Proving implications with (3.82)

Suppose you know that $a = b$ and $b > c$ and $c = d$.

Because $>$ and $=$ are together transitive, you can prove that $a > d$ like this.

Proof

$$
\begin{array}{ll}
 & a \\
= & \langle a = b \rangle \\
 & b \\
> & \langle b > c \rangle \\
 & c \\
= & \langle c = d \rangle \\
 & d \quad //
\end{array}
$$

Proving implications with (3.82)

(3.82) **Transitivity:**

(a) $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$

(b) $(p \equiv q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$

(c) $(p \Rightarrow q) \wedge (q \equiv r) \Rightarrow (p \Rightarrow r)$

Proving implications with (3.82)

Prove (4.2) $(p \Rightarrow q) \Rightarrow (p \vee r \Rightarrow q \vee r)$

Proof

$$
\begin{array}{ll}
 & p \vee r \Rightarrow q \vee r \\
= & \langle (3.57) \rangle \\
 & p \vee r \vee q \vee r \equiv q \vee r \\
= & \langle (3.26) \rangle \\
 & p \vee q \vee r \equiv q \vee r \\
= & \langle (3.27) \rangle \\
 & (p \vee q \equiv q) \vee r \\
= & \langle (3.57) \rangle \\
 & (p \Rightarrow q) \vee r \\
\Leftarrow & \langle (3.76a)\ p \Rightarrow p \vee q \rangle \\
 & (p \Rightarrow q) \quad //
\end{array}
$$

(4.2) **Monotonicity of $\vee$:** $(p \Rightarrow q) \Rightarrow (p \vee r \Rightarrow q \vee r)$

(4.3) **Monotonicity of $\wedge$:** $(p \Rightarrow q) \Rightarrow (p \wedge r \Rightarrow q \wedge r)$

Monotonicity is necessary in some proof steps.

<u>Example</u>

Suppose you have $p \wedge s$.

Then the following proof step is legal.

$p \wedge s$

$\Rightarrow$ $\langle$(3.76a) $p \Rightarrow p \vee q$ and (4.3) Monotonicity of $\wedge\rangle$

$(p \vee q) \wedge s$

(4.2) **Monotonicity of $\vee$:** $(p \Rightarrow q) \Rightarrow (p \vee r \Rightarrow q \vee r)$

(4.3) **Monotonicity of $\wedge$:** $(p \Rightarrow q) \Rightarrow (p \wedge r \Rightarrow q \wedge r)$

<u>Example</u>

Suppose you have $p \vee (s \equiv r)$.

Then the following proof step is legal.

$$
\begin{array}{ll}
 & p \vee (s \equiv r) \\
\Rightarrow & \langle \text{(3.76a) } p \Rightarrow p \vee q \text{ and (4.2) Monotonicity of } \vee \rangle \\
 & (p \vee q) \vee (s \equiv r)
\end{array}
$$

A Logical Approach to Discrete Math

(4.2) **Monotonicity of $\vee$:** $(p \Rightarrow q) \Rightarrow (p \vee r \Rightarrow q \vee r)$

(4.3) **Monotonicity of $\wedge$:** $(p \Rightarrow q) \Rightarrow (p \wedge r \Rightarrow q \wedge r)$

Using Monotonicity of $\vee$ in a proof step.

$$\begin{array}{ll} & p \vee r \\ \Rightarrow & \langle \text{Why } p \Rightarrow q \text{ and (4.2) Monotonicity of } \vee \rangle \\ & q \vee r \end{array}$$

Using Monotonicity of $\wedge$ in a proof step.

$$\begin{array}{ll} & p \wedge r \\ \Rightarrow & \langle \text{Why } p \Rightarrow q \text{ and (4.3) Monotonicity of } \wedge \rangle \\ & q \wedge r \end{array}$$

(4.2) **Monotonicity of** $\vee$ **:** $(p \Rightarrow q) \Rightarrow (p \vee r \Rightarrow q \vee r)$

(4.3) **Monotonicity of** $\wedge$ **:** $(p \Rightarrow q) \Rightarrow (p \wedge r \Rightarrow q \wedge r)$

<u>Caution</u>

$\equiv$ is **not** monotonic.

Suppose you have $p \equiv r \vee s$.

Then the following proof step is **not** legal.

$$\begin{array}{ll} & p \equiv r \vee s \\ \Rightarrow & \langle (3.76a)\ p \Rightarrow p \vee q \rangle \\ & p \vee q \equiv r \vee s \end{array}$$

(4.2) **Monotonicity of $\vee$:** $(p \Rightarrow q) \Rightarrow (p \vee r \Rightarrow q \vee r)$

(4.3) **Monotonicity of $\wedge$:** $(p \Rightarrow q) \Rightarrow (p \wedge r \Rightarrow q \wedge r)$

<u>Caution</u>

$\neg$ is **not** monotonic.

Suppose you have $\neg(p \wedge q)$.

Then the following proof step is **not** legal.

$$
\begin{array}{ll}
 & \neg(p \wedge q) \\
\Rightarrow & \langle (3.76c)\ p \wedge q \Rightarrow p \vee q \rangle \\
 & \neg(p \vee q)
\end{array}
$$

Proof techniques

Proof techniques

Metatheorem: A theorem about theorems.

Proof techniques: Technically, it is legal to use these proof techniques only after Chapter 4.

Reproofs: Because they make good exercises, we will illustrate the proof techniques by re-proving previous theorems. Strictly speaking, they are not legitimate proofs.

(4.4) **Deduction (assume conjuncts of antecedent):**
To prove $P_1 \wedge P_2 \Rightarrow Q$, assume P_1 and P_2, and prove Q.
You cannot use textual substitution in P_1 or P_2.

Prove $(p \wedge q) \Rightarrow (p \equiv q)$

Proof: Deduction

$$
\begin{array}{ll}
& p \equiv q \\
= & \langle \text{Assume conjunct } p \rangle \\
& true \equiv q \\
= & \langle \text{Assume conjunct } q \rangle \\
& true \equiv true
\end{array}
$$

which is (3.5) Reflexivity //

(4.5) **Case analysis:** If E^z_{true} and E^z_{false} are theorems, then so is E^z_P.

(3.89) **Shannon:** $E^z_p \equiv (p \wedge E^z_{true}) \vee (\neg p \wedge E^z_{false})$

(3.89.1) $E^z_{true} \wedge E^z_{false} \Rightarrow E^z_p$

(4.5) **Case analysis:** If E^z_{true} and E^z_{false} are theorems, then so is E^z_P.

Re-prove (3.80) Mutual implication: $(p \Rightarrow q) \wedge (q \Rightarrow p) \equiv (p \equiv q)$

Proof: Case analysis on p

Case 1. $(true \Rightarrow q) \wedge (q \Rightarrow true) \equiv (true \equiv q)$

Case 2. $(false \Rightarrow q) \wedge (q \Rightarrow false) \equiv (false \equiv q)$

Case 1 proof:

$$
\begin{array}{ll}
 & (true \Rightarrow q) \wedge (q \Rightarrow true) \\
= & \langle (3.73) \rangle \\
 & q \wedge (q \Rightarrow true) \\
= & \langle (3.72) \rangle \\
 & q \wedge true \\
= & \langle (3.39) \rangle \\
 & q \\
= & \langle (3.3) \rangle \\
 & true \equiv q \quad //
\end{array}
$$

A Logical Approach to Discrete Math

(4.5) **Case analysis:** If E^z_{true} and E^z_{false} are theorems, then so is E^z_P.

Re-prove (3.80) Mutual implication: $(p \Rightarrow q) \wedge (q \Rightarrow p) \;\equiv\; (p \equiv q)$

Proof: Case analysis on p

Case 1. $(true \Rightarrow q) \wedge (q \Rightarrow true) \;\equiv\; (true \equiv q)$

Case 2. $(false \Rightarrow q) \wedge (q \Rightarrow false) \;\equiv\; (false \equiv q)$

Case 2 proof:

$$
\begin{array}{ll}
& (false \Rightarrow q) \wedge (q \Rightarrow false) \\
= & \langle (3.75) \rangle \\
& true \wedge (q \Rightarrow false) \\
= & \langle (3.39) \rangle \\
& q \Rightarrow false \\
= & \langle (3.74) \rangle \\
& \neg q \\
= & \langle (3.15) \rangle \\
& false \equiv q \quad //
\end{array}
$$

(3.89) **Shannon:** $E^z_p \equiv (p \wedge E^z_{true}) \vee (\neg p \wedge E^z_{false})$

(3.89.1) $E^z_{true} \wedge E^z_{false} \Rightarrow E^z_p$

Prove (3.89.1) $E^z_{true} \wedge E^z_{false} \Rightarrow E^z_p$

Proof: Deduction

$$
\begin{array}{ll}
 & E^z_p \\
= & \langle (3.89 \text{ Shannon}) \rangle \\
 & (p \wedge E^z_{true}) \vee (\neg p \wedge E^z_{false}) \\
= & \langle \text{Assume conjunct } E^z_{true} \rangle \\
 & (p \wedge true) \vee (\neg p \wedge E^z_{false}) \\
= & \langle (3.39) \rangle \\
 & p \vee (\neg p \wedge E^z_{false}) \\
= & \langle \text{Assume conjunct } E^z_{false} \rangle \\
 & p \vee (\neg p \wedge true) \\
= & \langle (3.39) \rangle \\
 & p \vee \neg p \\
= & \langle (3.28) \text{ Excluded middle} \rangle \\
 & true \quad //
\end{array}
$$

(4.9) **Proof by contradiction:** To prove P, prove $\neg P \Rightarrow false$.

(4.9.1) **Proof by contradiction:** To prove P, prove $\neg P \equiv false$.

$$(3.74.1) \quad \neg p \Rightarrow false \equiv p$$

(4.9) **Proof by contradiction:** To prove P, prove $\neg P \Rightarrow false$.

(4.9.1) **Proof by contradiction:** To prove P, prove $\neg P \equiv false$.

Re-prove (3.15) $\neg p \equiv p \equiv false$

Proof: Contradiction

$$
\begin{array}{ll}
 & \neg(\neg p \equiv p \equiv false) \\
= & \langle (3.9) \rangle \\
 & \neg\neg p \equiv p \equiv false \\
= & \langle (3.12) \rangle \\
 & p \equiv p \equiv false \\
= & \langle (3.3) \rangle \\
 & true \equiv false \\
= & \langle (3.3) \rangle \\
 & false \quad //
\end{array}
$$

(4.12) **Proof by contrapositive:** To prove $P \Rightarrow Q$, prove $\neg Q \Rightarrow \neg P$.

(3.61) **Contrapositive:** $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$

(4.12) **Proof by contrapositive:** To prove $P \Rightarrow Q$, prove $\neg Q \Rightarrow \neg P$.

Re-prove (3.76b) $p \wedge q \Rightarrow p$

Proof: Contrapositive $\neg p \Rightarrow \neg(p \wedge q)$

$$
\begin{array}{ll}
 & \neg(p \wedge q) \\
= & \langle \text{(3.47a) De Morgan} \rangle \\
 & \neg p \vee \neg q \\
\Leftarrow & \langle \text{(3.76a)} \rangle \\
 & \neg p \quad //
\end{array}
$$