Chapter 4: **Propositional Proofs**

Based on Harry Gensler’s book

For CS2209A/B

By Dr. Charles Ling; cling@csd.uwo.ca

4.1/4.2: Easier Proofs

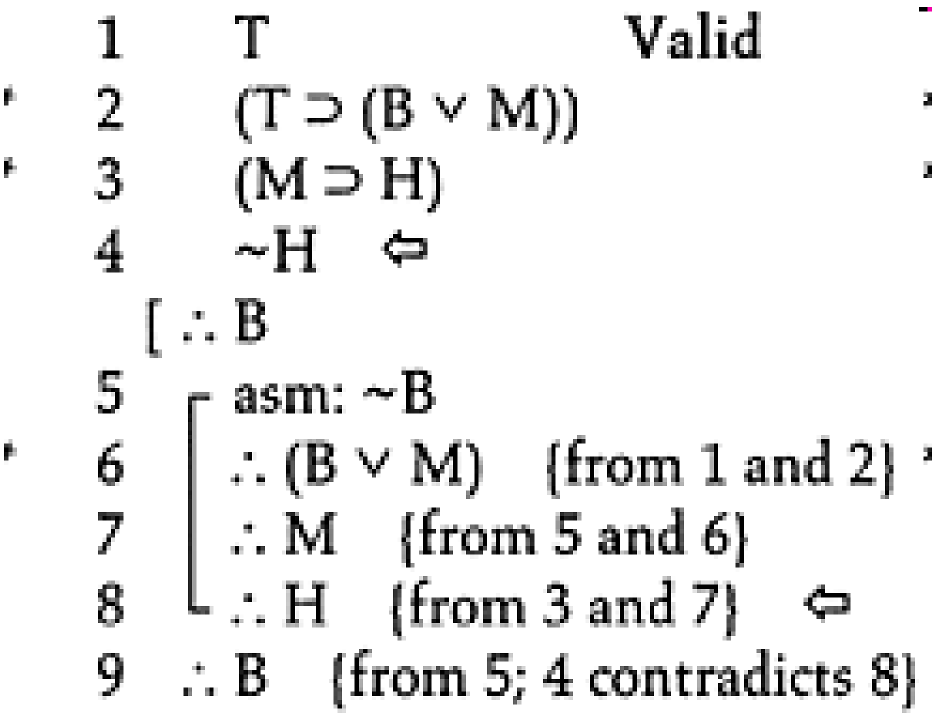
- Formal proofs: main way to prove
  - Use “rules” to syntactically derive; not with truth tables
- But using I/S-rules in Chapter 3 is incomplete
- A new way: ***prove by contradiction***
  - To prove a conclusion C, assume the opposite: ~C
  - Add ~C as a premise
  - Then try to derive a contradiction: A, ~A (A is some wff)
    - **RAA,** *reductio ad absurdum* (reduction to absurdity)
  - Then we prove the conclusion!
- A “universal”, more powerful method
  - If provable directly, then also provable by contradiction

Prove: square root 2 is not rational

1. The only people in the mansion were the butler and the maid.
2. If the only people in the mansion were the butler and the maid, then the butler or the maid did it.
3. If the maid did it, then she had a motive.
4. The maid didn’t have a motive.

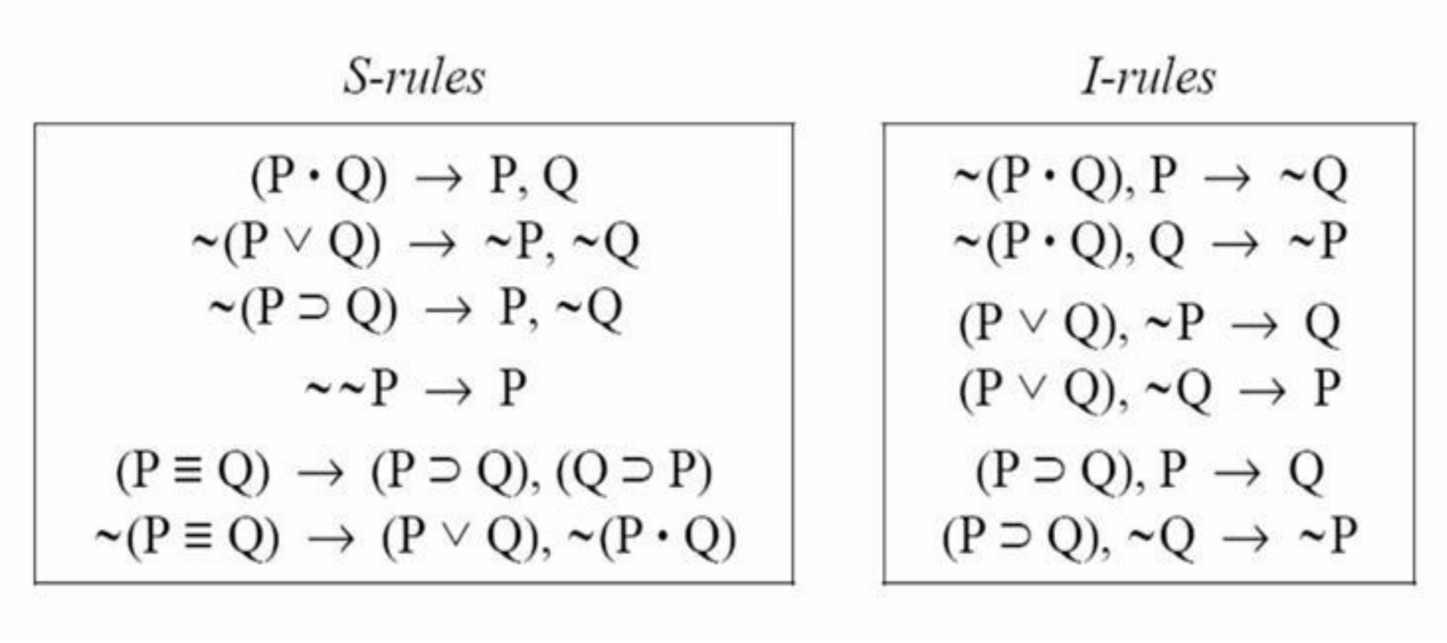
Prove: butler committed the murder

Assume that the butler didn’t do it.



```
1      T                           Valid
2      (T ⊃ (B ∨ M))
3      (M ⊃ H)
4      ~H   ⇦
   [ ∴ B
5    ┌ asm: ~B
6    │ ∴ (B ∨ M)   {from 1 and 2}
7    │ ∴ M   {from 5 and 6}
8    └ ∴ H   {from 3 and 7}   ⇦
9    ∴ B   {from 5; 4 contradicts 8}
```

Rules you can use



S-rules

$(P \cdot Q) \;\rightarrow\; P, Q$

$\sim(P \vee Q) \;\rightarrow\; \sim P, \sim Q$

$\sim(P \supset Q) \;\rightarrow\; P, \sim Q$

$\sim\sim P \;\rightarrow\; P$

$(P \equiv Q) \;\rightarrow\; (P \supset Q), (Q \supset P)$

$\sim(P \equiv Q) \;\rightarrow\; (P \vee Q), \sim(P \cdot Q)$

I-rules

$\sim(P \cdot Q), P \;\rightarrow\; \sim Q$

$\sim(P \cdot Q), Q \;\rightarrow\; \sim P$

$(P \vee Q), \sim P \;\rightarrow\; Q$

$(P \vee Q), \sim Q \;\rightarrow\; P$

$(P \supset Q), P \;\rightarrow\; Q$

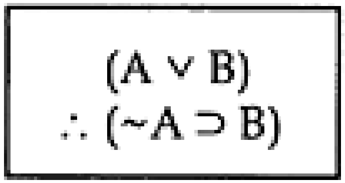
$(P \supset Q), \sim Q \;\rightarrow\; \sim P$

Key components in a proof

- A **premise** is a line consisting of a wff by itself
- An **assumption** is a line consisting of “asm:” and then a wff.
- A **derived step** is a line consisting of “∴” and then a wff.
- A **formal proof** is a vertical sequence of zero or more premises followed by one or more assumptions or derived steps, where each derived step follows from previously not-blocked-off lines by RAA or one of the inference rules listed above, and each assumption is blocked off using RAA.
- Two wffs are **contradictory** if they are exactly alike except that one starts with an additional “~.”

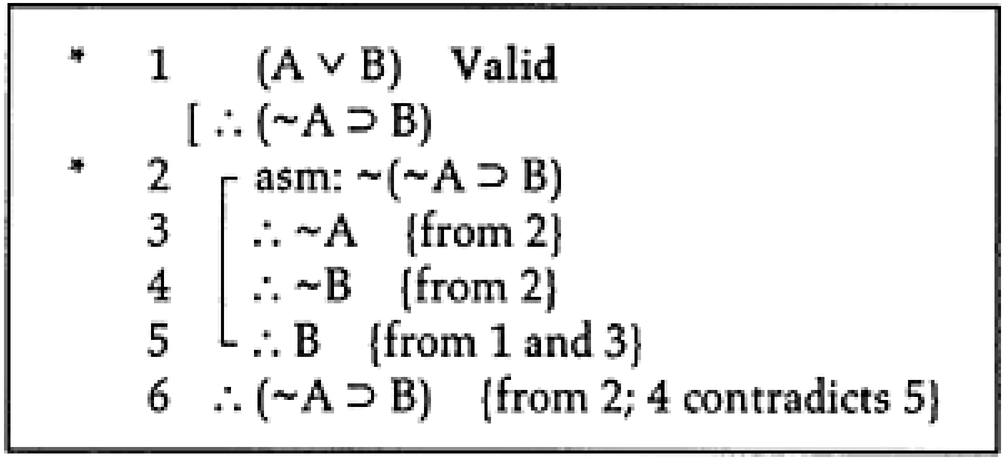
- **LogiCola: G-EV**

4.2a Exercise



$(A \vee B)$

$\therefore (\sim A \supset B)$



* 1 $(A \vee B)$ **Valid**

$[\ \therefore (\sim A \supset B)$

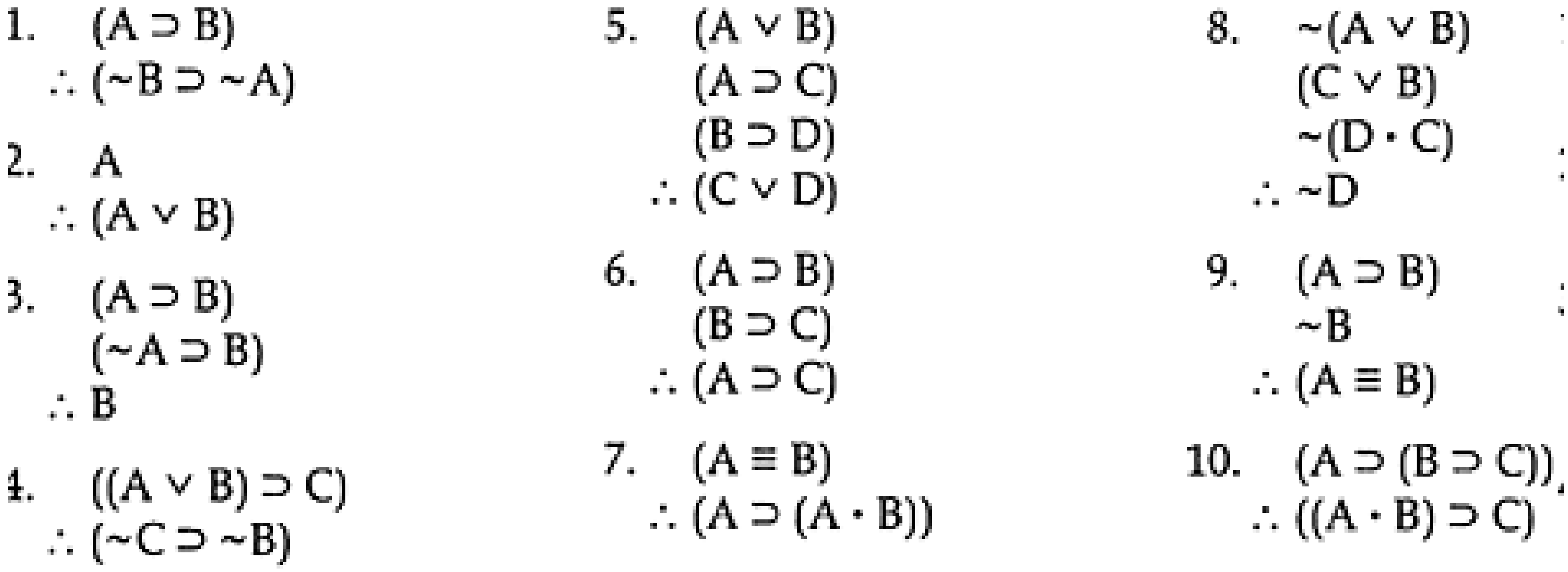
* 2 ┌ asm: $\sim(\sim A \supset B)$

3 │ $\therefore \sim A$ {from 2}

4 │ $\therefore \sim B$ {from 2}

5 └ $\therefore B$ {from 1 and 3}

6 $\therefore (\sim A \supset B)$ {from 2; 4 contradicts 5}



1. $(A \supset B)$
   $\therefore (\sim B \supset \sim A)$

2. A
   $\therefore (A \vee B)$

3. $(A \supset B)$
   $(\sim A \supset B)$
   $\therefore B$

4. $((A \vee B) \supset C)$
   $\therefore (\sim C \supset \sim B)$

5. $(A \vee B)$
   $(A \supset C)$
   $(B \supset D)$
   $\therefore (C \vee D)$

6. $(A \supset B)$
   $(B \supset C)$
   $\therefore (A \supset C)$

7. $(A \equiv B)$
   $\therefore (A \supset (A \cdot B))$

8. $\sim(A \vee B)$
   $(C \vee B)$
   $\sim(D \cdot C)$
   $\therefore \sim D$

9. $(A \supset B)$
   $\sim B$
   $\therefore (A \equiv B)$

10. $(A \supset (B \supset C))$
    $\therefore ((A \cdot B) \supset C)$

4.2b Exercise

1. If we had an absolute proof of God’s existence, then our will would be irresistibly attracted to do right.

   If our will were irresistibly attracted to do right, then we’d have no free will.

   ∴ If we have free will, then we have no absolute proof of God’s existence.

   (Use P, I, and F)

2. If the world had a beginning in time and it didn’t just pop into existence without any cause, then the world was caused by God.

   If the world was caused by God, then there is a God.

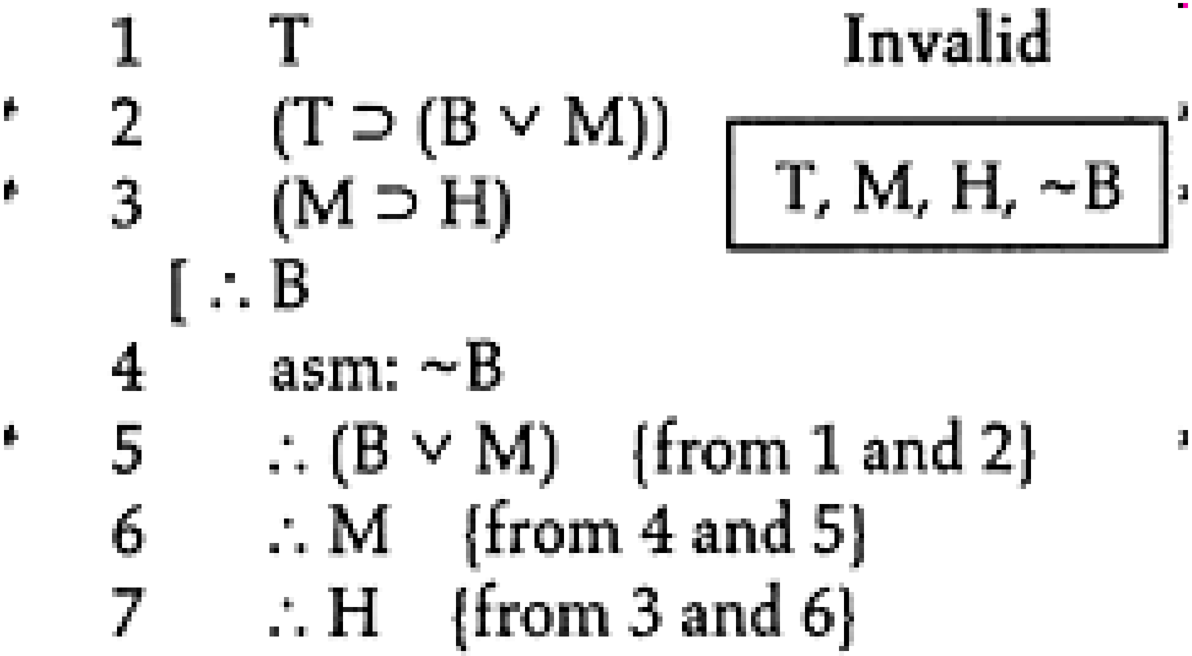
   There is no God.

   ∴ Either the world had no beginning in time, or it just popped into existence without any cause. (Use B, P, C, and G)

LogiCola: E-E, then prove with methods specified.

4.3 Easier refutations

- If we try to prove an invalid argument, we won’t succeed; instead, we’ll be led to *refute* the argument by finding a set of assignment making the premises all true and conclusion false. (Need to verify this!)
- Same as finding a counter example!



```
   1     T                                 Invalid
*  2     (T ⊃ (B ∨ M))                 ┌──────────────┐
*  3     (M ⊃ H)                       │ T, M, H, ~B  │
       [ ∴ B                           └──────────────┘
   4     asm: ~B
*  5     ∴ (B ∨ M)    {from 1 and 2}
   6     ∴ M    {from 4 and 5}
   7     ∴ H    {from 3 and 6}
```

Strategy for simple proof

1 START: Assume the opposite of the conclusion.

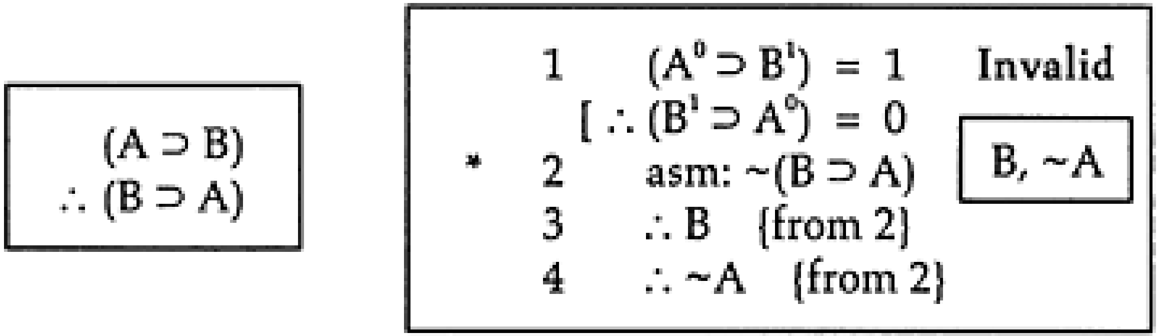
2 S&I: Derive whatever you can using the S- and I-rules, until you get nothing more

3 RAA: If you get a contradiction, apply RAA and you have proved the original conclusion.

4. REFUTE: Else: construct a refutation box and verify it (it makes all premises true and conclusion false).

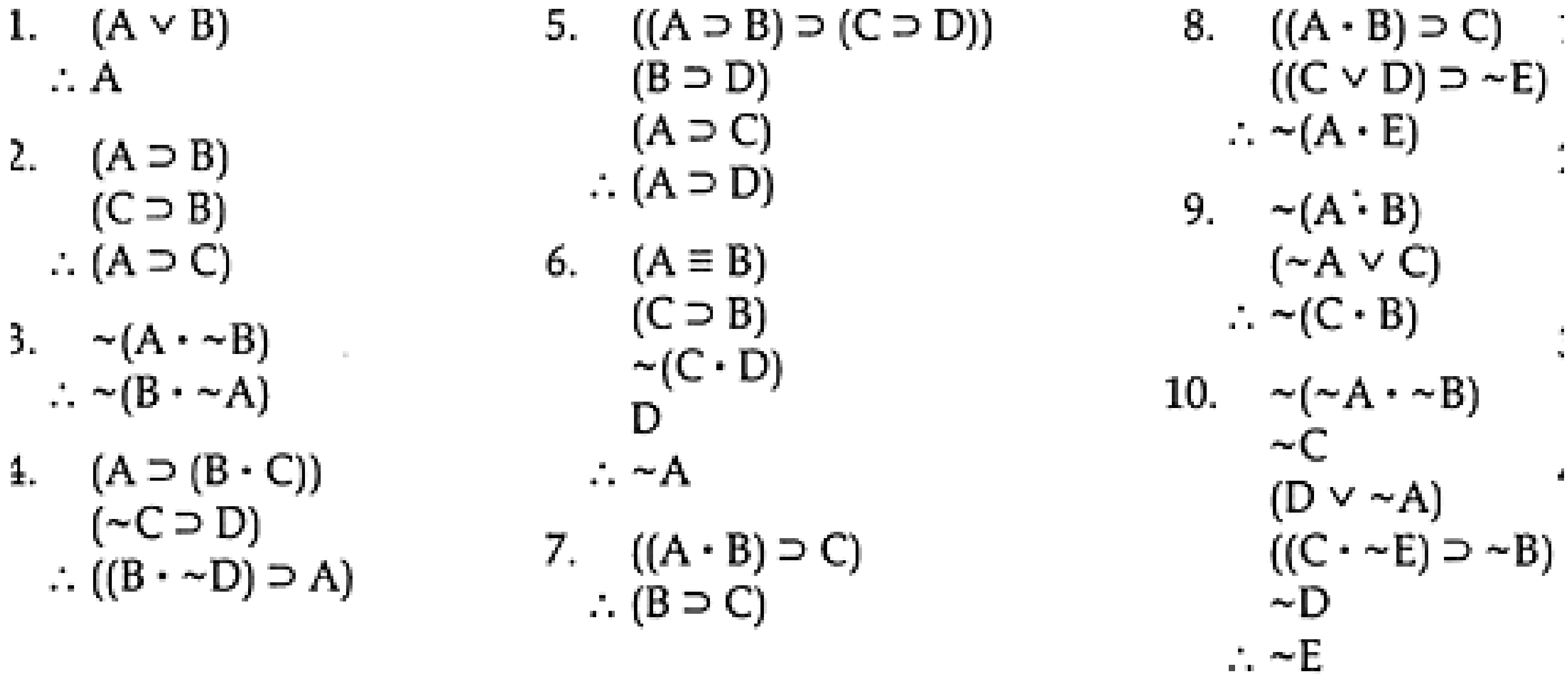
LogiCola: G-EI

4.3a Exercise



$(A \supset B)$
$\therefore (B \supset A)$

	1	$(A^0 \supset B^1) = 1$	Invalid
		$[\therefore (B^1 \supset A^0) = 0$	$\boxed{B, \sim A}$
*	2	asm: $\sim(B \supset A)$	
	3	$\therefore B$ {from 2}	
	4	$\therefore \sim A$ {from 2}	



1. $(A \vee B)$
$\therefore A$

2. $(A \supset B)$
$(C \supset B)$
$\therefore (A \supset C)$

3. $\sim(A \cdot \sim B)$
$\therefore \sim(B \cdot \sim A)$

4. $(A \supset (B \cdot C))$
$(\sim C \supset D)$
$\therefore ((B \cdot \sim D) \supset A)$

5. $((A \supset B) \supset (C \supset D))$
$(B \supset D)$
$(A \supset C)$
$\therefore (A \supset D)$

6. $(A \equiv B)$
$(C \supset B)$
$\sim(C \cdot D)$
D
$\therefore \sim A$

7. $((A \cdot B) \supset C)$
$\therefore (B \supset C)$

8. $((A \cdot B) \supset C)$
$((C \vee D) \supset \sim E)$
$\therefore \sim(A \cdot E)$

9. $\sim(A \cdot B)$
$(\sim A \vee C)$
$\therefore \sim(C \cdot B)$

10. $\sim(\sim A \cdot \sim B)$
$\sim C$
$(D \vee \sim A)$
$((C \cdot \sim E) \supset \sim B)$
$\sim D$
$\therefore \sim E$

4.3b Exercise

1. If the butler shot Jones, then he knew how to use a gun.

   If the butler was a former marine, then he knew how to use a gun.

   The butler was a former marine.

   ∴ The butler shot Jones.   [Use S, K, and M.]

2. If predestination is true, then God causes us to sin.

   If God causes us to sin and yet damns sinners to eternal punishment, then God isn’t good.

   ∴ If God is good, then either predestination isn’t true or else God doesn’t damn sinners to eternal punishment. [Use P, C, D, and G]

4.4 Multiple assumptions

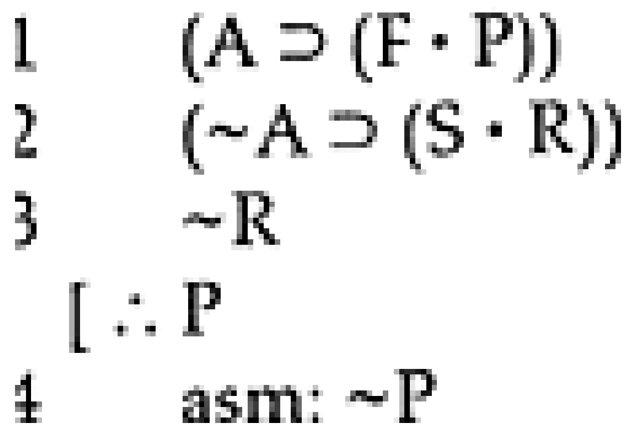
We may still get stuck…

If President Nixon knew about the massive Watergate cover-up, then he lied to the American people on national television and he should resign.

If President Nixon didn't know about the massive Watergate cover-up, then he was incompetently ignorant and he should resign.

∴ Nixon should resign. [Use K, L, R, and I.]

Still not complete… Solution: *make another assumption*



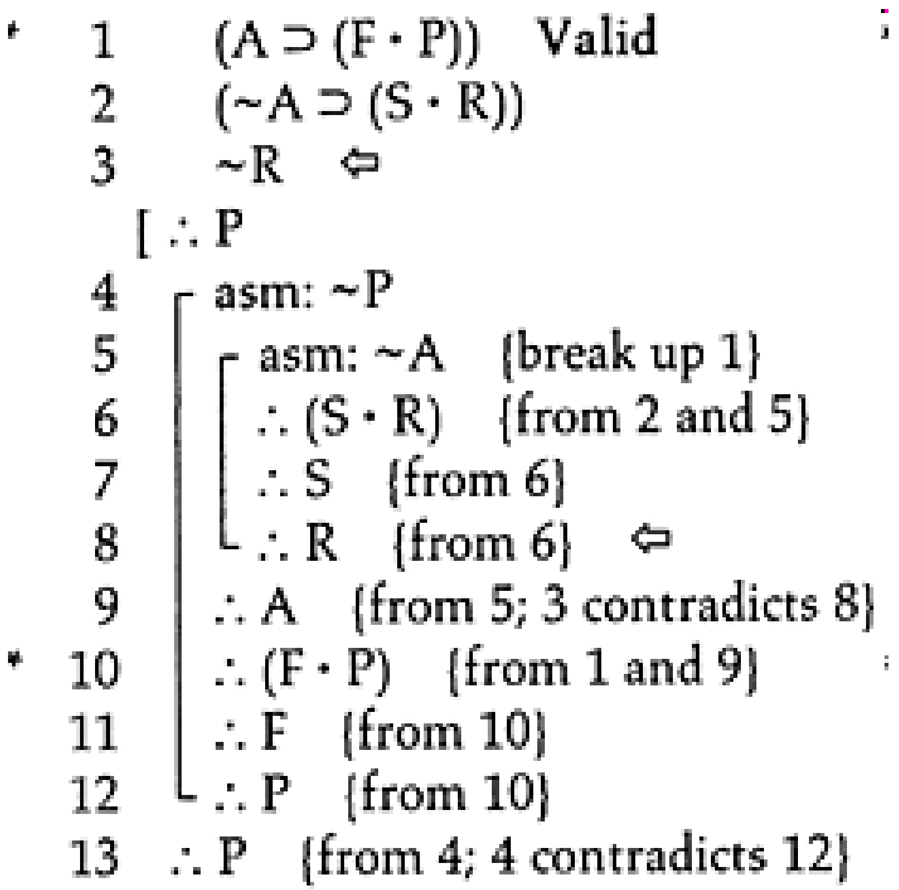
1 (A ⊃ (F • P))

2 (~A ⊃ (S • R))

3 ~R

[∴ P

4 asm: ~P



* 1 (A ⊃ (F • P)) Valid

2 (~A ⊃ (S • R))

3 ~R ⇦

[∴ P

4 ┌ asm: ~P

5 │ ┌ asm: ~A {break up 1}

6 │ │ ∴ (S • R) {from 2 and 5}

7 │ │ ∴ S {from 6}

8 │ └ ∴ R {from 6} ⇦

9 │ ∴ A {from 5; 3 contradicts 8}

* 10 │ ∴ (F • P) {from 1 and 9}

11 │ ∴ F {from 10}

12 └ ∴ P {from 10}

13 ∴ P {from 4; 4 contradicts 12}

LogiCola: G-HV

- Hints: if you have an unstarred, notblocked-off wff of one of these forms for which you don’t already have one side or its negation:

  ~(A·B) (A∨B) (A⊃B)

  Assume one side or its negation, such as

  asm: A asm: ~A asm: B asm: ~B

  (This allows you to continue to derive new wff)
- Then return to step 2 (S&I).
  - If you don’t get contradiction, the effort is wasted; try to make another assumption…

This proof strategy can prove or refute any propositional argument.

It is **sound** and **complete**

1 START: Assume the opposite of the conclusion.

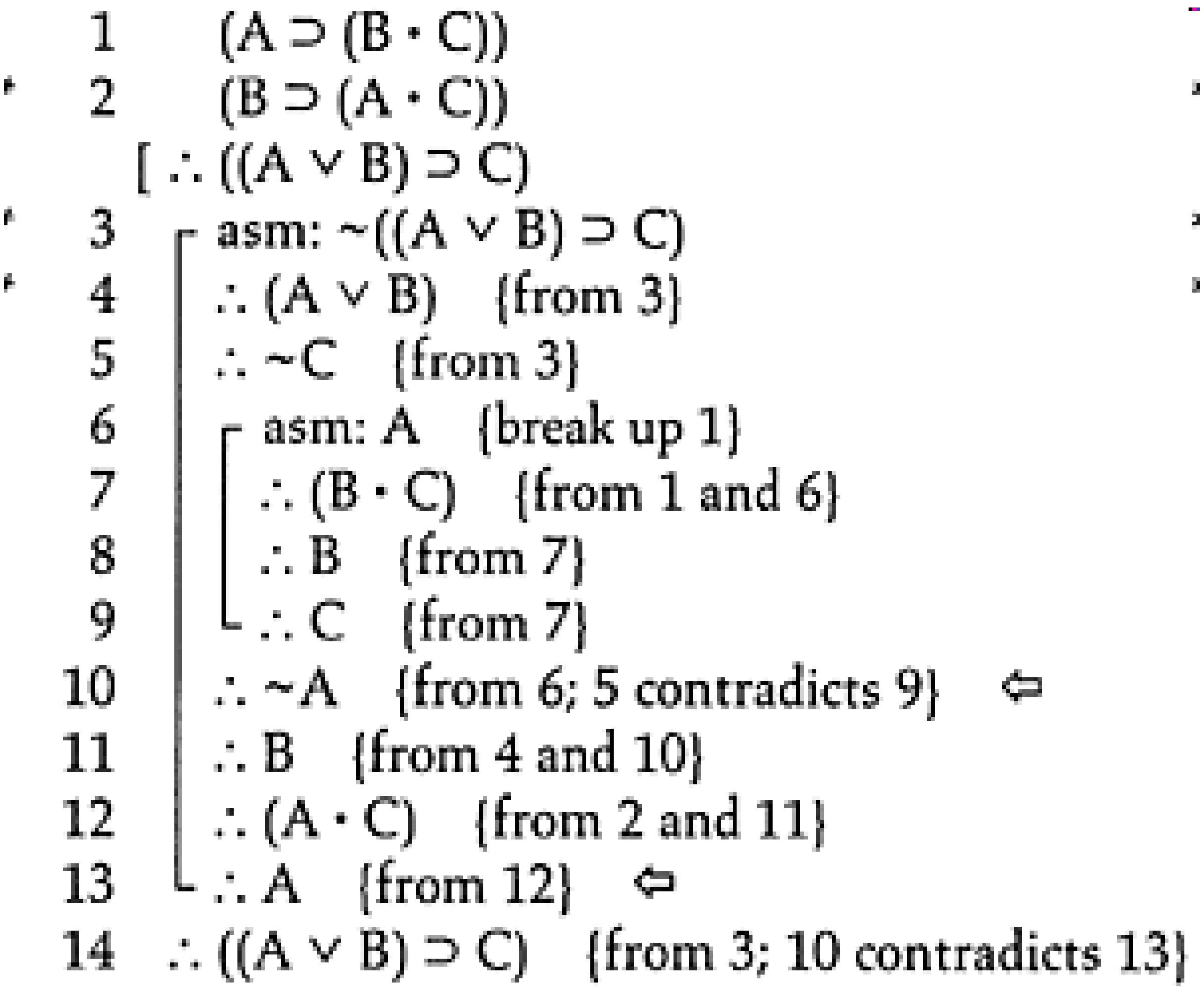
2 S&I: Derive whatever you can using the S- and I-rules. If you get a contradiction, Step 3; otherwise Step 4; otherwise Step 5

3 Apply RAA, so the negated assumption is derived

4. ASSUME: Make another assumption, Step 2

5. REFUTE: If you don’t get a contradiction, construct a refutation box from the derivation, and verify.

An Example



1 (A ⊃ (B • C))

2 (B ⊃ (A • C))

[∴ ((A ∨ B) ⊃ C)

3 asm: ~((A ∨ B) ⊃ C)

4 ∴ (A ∨ B) {from 3}

5 ∴ ~C {from 3}

6 asm: A {break up 1}

7 ∴ (B • C) {from 1 and 6}

8 ∴ B {from 7}

9 ∴ C {from 7}

10 ∴ ~A {from 6; 5 contradicts 9} ⇦

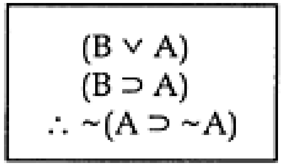
11 ∴ B {from 4 and 10}

12 ∴ (A • C) {from 2 and 11}

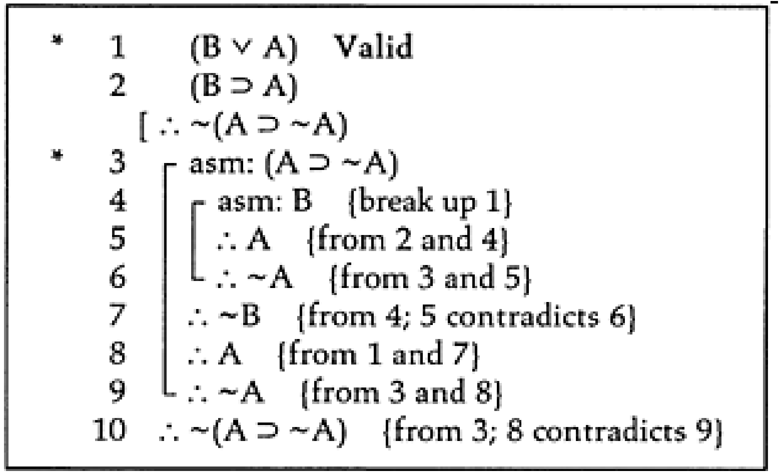
13 ∴ A {from 12} ⇦

14 ∴ ((A ∨ B) ⊃ C) {from 3; 10 contradicts 13}

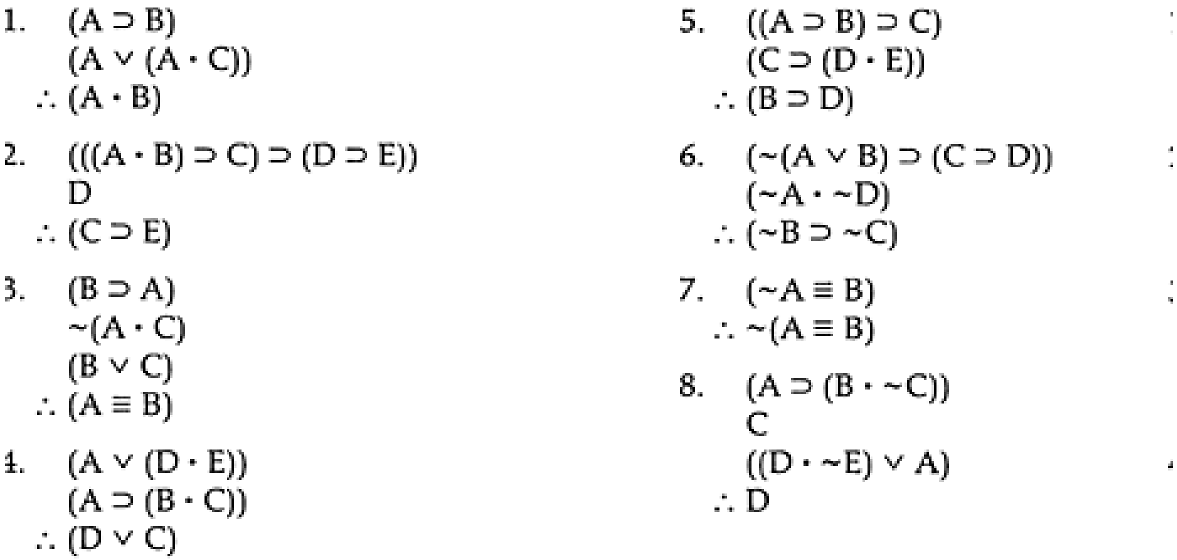
4.5a Exercise



(B ∨ A)
(B ⊃ A)
∴ ~(A ⊃ ~A)



```
*  1      (B ∨ A)    Valid
   2      (B ⊃ A)
        [ ∴ ~(A ⊃ ~A)
*  3    ┌ asm: (A ⊃ ~A)
   4    │ ┌ asm: B    {break up 1}
   5    │ │ ∴ A    {from 2 and 4}
   6    │ └ ∴ ~A    {from 3 and 5}
   7    │ ∴ ~B    {from 4; 5 contradicts 6}
   8    │ ∴ A    {from 1 and 7}
   9    └ ∴ ~A    {from 3 and 8}
  10    ∴ ~(A ⊃ ~A)    {from 3; 8 contradicts 9}
```



1. (A ⊃ B)
   (A ∨ (A · C))
   ∴ (A · B)

2. (((A · B) ⊃ C) ⊃ (D ⊃ E))
   D
   ∴ (C ⊃ E)

3. (B ⊃ A)
   ~(A · C)
   (B ∨ C)
   ∴ (A ≡ B)

4. (A ∨ (D · E))
   (A ⊃ (B · C))
   ∴ (D ∨ C)

5. ((A ⊃ B) ⊃ C)
   (C ⊃ (D · E))
   ∴ (B ⊃ D)

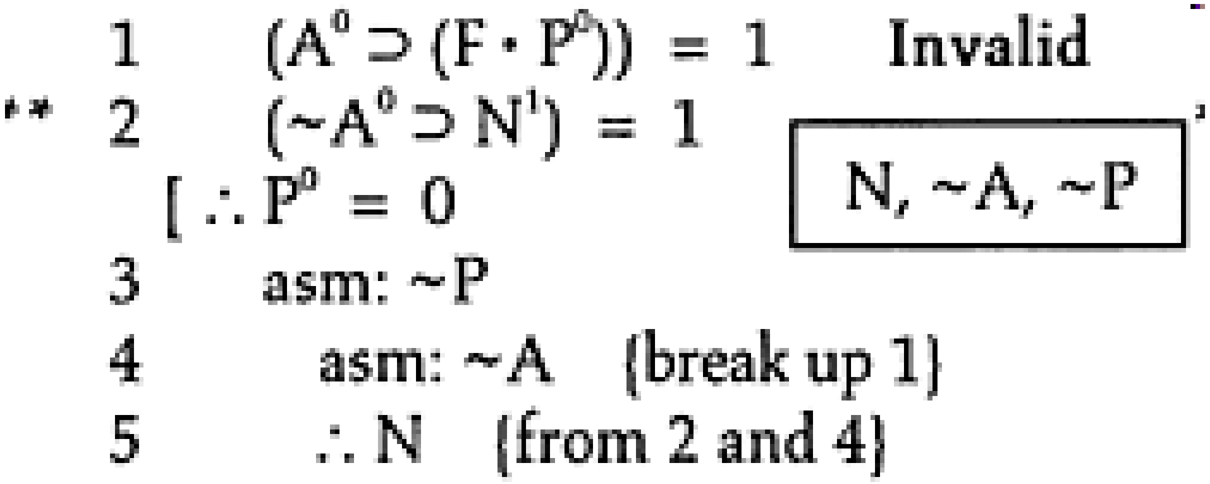
6. (~(A ∨ B) ⊃ (C ⊃ D))
   (~A · ~D)
   ∴ (~B ⊃ ~C)

7. (~A ≡ B)
   ∴ ~(A ≡ B)

8. (A ⊃ (B · ~C))
   C
   ((D · ~E) ∨ A)
   ∴ D

4.6 Harder refutations

- Multiple-assumption invalid arguments



1 $(A^0 \supset (F \cdot P^0)) = 1$ **Invalid**

** 2 $(\sim A^0 \supset N^1) = 1$

$[\ \therefore P^0 = 0$

3 asm: $\sim P$

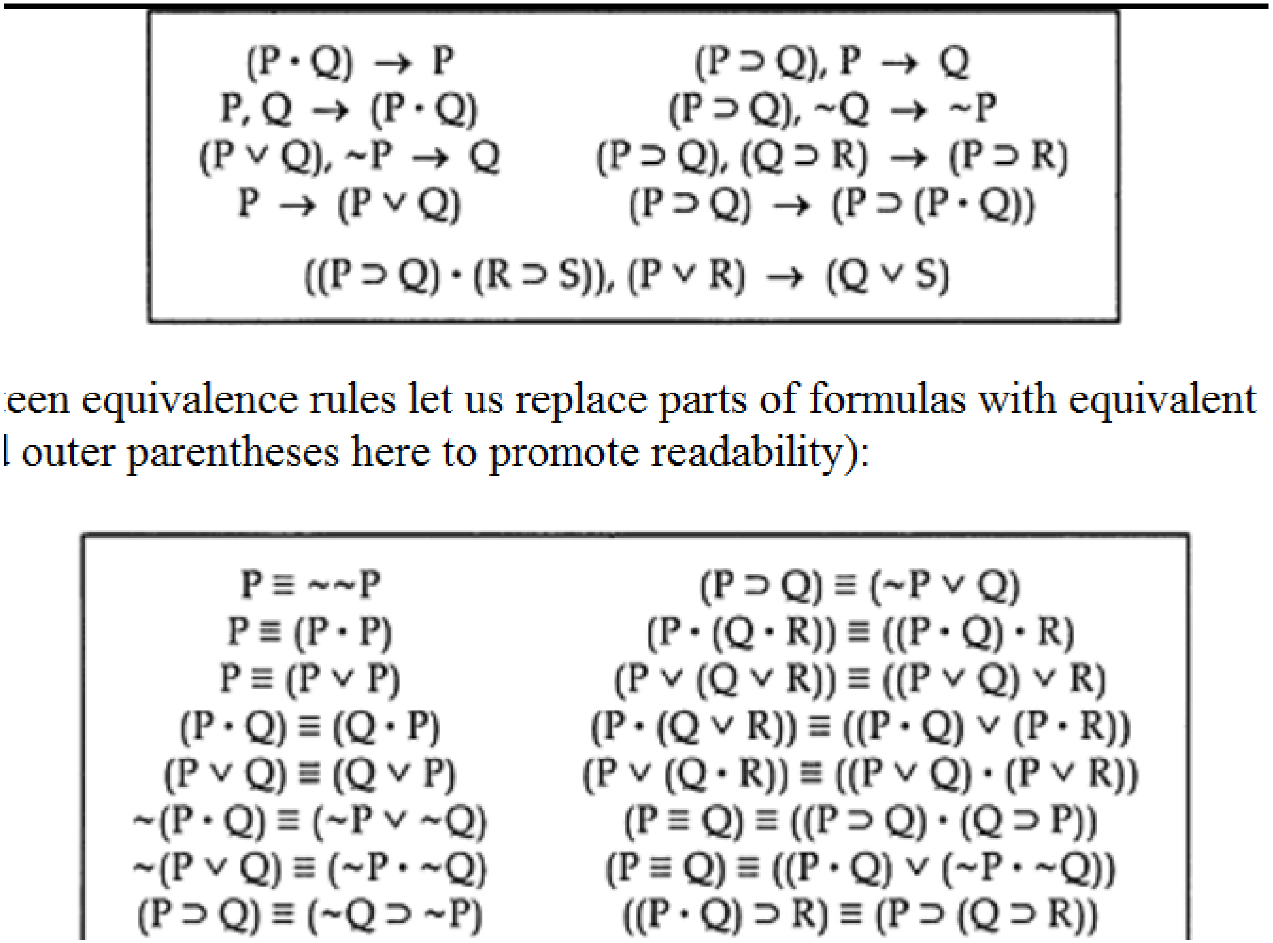
4 asm: $\sim A$ {break up 1}

5 $\therefore N$ {from 2 and 4}

$\boxed{N, \sim A, \sim P}$

Other Proof Systems

- Many sound and complete proof systems for prop logic
- Resolution Proof (later) …
- “Traditional Proofs”: More rules…



$(P \cdot Q) \rightarrow P$

$P, Q \rightarrow (P \cdot Q)$

$(P \vee Q), \sim P \rightarrow Q$

$P \rightarrow (P \vee Q)$

$(P \supset Q), P \rightarrow Q$

$(P \supset Q), \sim Q \rightarrow \sim P$

$(P \supset Q), (Q \supset R) \rightarrow (P \supset R)$

$(P \supset Q) \rightarrow (P \supset (P \cdot Q))$

$((P \supset Q) \cdot (R \supset S)), (P \vee R) \rightarrow (Q \vee S)$

een equivalence rules let us replace parts of formulas with equivalent
l outer parentheses here to promote readability):

$P \equiv \sim\sim P$

$P \equiv (P \cdot P)$

$P \equiv (P \vee P)$

$(P \cdot Q) \equiv (Q \cdot P)$

$(P \vee Q) \equiv (Q \vee P)$

$\sim(P \cdot Q) \equiv (\sim P \vee \sim Q)$

$\sim(P \vee Q) \equiv (\sim P \cdot \sim Q)$

$(P \supset Q) \equiv (\sim Q \supset \sim P)$

$(P \supset Q) \equiv (\sim P \vee Q)$

$(P \cdot (Q \cdot R)) \equiv ((P \cdot Q) \cdot R)$

$(P \vee (Q \vee R)) \equiv ((P \vee Q) \vee R)$

$(P \cdot (Q \vee R)) \equiv ((P \cdot Q) \vee (P \cdot R))$

$(P \vee (Q \cdot R)) \equiv ((P \vee Q) \cdot (P \vee R))$

$(P \equiv Q) \equiv ((P \supset Q) \cdot (Q \supset P))$

$(P \equiv Q) \equiv ((P \cdot Q) \vee (\sim P \cdot \sim Q))$

$((P \cdot Q) \supset R) \equiv (P \supset (Q \supset R))$