Programming Theory

Tutorial 1: Proof Theory

September 16, 2009

1 Proof Methods

Method 1: To prove \( p \) (or to “prove that \( p \) is a tautology”),
prove that \( p = T \) (i.e. \( p = \ldots = T \)).

Example 1.1 Prove \( p \Rightarrow (p \lor q) \).

Proof:

\[
\begin{align*}
p \Rightarrow (p \lor q) \\
= & \{ \text{Implication} \} \\
= & \neg p \lor p \lor q \\
= & \{ \text{Excluded Middle} \} \\
= & T \lor q \\
= & \{ \text{or-simplification} \} \\
= & T \\
\end{align*}
\]

Method 2: To prove that \( p = q \), prove that \( p = \ldots = q \) (or \( q = \ldots = p \)).

Example 1.2 Prove \( p \Rightarrow F = \neg p \).

Proof:

\[
\begin{align*}
p \Rightarrow F \\
= & \{ \text{Implication} \} \\
= & \neg p \lor F \\
= & \{ \text{or-simplification} \} \\
= & \neg p \\
\end{align*}
\]

Method 3: To prove \( p_1 \land \ldots \land p_n \Rightarrow q \), assume \( p_1, \ldots, p_n \) and prove \( q \).

Example 1.3 Prove \( p \land q \Rightarrow q \).

Assume \( p \)
Assume \( q \)
Prove: $q$

Proof:

\[
q = \{ \text{Assumption: “q”} \}
T \quad \square
\]

**Example 1.4** Prove $(p \land (p \Rightarrow q) \Rightarrow r) \land p \land q \Rightarrow r$.

Assume $p \land (p \Rightarrow q) \Rightarrow r$
Assume $p$
Assume $q$

Prove: $r$

Proof:

\[
r = \{ \text{Left identity of } \Rightarrow \}
T \Rightarrow r
= \{ \text{and-simplification} \}
(T \land T) \Rightarrow r
= \{ \text{Assumptions: “p” and “q”} \}
(p \land q) \Rightarrow r
= \{ \text{Introduction of } \Rightarrow \}
(p \land (p \Rightarrow q)) \Rightarrow r
= \{ \text{Assumption: “(p \land (p \Rightarrow q)) \Rightarrow r”} \}
T \quad \square
\]

1.1 Some Good Advice

- **Write lemmas!** State your lemma, then prove it. Make sure to write it separate from the main proof.

- Clearly state your assumptions.

- Do not perform any non-obvious steps and do not skip too many steps.

- **Think!** Do *not* just randomly apply rules and see where they take you. Always have a proof strategy in mind, and always have a clear goal that you work towards. It helps if you take the time to understand the meaning of the expressions you are working with - to this end, it is often helpful to first develop an informal proof, and then move on to a formal proof which mimics the structure of your informal proof.

2 Transforming sentences (in english) to formulas and proving them

**Example 2.1** Formulate and prove *proof by contradiction,*
"Assume $p$ is false and derive a contradiction"

The sentence is transformed into the formula $(p = F) \Rightarrow F \Rightarrow p$. We prove it using method 1:

**Proof:**

$$(p = F) \Rightarrow F \Rightarrow p$$

$$= \{ \text{Definition of } \neg \}$$

$$\neg p \Rightarrow F \Rightarrow p$$

$$= \{ \text{Example 1.2: } p \Rightarrow F = \neg p \}$$

$$\neg\neg p \Rightarrow p$$

$$= \{ \text{Negation} \}$$

$$p \Rightarrow p$$

$$= \{ \text{Implication} \}$$

$$\neg p \vee p$$

$$= \{ \text{Excluded Middle} \}$$

$$T \square$$

**Example 2.2** Formulate and prove *contrapositive/indirect* proof,

"To prove $p \Rightarrow q$, prove that $\neg q \Rightarrow \neg p$"

The sentence is transformed into the formula $(\neg p \Rightarrow \neg q) \Rightarrow (q \Rightarrow p)$. We prove the stronger version $(\neg p \Rightarrow \neg q) = q \Rightarrow p$ using method 2:

**Proof:**

$$\neg p \Rightarrow \neg q$$

$$= \{ \text{Implication} \}$$

$$\neg p \neg p \vee \neg q$$

$$= \{ \text{Negation} \}$$

$$p \vee \neg q$$

$$= \{ \text{Commutativity} \}$$

$$\neg q \vee p$$

$$= \{ \text{Implication} \}$$

$$q \Rightarrow p \square$$

**2.0.1 Formal Specification**

**Example 2.3**

**English Specification:** “The array $A$ of length $N$ is indexed by $1..N$. The procedure searches this array for a value $X$. If it finds the element then $Y$ is set to be equal to the index of the array element that is equal to $X$. If there is no element of the array equal to $X$ then $Y$ is set equal to 0.”
Formal Specification:

pre-condition: $N > 0$

post-condition: $\left( \begin{array}{c} X = A[Y] \land 1 \leq Y \leq N \\ \lor \\ Y = 0 \land \forall k : (1 \leq k \leq N) \Rightarrow A[k] \neq X \end{array} \right)$

3 Predicate Logic & Arrays

Example 3.1 Prove

$\left( m < n \right) \Rightarrow (\left( \sum i : m \leq i < n : b[i] \right) = x)$

$(m < n) \Rightarrow (\left( \sum i : m \leq i < n - 1 : b[i] \right) + b[n - 1] = x)$

Lemma:

$\left( m < n \right) \Rightarrow \left( \begin{array}{c} (\sum i : m \leq i < n : b[i]) = x \\ \left( \sum i : m \leq i < n - 1 : b[i] \right) + b[n - 1] = x \end{array} \right)$

Proof of lemma:

Assume $m < n$

$\left( \sum i : m \leq i < n : b[i] \right) = x$

$\left( \sum i : m \leq i < n : b[i] \right) = T \land \left( \sum i : m \leq i < n : b[i] \right) = x$

$\left( \sum i : m \leq i < n - 1 : b[i] \right) + b[n - 1] = x$

Assumption: "$m < n$"

$T \Rightarrow \left( \begin{array}{c} \sum i : m \leq i < n : b[i] \\ \left( \sum i : m \leq i < n - 1 : b[i] \right) + b[n - 1] \end{array} \right)$

$\left( \sum i : m \leq i < n : b[i] \right) = x$

$\left( \sum i : m \leq i < n - 1 : b[i] \right) + b[n - 1] = x$

Left identity of $\Rightarrow$

$\left( \begin{array}{c} \sum i : m \leq i < n : b[i] \\ \left( \sum i : m \leq i < n - 1 : b[i] \right) + b[n - 1] \end{array} \right)$

$\left( \sum i : m \leq i < n : b[i] \right) = x$
\[ \sum_{i : m \leq i < n} b[i] = (\sum_{i : m \leq i < n-1} b[i]) + b[n-1] = x \]

Main proof:
\[ (m < n) \Rightarrow ((\sum_{i : m \leq i < n} b[i]) = x) \]
\[ (m < n) \Rightarrow ((\sum_{i : m \leq i < n-1} b[i]) + b[n-1] = x) \]
\[ (m < n) \Rightarrow (\sum_{i : m \leq i < n} b[i] = x) \]
\[ (m < n) \Rightarrow (\sum_{i : m \leq i < n-1} b[i]) + b[n-1] = x \]
\[ T \]

Example 3.2 The lemma from example 3.1 proved using conditional substitution:

Lemma:
\[ (m < n) \Rightarrow ((\sum_{i : m \leq i < n} b[i]) = x) \]
\[ (\sum_{i : m \leq i < n-1} b[i]) + b[n-1] = x \]
Proof of lemma: Assume \( m < n \)

\[
\sum_{i : m \leq i < n : b[i]} = x
\]

\[
= \{ \text{Conditional Substitution: Assumption: } m < n \text{ and Definition of } \Sigma \} \\
\sum_{i : m \leq i < n - 1 : b[i]} + b[n - 1] = x \quad \square
\]