align*}
\]

Example. Below, a mathematical proof is compared to its corresponding formal deduction.

**Definition.** $n \in \mathbb{N}$ is even if there exists a $q$ such that $n = 2q$.

**Theorem** If $n$ and $m$ are even, then so is $n + m$.

**Proof.** If $n$ is even then $n = 2k$ for some $k$, and if $m$ is even then $m = 2\ell$ for some $\ell$. Hence,

\[
m + n = 2k + 2\ell = 2(k + \ell)
\]

Therefore, $m + n$ is even.
\[(\exists q : (n + m) = 2q) \vdash (\exists q : (n + m) = 2q)\]

\[(m + n = 2(k + \ell) \vdash (\exists q : (n + m) = 2q)\]

\[(\vdots)\]

\[(m = 2\ell, n = 2k \vdash (\exists q : (n + m) = 2q)\]

\[(m = 2\ell, (\exists q : n = 2q) \vdash (\exists q : (n + m) = 2q)\]

\[(\exists q : m = 2q), (\exists q : n = 2q) \vdash (\exists q : (n + m) = 2q)\]

\[even?(m), even?(n) \vdash even?(n + m)\]
PVS commands

\[
\begin{align*}
\Gamma &\vdash A, \Delta \\
\Gamma &\vdash \neg A, \Delta & \quad \text{自动} \\
\end{align*}
\]

\[
\frac{\Gamma, A, B \vdash \Delta}{\Gamma, A \land B \vdash \Delta} & \quad \text{(FLATTEN}\ n) \\
\frac{\Gamma \vdash A, \Delta}{\Gamma, A \lor B \vdash \Delta} & \quad \text{(SPLIT} \ n) \\
\end{align*}
\]

\[
\frac{\Gamma, A \{t \leftarrow x\} \vdash \Delta}{\Gamma, \forall x : A \vdash \Delta} & \quad \text{(INST}\ n \ t) \\
\frac{\Gamma, A \{a \leftarrow x\} \vdash \Delta}{\Gamma, \forall x : A \vdash \Delta} & \quad \text{(SKOLEM}\ n \ a)
\]

Copyright © 2003 Steven D. Johnson  Draft Material  January 18, 2011
### Implication

\[
\begin{array}{c}
\Gamma \vdash A, \Delta \\
\hline
\Gamma, \neg A \vdash \Delta \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\Gamma, A, B \vdash \Delta \\
\hline
\Gamma, A \land B \vdash \Delta \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\Gamma, A, B, \Delta \\
\hline
\Gamma \vdash A \lor B, \Delta \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\Gamma, A, \Delta, B \vdash \Delta \\
\hline
\Gamma, A \Rightarrow B \rightarrow \Gamma, \Delta \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\Gamma, A, \Delta, B \vdash \Delta \\
\hline
\Gamma, A \land B \vdash \Delta \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\Gamma, A, \Delta, B, \Gamma \vdash \Delta \\
\hline
\Gamma, A \Rightarrow B \rightarrow \Gamma, \Delta \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\Gamma, A \{t \leftarrow x\} \vdash \Delta \\
\hline
\Gamma, \forall x : A \vdash \Delta \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\Gamma, A \{t \leftarrow x\} \vdash \Delta \\
\hline
\Gamma \vdash A \{t \leftarrow x\}, \Delta \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\Gamma \vdash A \{a \leftarrow x\} \Delta \\
\hline
\Gamma, A \{a \leftarrow x\} \vdash \Delta \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\Gamma, A \{a \leftarrow x\} \vdash \Delta \\
\hline
\Gamma, \exists x : A \vdash \Delta \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\Gamma, A \{a \leftarrow x\} \vdash \Delta \\
\hline
\Gamma, \forall x : A \vdash \Delta \\
\hline
\end{array}
\]

\[
\begin{array}{c}
\Gamma, A \{a \leftarrow x\} \vdash \Delta \\
\hline
\Gamma, \exists x : A \vdash \Delta \\
\hline
\end{array}
\]