#### CS477 Formal Software Dev Methods

Elsa L Gunter 2112 SC, UIUC egunter@illinois.edu

http://courses.engr.illinois.edu/cs477

Slides based in part on previous lectures by Mahesh Vishwanathan, and by Gul Agha

January 18, 2018

#### Propositional Logic

The Language of Propositional Logic

- Begins with constants {T, F}
- Assumes countable set AP of propositional variables, a.k.a. propositional atoms, a.k.a. atomic propositions
- Assumes logical connectives: ∧ (and); ∨ (or); ¬ (not); ⇒ (implies);  $\Leftrightarrow$  = (if and only if)
- The set of propositional formulae PROP is the inductive closure of these as follows:
  - {**T**, **F**} ⊆ *PROP AP* ⊆ *PROP*

  - if  $A \in PROP$  then  $(A) \in PROP$  and  $\neg A \in PROP$
  - if  $A \in PROP$  and  $B \in PROP$  then  $(A \land B) \in PROP$ ,  $(A \lor B) \in PROP$ ,  $(A \Rightarrow B) \in PROP$ ,  $(A \Leftrightarrow B) \in PROP$ .
  - Nothing else is in PROP
- Informal definition; formal definition requires math foundations, set theory, fixed point theorem ...

#### Semantics of Propositional Logic: Model Theory

Model for Propositional Logic has three parts

- Mathematical set of values used as meaning of propositions
- Interpretation function giving meaning to props built from logical connectives, via structural recursion

Standard Model of Propositional Logic

- $\mathcal{B} = \{\text{true}, \text{false}\}$  boolean values
- $v : AP \rightarrow \mathcal{B}$  a valuation
- Interpretation function . . .

#### Semantics of Propositional Logic: Model Theory

Standard Model of Propositional Logic (cont)

- ullet Standard interpretation  $\mathcal{I}_{V}$  defined by structural induction on formulae:
  - $\mathcal{I}_{\nu}(T) = \text{true and } \mathcal{I}_{\nu}(F) = \text{false}$
  - If  $a \in AP$  then  $\mathcal{I}_{v}(a) = v(a)$
  - For  $p \in PROP$ , if  $\mathcal{I}_{\nu}(p) = \text{true}$  then  $\mathcal{I}_{\nu}(\neg p) = \text{false}$ , and if  $\mathcal{I}_{\nu}(p) = \mathrm{false} \ \mathrm{then} \ \mathcal{I}_{\nu}(\neg p) = \mathrm{true}$
  - For  $p, q \in PROP$ 
    - $\quad \text{ If } \mathcal{I}_{\nu}(p) = \mathrm{true} \text{ and } \mathcal{I}_{\nu}(q) = \mathrm{true} \text{, then } \mathcal{I}_{\nu}(p \wedge q) = \mathrm{true} \text{, else}$  $\mathcal{I}_{\nu}(p \wedge q) = \text{false}$
    - If  $\mathcal{I}_{\nu}(p) = \text{true}$  or  $\mathcal{I}_{\nu}(q) = \text{true}$ , then  $\mathcal{I}_{\nu}(p \vee q) = \text{true}$ , else  $\mathcal{I}_{\nu}(p \vee q) = \text{false}$
    - If  $\mathcal{I}_{\nu}(q)=\mathrm{true}$  or  $\mathcal{I}_{\nu}(p)=\mathrm{false}$ , then  $\mathcal{I}_{\nu}(p\Rightarrow q)=\mathrm{true}$ , else  $\mathcal{I}_{\nu}(p \Rightarrow q) = \text{false}$
    - $\bullet \ \text{ If } \ \mathcal{I}_{\nu}(\rho) = \mathcal{I}_{\nu}(q) \ \text{then } \ \mathcal{I}_{\nu}(\rho \Leftrightarrow q) = \mathrm{true}, \ \text{else } \ \mathcal{I}_{\nu}(\rho \Leftrightarrow q) = \mathrm{false}$

# Truth Tables

Interpretation function often described by truth table

p	q	$\neg p$	$p \wedge q$	$p \lor q$	$p \Rightarrow q$	$p \Leftrightarrow q$
true	true					
true	false					
false	true					
false	false					

#### Truth Tables

Interpretation function often described by truth table

p	q	$\neg p$	$p \wedge q$	$p \lor q$	$p \Rightarrow q$	$p \Leftrightarrow q$
true	true	false				
true	false	false				
false	true	true				
false	false	true				

#### Truth Tables

Interpretation function often described by truth table

р	q	$\neg p$	$p \wedge q$	$p \lor q$	$p \Rightarrow q$	$p \Leftrightarrow q$
true	true	false	true			
true	false	false	false			
false	true	true	false			
false	false	true	false			

## Truth Tables

Interpretation function often described by truth table

p	q	$\neg p$	$p \wedge q$	$p \lor q$	$p \Rightarrow q$	<i>p</i> ⇔ <i>q</i>
true	true	false	true	true		
true	false	false	false	true		
false	true	true	false	true		
false	false	true	false	false		

# Truth Tables

Interpretation function often described by truth table

р	q	$\neg p$	$p \wedge q$	$p \lor q$	$p \Rightarrow q$	$p \Leftrightarrow q$
true	true	false	true	true	true	
true	false	false	false	true	false	
false	true	true	false	true	true	
false	false	true	false	false	true	

# Truth Tables

Interpretation function often described by truth table

p	q	$\neg p$	$p \wedge q$	$p \lor q$	$p \Rightarrow q$	$p \Leftrightarrow q$
true	true	false	true	true	true	true
true	false	false	false	true	false	false
false	true	true	false	true	true	false
false	false	true	false	false	true	true

## Modeling Propositional Formulae

- ullet ( $\mathcal{B},\mathcal{I}$ ) is the standard model of proposition logic
- Given valuation v and proposition  $p \in PROP$ , write  $v \models p$  iff  $\mathcal{I}_{v}(p) = \text{true}$ 
  - More fully written as  $\mathcal{B}, \mathcal{I}, v \models p$

  - Say v satisfies p, or v models p
    Write v ⊭ p if T<sub>v</sub>(p) = false
- p is satisfiable if there exists valuation v such that  $v \models p$
- p is valid, a.k.a. a tautology if for every valuation v we have  $v \models p$
- p is logically equivalent to q,  $p \equiv q$  if for every valuation, v, we have  $v \models p \text{ iff } v \models q$ 
  - Claim: Logical equivalence is an equivalence relation

Example Tautology

$$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$$

l	Α	В	$A \Rightarrow B$	$(A \Rightarrow B) \Rightarrow B$	$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$
	true	true			
ĺ	true	false			
ĺ	false	true			
ĺ	false	false			

# Example Tautology

$$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$$

Α	В	$A \Rightarrow B$	$(A \Rightarrow B) \Rightarrow B$	$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$
true	true	true		
true	false	false		
false	true	true		
false	false	true		

# Example Tautology

$$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$$

Α	В	$A \Rightarrow B$	$(A \Rightarrow B) \Rightarrow B$	$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$
true	true	true	true	
true	false	false	true	
false	true	true	true	
false	false	true	false	

# Example Tautology

$$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$$

Α	В	$A \Rightarrow B$	$(A \Rightarrow B) \Rightarrow B$	$A \Rightarrow ((A \Rightarrow B) \Rightarrow B)$
true	true	true	true	true
true	false	false	true	true
false	true	true	true	true
false	false	true	false	true

# Example Tautology – Your Turn

## Example: Logical Equivalence

$$A \Rightarrow B \equiv ((\neg A) \lor B)$$

A	В	$A \Rightarrow B$	$\neg A$	$(\neg A) \lor B$
true	true	true	false	true
true	false	false	false	false
false	true	true	true	true
false	false	true	true	true

# More Useful Logical Equivalences

$$\neg \neg A \equiv A \qquad \neg T \equiv F \qquad \neg F \equiv T \\
(A \lor A) \equiv A \qquad (A \lor B) \lor C \equiv A \lor (B \lor C) \\
(A \land A) \equiv A \qquad (A \land B) \land C \equiv A \land (B \land C) \\
A \lor B \equiv B \lor A \qquad \neg (A \lor B) \equiv (\neg A) \land (\neg B) \\
A \land B \equiv B \land A \qquad \neg (A \land B) \equiv (\neg A) \lor (\neg B) \\
(A \land \neg A) \equiv F \qquad A \lor (B \land C) \equiv (A \lor B) \land (A \lor C) \\
(A \lor \neg A) \equiv T \qquad (A \land B) \lor C \equiv (A \lor C) \land (B \lor C) \\
(T \land A) \equiv A \qquad A \land (B \lor C) \equiv (A \land B) \lor (A \land C) \\
(T \lor A) \equiv T \qquad (A \land B) \lor C \equiv (A \land C) \lor (B \land C) \\
(F \land A) \equiv F \qquad (F \lor A) \equiv A$$

## Logical Equivalence a Structural Congruence

#### Theorem

Logical equivalence is a structural congruence. That is, if  $p \equiv p'$  and  $q \equiv q'$  then

- $p \wedge q \equiv p' \wedge q'$

## Logical Equivalence a Structural Congruence

#### Proof.

- Assume  $p \equiv p'$  and  $q \equiv q'$
- **Hyp**: Then for all valuations v,  $v \models p$  iff  $v \models p'$  and  $v \models q$  iff  $v \models q'$ , i.e.  $\mathcal{I}_{v}(p) = \text{true iff } \mathcal{I}_{v}(p') = \text{true and } \mathcal{I}_{v}(q) = \text{true iff }$  $\mathcal{I}_{\nu}(q') = \text{true}$
- Case 4: Show  $p \Rightarrow q \equiv p' \Rightarrow q'$ 
  - Other cases done same way
- Need to show for all v,  $\mathcal{I}_v(p\Rightarrow q)=\mathrm{true}$  iff  $\mathcal{I}_v(p'\Rightarrow q')=\mathrm{true}$
- ullet Need to show if  $\mathcal{I}_{\nu}(p\Rightarrow q)=\mathrm{true}$  then  $\mathcal{I}_{\nu}(p'\Rightarrow q')=\mathrm{true}$ , and if  $\mathcal{I}_{\nu}(p'\Rightarrow q')=\mathrm{true}\;\mathrm{then}\;\mathcal{I}_{\nu}(p\Rightarrow q)=\mathrm{true}\;$

## Logical Equivalence a Structural Congruence

#### Proof.

- **●** (**⇒**)
  - Assume  $\mathcal{I}_{\nu}(p \Rightarrow q) = \text{true}$
  - $\bullet$  By closure property of inductive definition of  $\mathcal{I},$  either  $\mathcal{I}_{v}(\mathit{q}) = \mathrm{true}$  or
  - Therefore, by **Hyp**, either  $\mathcal{I}_{\nu}(q') = \text{true or } \mathcal{I}_{\nu}(p') = \text{false}$ 
    - $\bullet$  since  ${\cal B}$  has only two elements, and  ${\cal I}_{\nu}$  total (proof?)
  - ullet By  ${\mathcal I}$  def, have  ${\mathcal I}_{\scriptscriptstyle V}({p^\prime}\Rightarrow {q^\prime})$
- **●** (←=)

Non-standard Model of Propositional Logic

Other models possible

Example:

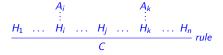
- $\mathcal{C} = \{\text{true}, \text{false}, \bot\}$
- ullet Valuations assign values in  ${\cal C}$  to propositional atoms
- If  $\mathcal{J}_w(p) = \bot$  then  $\mathcal{J}_w(\neg p) = \bot$ , otherwise same as for  $\mathcal{I}$
- $\mathcal{J}_w(p) = \bot$  or  $\mathcal{J}_w(q) = \bot$  then  $\mathcal{J}_w(\neg p) = \bot$ ,  $\mathcal{J}_w(p \land q) = \bot$ ,  $\mathcal{J}_w(p \lor q) = \bot$ ,  $\mathcal{J}_w(p \Rightarrow q) = \bot$ , and  $\mathcal{J}_w(p \Leftrightarrow q) = \bot$ ; otherwise same as for  ${\cal I}$
- Note:  $A \lor \neg A \not\equiv \mathbf{T}$
- Other variants possible

#### Proofs in Propositional Logic

- Natural Deduction proof is tree and a discharge function
  - Nodes are instances of inference rules
  - Leaves are assumptions of subproofs
  - Discharge function maps each leaf of the tree to an ancestor as prescribed by the inference rules

#### Natural Deduction Inference Rules

- Inference rule has hypotheses and conclusion
- Conclusion a single proposition
- Hypotheses zero or more propositions, possibly with (discharged)
- Rule with no hypotheses called an axiom
- Inference rule graphically presents as



#### Natural Deduction Inference Rules

- Inference rules associated with connectives
- Two main kinds of inference rules:
  - Introduction says how to conclude proposition made from connective

#### Natural Deduction Inference Rules

- Inference rules associated with connectives
- Two main kinds of inference rules:
  - Introduction says how to conclude proposition made from connective is true
    - Example:



Natural Deduction Inference Rules

• Two main kinds of inference rules:

• Inference rules associated with connectives

is true

# Natural Deduction Inference Rules

- Inference rules associated with connectives
- Two main kinds of inference rules:
  - Introduction says how to conclude proposition made from connective is true
    - Example:

$$\begin{array}{c}
A \\
\vdots \\
B \\
\hline
A \rightarrow B
\end{array}$$
 Imp

• Eliminations – says how to use a proposition made from connective to prove result

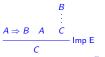
 $\frac{B}{A \Rightarrow B} \operatorname{Imp} I$ 

• Eliminations – says how to use a proposition made from connective to prove result

• Introduction – says how to conclude proposition made from connective

Example:

Example:



## Introduction Rules

Truth Introduction:

And Introduction:

$$\frac{1}{T}$$
TI

$$\frac{A \quad B}{A \land B}$$
 And  $A \land B$ 

Or Introduction:

$$\frac{A}{A \times A \times B}$$
 Or<sub>L</sub>

$$\frac{A \vee B}{B \vee A \vee B}$$
 Or<sub>R</sub> I

Not Introduction:

Implication Introduction:

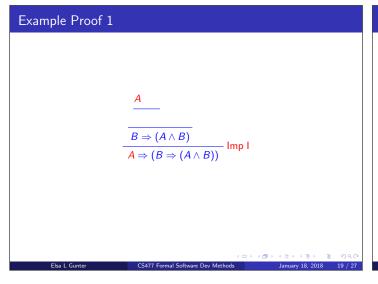


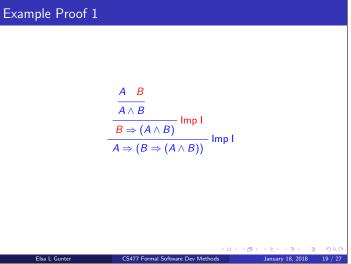


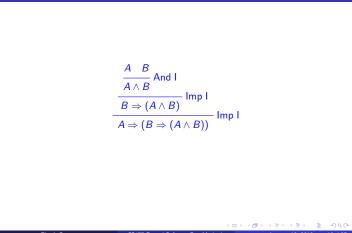
No False Introduction

#### Example Proof 1

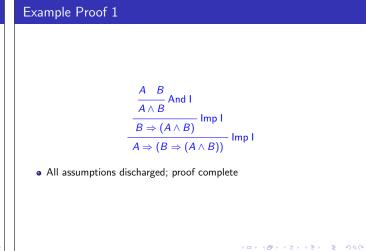
$$A \Rightarrow (B \Rightarrow (A \land B))$$

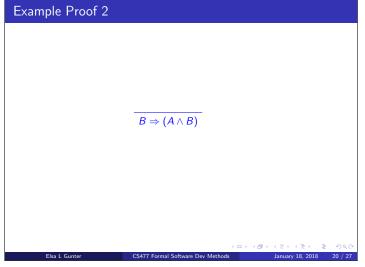


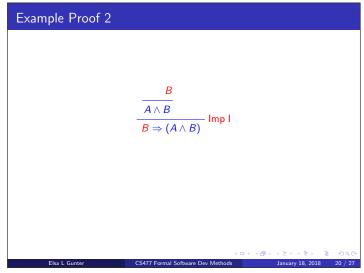




Example Proof 1







## Example Proof 2

$$\frac{\frac{A \quad B}{A \wedge B} \text{And I}}{B \Rightarrow (A \wedge B)} \text{Imp I}$$

Isa L Gunter CS477 Formal Software Dev Methods January 18, 2

# Example Proof 2

$$\frac{\frac{A? \quad B}{A \land B} \text{ And I}}{B \Rightarrow (A \land B)} \text{ Imp I}$$

# Example Proof 2

$$\frac{\frac{A \quad B}{A \land B} \text{ And I}}{B \Rightarrow (A \land B)} \text{ Imp I}$$

- Closed proofs must discharge all hypotheses
- $\bullet$  Otherwise have theorem relative to / under undischarged hypotheses
- ullet Here have proved "Assuming A, we have  $B\Rightarrow (A\wedge B)$

# Discharging Hypothesis

$$A \Rightarrow (A \wedge A)$$

+ロト・(**が**) + (さ) + (き) - き - かく()

a L Gunter CS477 Formal Software Dev Method

#### January 18, 2018 21 / 27

# Discharging Hypothesis

$$\frac{\frac{A \quad A}{A \land A} \text{ And I}}{A \Rightarrow (A \land A)} \text{ Imp I}$$

<□> <<mark>□</mark>> <<u>□</u>> <<u>□</u> < <u>□</u> <

# Discharging Hypothesis

$$\frac{\frac{A \quad A}{A \wedge A} \text{ And I}}{A \Rightarrow (A \wedge A)} \text{ Imp I}$$

 Imp I (and other rules discharging assumptions) may discharge multiple instance of hypothesis

(□) (∰) (E) (E) E 9Q@

#### Discharging Hypothesis

$$\frac{\frac{A \quad A}{A \wedge A} \text{ And I}}{A \Rightarrow (A \wedge A)} \text{ Imp I} \qquad \qquad \overline{A \Rightarrow (B \Rightarrow A)}$$

• Imp I (and other rules discharging assumptions) may discharge multiple instance of hypothesis

# Discharging Hypothesis

$$\frac{\frac{A}{A \wedge A} \text{And I}}{A \Rightarrow (A \wedge A)} \text{Imp I} \qquad \frac{\frac{A}{B \Rightarrow A} \text{Imp I}}{A \Rightarrow (B \Rightarrow A)} \text{Imp I}$$

• Imp I (and other rules discharging assumptions) may discharge multiple instance of hypothesis

## Discharging Hypothesis

$$\frac{\frac{A \quad A}{A \land A} \text{And I}}{A \Rightarrow (A \land A)} \text{Imp I} \qquad \frac{\frac{A}{B \Rightarrow A} \text{Imp I}}{A \Rightarrow (B \Rightarrow A)} \text{Imp I}$$

• Imp I (and other rules discharging assumptions) may discharge multiple instance of hypothesis

# Discharging Hypothesis

$$\frac{A \quad A}{A \wedge A} \text{And I}$$

$$A \Rightarrow (A \wedge A) \quad \text{Imp I}$$

$$A \Rightarrow (B \Rightarrow A) \quad \text{Imp I}$$

$$A \Rightarrow (B \Rightarrow A) \quad \text{Imp I}$$

- Imp I (and other rules discharging assumptions) may discharge multiple instance of hypothesis
- Or may discharge none at all
- Every assumption instance discharged only once

# Your Turn

$$A \Rightarrow (A \lor B)$$

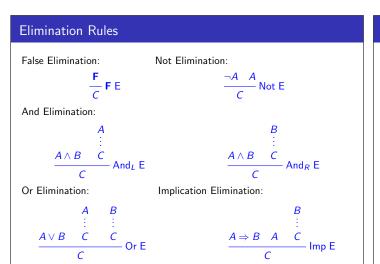
## Elimination Rules

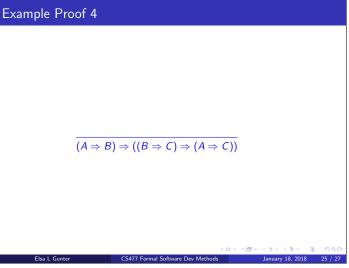
- So far, have rules to "introduce" logical connectives into propositions
- No rules for how to "use" logical connectives
  - No assumptions with logical connectives
- Need "elimination" rules
- Example: Can't prove

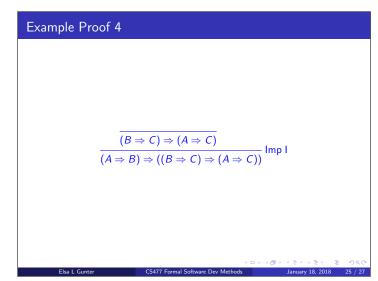
$$(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))$$

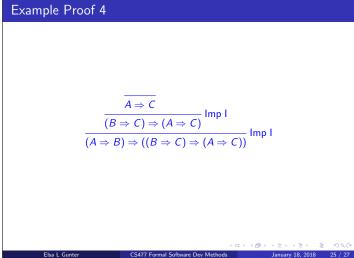
with what we have so far

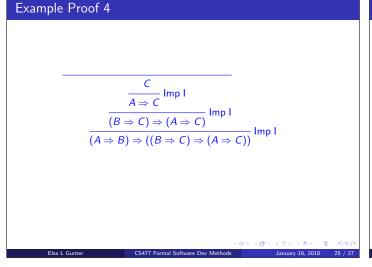
- Elimination rules assume assumption with a connective; have general conclusion
  - Generally needs additional hypotheses

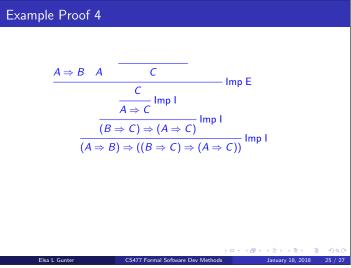




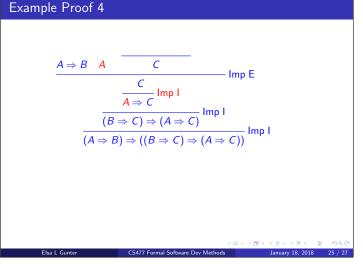


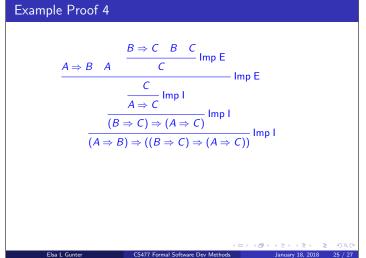


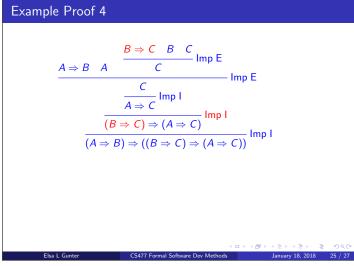


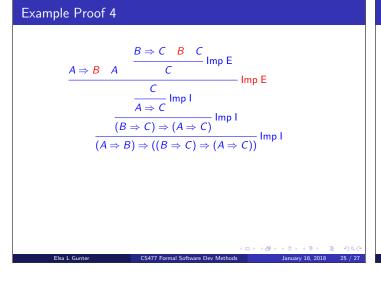


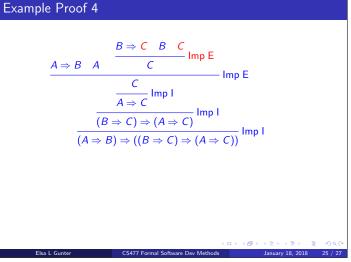
# Example Proof 4 $\frac{A \Rightarrow B \quad A \qquad C}{C \qquad \text{Imp I}}$ $\frac{C}{A \Rightarrow C \quad \text{Imp I}}$ $\frac{(B \Rightarrow C) \Rightarrow (A \Rightarrow C)}{(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}$ Imp I











# Some Well-Known Derived Rules

Modus Ponens

$$\frac{A \Rightarrow B \quad A}{B} \text{MP}$$

$$\frac{A \Rightarrow B \quad A \quad B}{B} \operatorname{Imp} \mathsf{E}$$

Left Conjunct

$$\frac{A \wedge B}{A}$$
 AndL

$$\frac{A \wedge B \quad A}{A} \operatorname{And}_{L} \mathsf{E}$$

Right Conjunct

$$\frac{A \wedge B}{B}$$
 AndR

$$\frac{A \wedge B \quad A}{A} \operatorname{And}_{R} \mathsf{E}$$

←□→ ←□→ ←∃→ ←∃→ □

sa L Gunter CS4

CS477 Formal Software Dev Method

ary 18, 2018 26

Your Turn

$$(A \wedge B) \Rightarrow (A \vee B)$$

←□→ ←□→ ←□→ ←□→ □ ←○○

unter CS477 Formal Software Dev I

nuary 18, 2018 27 / 27