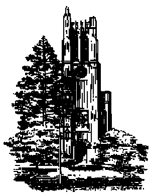
Tuesday May 24, 2016
Lecture 06

Proof Techniques



Notables

- Homework#4
  - Page 78, Problem 4
  - Page 80, Problem 20, and 24
  - Page 91, Problem 6, and 8
  - Due Thursday May 26, 2016
- Read Chapter 2
- Tentative Schedule for the week

Week	M	T	W	R	Topic	Section
1	5-23				Nested Quantifiers, Rules of Inference	1.5, 1.6
		5-23			Proof	1.7
			5-25		Proofs, Sets	1.8
				5-26	Sets	2.1

Proof Methods (Does p *logically imply* c)

		Direct	*Contrapositive*	*Contradiction*
p	c	$p \to c$	$\neg c \to \neg p$	$p \wedge \neg c$
T	T	T	T	F
T	F	F	F	T
F	T	T	T	F
F	F	T	T	F

Example

- Let
  $h_1 = q \vee d$
  $h_2 = (q \vee d\,) \to \neg\, p$
  $h_3 = \neg\, p \to (a \wedge \neg\, b)$
  $h_4 = (a \wedge \neg\, b) \to (r \vee s)$
  $c = r \vee s$

  we want to establish $h_1 \wedge h_2 \wedge h_3 \wedge h_4 \Rightarrow c$.

Solution 1

- Let
  $h_1 = q \vee d$ $\quad h_2 = (q \vee d\,) \to \neg\, p$
  $h_3 = \neg\, p \to (a \wedge \neg\, b)$ $\quad h_4 = (a \wedge \neg\, b) \to (r \vee s)$
  $c = r \vee s$
  we want to establish $h_1 \wedge h_2 \wedge h_3 \wedge h_4 \Rightarrow c$.

1. $(q \vee d\,) \to \neg\, p$ — Premise
2. $\neg\, p \to (a \wedge \neg\, b)$ — Premise
3. $(q \vee d\,) \to (a \wedge \neg\, b)$ — 1&2, Hypothetical Syllogism
4. $(a \wedge \neg\, b) \to (r \vee s)$ — Premise
5. $(q \vee d\,) \to (r \vee s)$ — 3&4, HS
6. $q \vee d$ — Premise
7. $r \vee s$ — 5&6, Modus Ponens

Solution 2

- Let
  $h_1 = q \vee d$ $\quad h_2 = (q \vee d\,) \to \neg\, p$
  $h_3 = \neg\, p \to (a \wedge \neg\, b)$ $\quad h_4 = (a \wedge \neg\, b) \to (r \vee s)$
  $c = r \vee s,$
  we want to establish $h_1 \wedge h_2 \wedge h_3 \wedge h_4 \Rightarrow c$.

1. $q \vee d$ — Premise
2. $(q \vee d\,) \to \neg\, p$ — Premise
3. $\neg\, p$ — 1&2, and modus ponens
4. $\neg\, p \to (a \wedge \neg\, b)$ — Premise
5. $(a \wedge \neg\, b)$ — 3&4, modus ponens
6. $(a \wedge \neg\, b) \to (r \vee s)$ — Premise
7. $r \vee s$ — 5&6, modus ponens

© 2016 by A-H. Esfahanian. All Rights Reserved.

Example

- Question: Is
  $[(\neg (p \wedge q)) \rightarrow (\neg p \vee q)] \equiv (\neg p \vee q)$?
- Different ways to answer the above question
  1. By means of the Truth Table.
  2. By means of derivation.
  3. By formulating it as a logical implication, that is, as a "proof".

164

Is $[(\neg (p \wedge q)) \rightarrow (\neg p \vee q)] \equiv (\neg p \vee q)$?
Truth Table Method

p	q	$\neg (p \wedge q)$	$(\neg p \vee q)$	LHS	RHS	Answer
T	T	F	T	T	T	YES
T	F	T	F	F	F	YES
F	T	T	T	T	T	YES
F	F	T	T	T	T	YES

165

Is $[(\neg (p \wedge q)) \rightarrow (\neg p \vee q)] \equiv (\neg p \vee q)$?
Derivation Method

$$
\begin{aligned}
(\neg (p \wedge q)) \rightarrow (\neg p \vee q) &\equiv \neg(\neg (p \wedge q)) \vee (\neg p \vee q) && \text{EQ} \\
&\equiv (p \wedge q) \vee (\neg p \vee q) && \text{DM} \\
&\equiv ((p \wedge q) \vee \neg p) \ \vee q \\
&\equiv (\neg p \vee (p \wedge q)) \ \vee q \\
&\equiv ((\neg p \vee p) \wedge (\neg p \vee q)) \vee q \\
&\equiv ((\mathrm{T}) \wedge (\neg p \vee q)) \ \vee q \\
&\equiv (\neg p \vee q) \ \vee q \\
&\equiv (\neg p) \vee \ (q \vee q) \\
&\equiv (\neg p) \vee \ (q) \\
&\equiv (\neg p \vee \ q)
\end{aligned}
$$

166

Is $[(\neg (p \wedge q)) \rightarrow (\neg p \vee q)] \equiv (\neg p \vee q)$?
Logical Implication Method

Let S and R be wffs. To show that $S \equiv R$ it suffices to show that

$S \Rightarrow R$ and

$R \Rightarrow S$

In this case, we have

$S = [\neg (p \wedge q)) \rightarrow (\neg p \vee q)]$ and

$R = (\neg p \vee q)$

167

Does $[(\neg (p \wedge q)) \rightarrow (\neg p \vee q)] \Rightarrow (\neg p \vee q)$?

1.	$(\neg (p \wedge q)) \rightarrow (\neg p \vee q)$	Premise
2.	p	*Assumption* (p=*F*, NTP)
3.	$\neg q \rightarrow q$	2 &1,simplification
4.	q	3
5.	$\mathrm{F} \vee q$	*4 & …*
6.	$\neg p \vee q$	

p	q	$\neg (p \wedge q)$	$(\neg p \vee q)$	LHS	RHS
T	T	F	T	T	T
T	F	T	F	F	F
F	T	T	T	T	T
F	F	T	T	T	T

168

Does $(\neg p \vee q) \Rightarrow (\neg (p \wedge q)) \rightarrow (\neg p \vee q)$?

1.	$(\neg p \vee q)$	Conclusion stays True
2.	$s \rightarrow (\neg p \vee q)$	1 & property of $\rightarrow$, for any s
3.	$(\neg (p \wedge q)) \rightarrow (\neg p \vee q)$	

- So, we have established that
  $[(\neg (p \wedge q)) \rightarrow (\neg p \vee q)] \equiv (\neg p \vee q)$

169

© 2016 by A-H. Esfahanian. All Rights Reserved.

Example

- Is the following reasoning logical?
  - It is a fact that if you are poor then you have no money. It is also a fact that if you have money then you are not poor. Therefore, being poor is the same as having no money!
- Define the following propositions:
  - p = "you are poor" q = "you have no money"
  - We need to prove that $p \equiv q$ given that $p \to q$ *and* $\neg q \to \neg p$, that is, $[(p \to q) \wedge (\neg q \to \neg p)] \Rightarrow (p \leftrightarrow q)$.

170

Solution:

Does $[(p \to q) \wedge (\neg q \to \neg p)] \Rightarrow (p \leftrightarrow q)$?

p	q	$p \to q$	$\neg q$	$\neg p$	$\neg q \to \neg p$	LSH	$p \leftrightarrow q$
T	T	T	F	F	T	T	T
T	F	F	T	F	F	F	F
F	T	T	F	T	T	T	F
F	F	T	T	T	T	T	T

There is a possibility of not being poor while having no money!

171

More Example

- Let
  $h_1 = p \to (q \to s)$
  $h_2 = \neg r \vee p$
  $h_3 = q$
  $c = r \to s$
  we want to establish $h_1 \wedge h_2 \wedge h_3 \Rightarrow c$

172

Does $(p \to (q \to s)) \wedge (\neg r \vee p) \wedge q \Rightarrow (r \to s)$?

1.	$\neg r \vee p$	Premise
2.	r	Assumption
3.	p	Rule II, 1&2, …
4.	$p \to (q \to s)$	Premise
5.	$q \to s$	Rule II, 3&4, …
6.	q	Premise
7.	s	Rule II, 5&6, …
8.	$r \to s$	Rule II. 2&7, …

173

$[(p \to (q \to s)) \wedge (\neg r \vee p) \wedge q] \to (r \to s) \equiv \mathrm{T}$?

Direct Method

1. $[(p \to (q \to s)) \wedge (\neg r \vee p) \wedge q] \to (r \to s)$
2. $\neg [(p \to (q \to s)) \wedge (\neg r \vee p) \wedge q] \vee (r \to s)$
3. $\neg [(\neg p \vee (q \to s)) \wedge (\neg r \vee p) \wedge q] \vee (r \to s)$
4. $\neg [(\neg p \vee (\neg q \vee s)) \wedge (\neg r \vee p) \wedge q] \vee (r \to s)$
5. $\neg [(\neg p \vee \neg q \vee s) \wedge (\neg r \vee p) \wedge q] \vee (\neg r \vee s)$
6. $(\neg (\neg p \vee \neg q \vee s)) \vee (\neg (\neg r \vee p)) \vee (\neg q) \vee (\neg r \vee s)$
7. $(p \wedge q \wedge \neg s) \vee (r \wedge \neg p) \vee (\neg q) \vee (\neg r \vee s)$
8. $(s \vee \neg s) \wedge (s \vee (p \wedge q)) \vee (r \wedge \neg p) \vee (\neg q) \vee (\neg r)$
9. $s \vee (p \wedge q) \vee (r \wedge \neg p) \vee (\neg q) \vee (\neg r)$
10. $s \vee (\neg q \vee q) \wedge (\neg q \vee p) \vee (r \wedge \neg p) \vee (\neg r)$
11. $s \vee (\neg q \vee p) \vee (r \wedge \neg p) \vee (\neg r)$
12. $s \vee (\neg q \vee p) \vee (\neg r \vee r) \wedge (\neg r \vee \neg p)$
13. $s \vee \neg q \vee p \vee (\neg r \vee \neg p)$
14. $s \vee \neg q \vee p \vee \neg r \vee \neg p$
15. T

174

Does $(p \to (q \to s)) \wedge (\neg r \vee p) \wedge q \Rightarrow (r \to s)$?

Contradiction Method:

$(p \to (q \to s)) \wedge (\neg r \vee p) \wedge q \wedge (\neg (r \to s)) \Rightarrow F$?

1.	$\neg (r \to s)$	Contrary Assumption
2.	$\neg (\neg r \vee s)$	Rule II, substitution
3.	$r \wedge \neg s$	2, and De Morgan's
4.	r	3, simplification
5.	$\neg s$	3, simplification
6.	$\neg r \vee p$	Premise
7.	p	4&6
8.	$p \to (q \to s)$	Premise
9.	$q \to s$	7&8, MP
10.	q	Premise
11.	s	9&10, MP
12.	Contradiction	11&5

175

© 2016 by A-H. Esfahanian. All Rights Reserved.

Example: Proof by Contradiction

- Let
  $h_1 = q \vee d$
  $h_2 = (q \vee d) \rightarrow \neg p$
  $h_3 = \neg p \rightarrow (a \wedge \neg b)$
  $h_4 = (a \wedge \neg b) \rightarrow (r \vee s)$
  $c = r \vee s$,

  Prove by contradiction that

  $h_1 \wedge h_2 \wedge h_3 \wedge h_4 \Rightarrow c$.

176

$h_1 \wedge h_2 \wedge h_3 \wedge h_4 \wedge \neg c \Rightarrow \text{F}$

$(q \vee d) \wedge ((q \vee d) \rightarrow \neg p) \wedge (\neg p \rightarrow (a \wedge \neg b)) \wedge ((a \wedge \neg b) \rightarrow (r \vee s)) \wedge \neg (r \vee s) \Rightarrow F$

1.	$q \vee d$	Premise
2.	$(q \vee d) \rightarrow \neg p$	Premise
3.	$\neg p$	1&2, and modus ponens
4.	$\neg p \rightarrow (a \wedge \neg b)$	Premise
5.	$(a \wedge \neg b)$	3&4, modus ponens
6.	$(a \wedge \neg b) \rightarrow (r \vee s)$	Premise
7.	$r \vee s$	5&6, modus ponens
8.	$\neg (r \vee s)$	Contrary Assumption
9.	F	

177

Rules of Inference for Predicates

- All the Propositional logic rules.
- The *Universal Specification* (US) rule:
  $\forall x\, P(x) \Rightarrow P(y)$ for any y in the domain.
  The rule is also know as Instantiation rule
- The *Existential Specification* (ES)
  $\exists x\, P(x) \Rightarrow P(y)$ for some y in the domain.
- The *Existential Generalization* (EG)
  $P(y) \Rightarrow \exists x\, P(x)$

178

Other Facts

- $\exists x\, (A(x) \rightarrow B(x)) \equiv \forall x\, A(x) \rightarrow \exists x\, B(x)$
- $\exists x\, A(x) \rightarrow \forall x\, B(x) \equiv \forall x\, (A(x) \rightarrow B(x))$
- $\exists x\, (A(x) \vee B(x)) \equiv \exists x\, A(x) \vee \exists x\, B(x)$
- $\forall x\, (A(x) \wedge B(x)) \equiv \forall x\, A(x) \wedge \forall x\, B(x)$

179

Prove that $\forall x\, (H(x) \rightarrow M(x)) \wedge H(s) \Rightarrow M(s)$

- This is the famous Socrates's argument
  All men are mortal
  Socrates is a man
  Therefore, Socrates is a mortal
  - Let $H(x)$ be "x is a man",
  - Let $M(x)$ be "x is a mortal" and
  - Let s be "Socrates".

180

Prove that $\forall x\, (H(x) \rightarrow M(x)) \wedge H(s) \Rightarrow M(s)$

1.	$\forall x\, (H(x) \rightarrow M(x))$	Premise
2.	$H(s) \rightarrow M(s)$	1, Universal Specification
3.	$H(s)$	Premise
4.	$M(s)$	2&3 and MP

181

© 2016 by A-H. Esfahanian. All Rights Reserved.

Prove that $\forall x\,(H(x) \rightarrow M(x)) \wedge \exists x\, H(x) \Rightarrow \exists x\, M(x)$

1. $\exists x\, H(x)$ Premise
2. $H(y)$ Existential Specification, for some y
3. $\forall x\,(H(x) \rightarrow M(x))$ Premise
4. $H(y) \rightarrow M(y)$ 3 & US
5. $M(y)$ 2&3, MP
6. $\exists x\, M(x)$ 5, Existential Generalization

182

Prove that $\exists x\,(A(x) \wedge B(x)) \Rightarrow \exists x\, A(x) \wedge \exists x\, B(x)$

1. $\exists x\,(A(x) \wedge B(x))$ Premise
2. $A(y) \wedge B(y)$ 1, ES, Note that y is fixed now.
3. $A(y)$
4. $B(y)$
5. $\exists x\, A(x)$ 3, EG
6. $\exists x\, B(x)$ 4, EG
7. $\exists x\, A(x) \wedge \exists x\, B(x)$ 5&6

Question: Is the converse true?

183

Does $\exists x\, A(x) \wedge \exists x\, B(x) \Rightarrow \exists x\,(A(x) \wedge B(x))$?

1. $\exists x\, A(x)$ Premise
2. $A(y)$ 1, ES
3. $\exists x\, B(x)$ Premise, ES
4. $B(y)$ 3, ES
5. $A(y) \wedge B(y)$ 2 and 4
6. $\exists x\,(A(x) \wedge B(x))$ 5, EG

This is a wrong proof. The "y" in step 2 and 4 should not be assumed to be the same.

184

© 2016 by A-H. Esfahanian. All Rights Reserved.