1 Lecture 5 (2/3/2011)

Key Terms: Theorem, Proof, Modus Ponens,
Key Symbols: ⊢

1.1 Proofs

Definition 1 A theorem is a statement of the form "If \( H_1, \ldots, H_n \) are true then \( Q \) is true". Here the \( H_i \) are propositions called hypotheses and \( Q \) is a proposition called the conclusion.

Definition 2 A proof of a theorem is a list of propositions \( P_1, P_2, \ldots, P_k \), where the last proposition is \( P_k = Q \), and each \( P_i \) is one of the following:

1. A hypothesis \((H)\)
2. A tautology \((T)\)
3. Obtained from two preceding propositions by the Modus Ponens rule \((M)\)

The Modus Ponens rule simply says "if the propositions \( A \) and \( A \Rightarrow B \) have previously occurred in the list then we are allowed to write down \( B \)".

It is a good idea to think of \( P_1, P_2, \ldots, P_k \) as the moves of a solitaire game (or a maze) in which objective is to reach the conclusion \( Q \). Conditions 1, 2, 3 are the rules of the game that tell us whether a move is legal or not.

If \( Q \) is provable from \( H_1, \ldots, H_n \) then we write

\[
H_1, \ldots, H_n \vdash Q.
\]

We now look at some simple examples.

**Theorem 3 (E)** If \( P \), "\( P \) is equivalent to \( Q \)" are true then \( Q \) is true.

**Proof.**

\[
\begin{array}{c|c|c|c|c|c}
P & P \Leftrightarrow Q & (P \Leftrightarrow Q) \Rightarrow (P \Rightarrow Q) & P \Rightarrow Q & Q \\
\hline
H & H & T & M & M
\end{array}
\]

**Theorem 4 (C)** If \( P, Q \) are true then \( P \land Q \) is true.

**Proof.**

\[
\begin{array}{c|c|c|c|c|c}
P & Q & P \Rightarrow (Q \Rightarrow (P \land Q)) & Q \Rightarrow (P \land Q) & P \land Q \\
\hline
H & H & T & M & M
\end{array}
\]

We can use the above theorems to shorten other proofs.

**Theorem 5 (O)** If \( \neg P, P \lor Q \) are true then \( Q \) is true.

**Proof.**

\[
\begin{array}{c|c|c|c|c|c}
\neg P & P \lor Q & (\neg P) \land (P \lor Q) & (\neg P) \land (P \lor Q) \Rightarrow Q & Q \\
\hline
H & H & C & T & M
\end{array}
\]

In all cases the central tautology of the proof is easily verified.
1.2 Exercises

For the first two exercises, use a truth table:

1. Verify the tautologies of Theorems E, C, O.

2. Show that \((P \land Q) \land R\) and \(P \land (Q \land R)\) are equivalent.

The next two exercises are a formalized version of Ex 1.4.4. in the text, and should be proved in a manner similar to Theorems O. You can use Theorems E,C,O to shorten your proofs. In each case only state the hypotheses you need.

Consider the statements

\[ \neg P \Rightarrow K, M \Rightarrow P, C \Rightarrow \neg S, \neg S \Rightarrow C, C \lor L, S \lor P \]

and prove the following theorems:

3. If the above statements and \(\neg L\) are true then \(P\) is true.

4. If the above statements and \(\neg M, \neg C\) are true then \(P\) is true.