Philosophy 240: Symbolic Logic
Fall 2010
Mondays, Wednesdays, Fridays: 9am - 9:50am

Hamilton College
Russell Marcus
rmarcus1@hamilton.edu

Class 18 - October 6
Indirect Proof (§7.6)

I. Indirect Proof: Another Method for Derivation

Consider the following two proofs:

1.

	1. A · ~A	/ B
	2. A	1, Simp
	3. A ∨ B	2, Add
	4. ~A	1, Com, Simp
	5. B	3, 4, DS

QED

2.

	1. B ⊃ (P · ~P)	/ ~B
	| 2. B	ACP
	| 3. P · ~P	1, 2, MP
	| 4. P	3, Simp
	| 5. P ∨ ~B	4, Add
	| 6. ~P	5, 3, Com, Simp
	| 7. ~B	5, 6, DS
	8. B ⊃ ~B	2-7, CP
	9. ~B ∨ ~B	8, Impl
	10. ~B	9, Taut

QED

The moral of the first argument, which is an instance of what logicians call explosion, is that anything follows from a contradiction.
The moral of the second is that if a statement entails a contradiction, then its negation is true.
Indirect proof is based on these two morals.
Indirect proof is also called reductio ad absurdum, or just reductio.
Assume your desired conclusion is false, and try to get a contradiction.
If you get it, then you know the opposite of the assumption is true.

Procedure for Indirect Proof, (IP)

1. Indent, assuming the opposite of what you want to conclude (one more or one fewer '~').
2. Derive a contradiction, using any letter.
3. Discharge the negation (not the opposite!) of your assumption.

A contradiction is any statement of the form: α • ~α
The following wffs are all contradictions:

P •~ P
~~P • ~~~P
~(P∨ ~Q) • ~~(P ∨ ~Q)

Sample Derivation:

1. A ⊃ B			
2. A ⊃ ~B	/~A		
| 3. A	AIP	Let's see what happens if the opposite of the conclusion is true.	
| 4. B	1, 3, MP		
| 5. ~B	2, 3, MP		
| 6. B · ~B	4, 5, Conj	This is impossible - a contradiction.	
7. ~A	3-6, IP	So ~~A must be false, and so ~A is true.	

QED

The method of indirect proof is especially useful for proving disjunctions as well as simple statements and negations.

II. More sample derivations

Plain indirect proof:

1. F ⊃ ~D		
2. D		
3. (D · ~E) ⊃ F	/ E	
| 4. ~E	AIP	
| 5. D · ~E	2, 4, Conj	
| 6. F	3, 5, MP	
| 7. ~D	1, 6, MP	
| 8. D · ~D	2, 7, Conj	
9. ~~E	4-8, CP	
10. E	9, DN	

QED

Indirect proof with conditional proof:

1. E ⊃ (A · D)		
2. B ⊃ E	/ (E ∨ B) ⊃ A	
| 3. E ∨ B		ACP
| | 4. ~A		AIP
| | 5. ~A ∨ ~D		4, Add
| | 6. ~(A · D)		5, DM
| | 7. ~E		1, 6, MT
| | 8. B		3, 7, DS
| | 9. ~B		2, 7, MT
| | 10. B · ~B		8, 9, Conj
| 11. ~~A		4-10, IP
| 12. A		11, DN
12. (E ∨ B) ⊃ A		3-12, CP

QED

This last method has the form of many (almost all?) proofs in mathematics.
First, one states one's assumptions, one's specific axioms.
Then one assumes one's conclusion is false, and derives a contradiction.

III. Exercises A. Derive the conclusions of the following arguments using the 18 rules, and either CP or IP.

1. 1. $A \supset B$
   2. $\sim A \vee \sim B$ / $\sim A$

2. 1. $F \supset (\sim E \vee D)$
   2. $F \supset \sim D$ / $F \supset \sim E$

3. 1. $\sim J \supset (G \cdot H)$
   2. $G \supset I$
   3. $H \supset \sim I$ / J

4. 1. $S \supset (T \vee U)$
   2. $W \supset \sim U$ / $S \supset \sim(W \cdot \sim T)$

5. 1. $(L \supset M) \cdot (N \supset O)$
   2. $(M \vee O) \supset P$
   3. $\sim P$ / $\sim(L \vee N)$

Solutions will vary.

IV. Using IP to derive logical truths

Like conditional proof, the method of indirect proof is easily adapted to proving logical truths.

To prove that '$\sim[(X \equiv Y) \cdot \sim(X \vee \sim Y)]$' is a logical truth, we start with an assumption.

	1. $(X \equiv Y) \cdot \sim(X \vee \sim Y)$	AIP
	2. $X \equiv Y$	1, Simp
	3. $(X \supset Y) \cdot (Y \supset X)$	2, Equiv
	4. $\sim(X \vee \sim Y)$	1, Com, Simp
	5. $\sim X \cdot Y$	4, DM DN
	6. $Y \supset X$	3, Com, Simp
	7. $\sim X$	5, Simp
	8. $\sim Y$	6, 7, MT
	9. Y	5, Com, Simp
	10. $Y \cdot \sim Y$	9, 8, Conj
11.	$\sim[(X \equiv Y) \cdot \sim(X \vee \sim Y)]$	1-10, IP

QED

Here is another example: Show that '(P ⊃ Q) ∨ (~Q ⊃ P)' is a logical truth.

| 1. ~[(P ⊃ Q) ∨ (~Q ⊃ P)]	AIP
| 2. ~(P ⊃ Q) · ~(~Q ⊃ P)	1, DM
| 3. ~(P ⊃ Q)	2, Simp
| 4. ~(~P ∨ Q)	3, Impl
| 5. P · ~Q	4, DM, DN
| 6. ~(~Q ⊃ P)	2, Com, Simp
| 7. ~(Q ∨ P)	6, Impl, DN
| 8. ~Q · ~P	7, DM
| 9. P	5, Simp
| 10. ~P	8, Com, Simp
| 11. P · ~P	9, 10, Conj
12. (P ⊃ Q) ∨ (~Q ⊃ P)	1-11, IP

QED

Here are some hints to help determine whether to use conditional proof or indirect proof to derive a logical truth.

If the main connective is a conditional or a biconditional, we generally use conditional proof.
If the main connective is a disjunction or a negation, we generally use indirect proof.
If the main connective is a conjunction, we look to the main connectives of each conjunct to determine the best method of proof.

Sometimes, we might need a logical truth as an intermediate step in a proof:

1. B ⊃ [(D ⊃ D) ⊃ E]		
2. E ⊃ {[F ⊃ (G ⊃ F)] ⊃ (H · ~H)}	/ ~B	
| 3. B		AIP
| 4. (D ⊃ D) ⊃ E		1, 3, MP
| | 5. ~(D ⊃ D)		AIP
| | 6. ~(~D ∨ D)		5, Impl
| | 7. D · ~D		6, DM, DN
| 8. D ⊃ D		5-7, IP, DN
| 9. E		4, 8, MP
| 10. [F ⊃ (G ⊃ F)] ⊃ (H · ~H)		2, 9, MP
| | 11. F		ACP
| | 12. F ∨ ~G		11, Add
| | 13. ~G ∨ F		12, Com
| | 14. G ⊃ F		13, Impl
| 15. F ⊃ (G ⊃ F)		11-14, CP
| 16. H · ~H		10, 15, MP
17. ~B		3-16, IP

QED

Here are two observation about the above proof.

At step 4, 'D ⊃ D' is derivable using IP or CP.
At step 10, the antecedent is another logical truth.

V. Exercises B. Show that the following propositions are logical truths using the 18 rules, and either CP or IP.

1. $(A \supset B) \vee (B \supset A)$
2. $(P \supset Q) \supset [(P \cdot R) \supset (Q \cdot R)]$
3. $(P \cdot Q) \supset [(P \vee R) \cdot (Q \vee R)]$
4. $(A \supset B) \vee (\sim A \supset C)$
5. $(P \supset Q) \supset \{(P \supset R) \supset [P \supset (Q \cdot R)]\}$

Solutions will vary.

VI. Converting Derivations to Logical Truths

Almost all of the proofs we have done so far have required assumptions as premises.
Assumptions are usually empirical, taken from observation, though they may be *a priori*.
In either case, they are generally not justified by the same methods which we use to justify our system of logic.
Thus, the derivations we have done are not strictly logical.
They are not, as they stand, proofs of logical conclusions.
They are merely logical derivations from premises to conclusions.
But, for every valid argument requiring premises, we can create a proof of a purely logical truth.

Consider

1. $P \supset (Q \bullet R)$
2. $\sim R$ / $\sim P$

This argument contains two assumptions, at premises 1 and 2.
To convert this argument to a logical truth requiring no assumptions, construct a conditional statement with the former premises as antecedents and the former conclusion as consequent.
You can either conjoin the premises into a single antecedent, or form nested conditionals:

$\{[P \supset (Q \bullet R)] \bullet \sim R\} \supset \sim P$
$[P \supset (Q \bullet R)] \supset (\sim R \supset \sim P)$

Note the equivalence between the two statements by one rule of exportation.
Each of these propositions is a logical truth.

1. $[P \supset (Q \bullet R)] \bullet \sim R$	ACP
2. $P \supset (Q \bullet R)$	1, Simp
3. $\sim R$	1, Com, Simp
4. $\sim Q \vee \sim R$	3, Add, Com
5. $\sim(Q \bullet R)$	4, DM
6. $\sim P$	2, 5, MT
7. $\{[P \supset (Q \bullet R)] \bullet \sim R\} \supset \sim P$	1-6, CP

QED

Similarly, the argument:

1. $P \vee Q$
2. $Q \supset (R \bullet S)$
3. $\sim R$
4. $Q \equiv T$ / $P \bullet \sim T$

can be converted to the logical truths:

$\{\{(P \vee Q) \bullet [Q \supset (R \bullet S)]\} \bullet [\sim R \bullet (Q \equiv T)]\} \supset (P \bullet \sim T)$
$(P \vee Q) \supset \{[Q \supset (R \bullet S)] \supset \{\sim R \supset \{(Q \equiv T) \supset (P \bullet \sim T)\}\}\}$

(I'll leave the proofs to you as an exercise.)

The relation between derivations requiring assumptions and their corresponding logical truths is guaranteed by a meta-logical result called the Deduction Theorem; see Hunter §26, or Mendelson 37-8. The theorem may have been first proved by Tarski in 1921, but the first published proof was by Herbrand in 1930.

We spoke earlier in the semester about how a logical theory, like any theory, can be characterized by its theorems.
For logical theories, the theorems are the logical truths.
The arguments we have been deriving are useful in application.
But, these logical truths are the logician's real interest.

The transformations we have made at the object-language level can be made at the metalinguistic level.
Our rules of inference are written in a meta-language.
We say that any substitution instances of the premises in our rules of inference entail a substitution instance of the conclusion.
We can similarly convert all of our rules of inference.

$\alpha \supset \beta$
α / β

can be converted to:

$[(\alpha \supset \beta) \bullet \alpha] \supset \beta$

Similarly:

$(\alpha \supset \beta) \bullet (\gamma \supset \delta)$
$\alpha \vee \gamma$ / $\beta \vee \delta$

can be converted to:

$\{[(\alpha \supset \beta) \bullet (\gamma \supset \delta)] \bullet (\alpha \vee \gamma)\} \supset (\beta \vee \delta)$

Any substitution instance of these new forms will be a logical truth.

All rules of replacement can easily be turned into templates for constructing logical truths.
For examples:

$\sim(\alpha \vee \beta) \equiv (\sim\alpha \bullet \sim\beta)$
$(\alpha \supset \beta) \equiv (\sim\alpha \vee \beta)$

Any substitution instance of these forms will be a logical truth, too.
Logical truths, as we have seen, are provable with no premises.
We can, using our method, eliminate nearly all of our eighteen rules.
Instead, we can adopt a small group of templates for constructing logical truths, along with a single rule of inference, usually modus ponens.
Many logical theories consist of only a few templates for constructing logical truths along with modus ponens and a rule of substitution.

VII. Exercises C. Convert each of the following arguments to a logical truth.

1. 1. $A \supset \sim B$
   2. B / $\sim A$

2. 1. $C \supset (D \bullet E)$
   2. $E \supset F$ / $C \supset F$

3. 1. $G \supset (H \vee I)$
   2. $I \supset (J \bullet \sim K)$
   3. $\sim H$ / $G \supset \sim K$

VIII. Sample solutions to Exercises C.

1. $(A \supset \sim B) \supset (B \supset \sim A)$
2. $\{[C \supset (D \bullet E)] \bullet (E \supset F)\} \supset (C \supset F)$
3. $[G \supset (H \vee I)] \supset \{[I \supset (J \bullet \sim K)] \supset [\sim H \supset (G \supset \sim K)]\}$