CS477 Formal Software Development Methods

Elsa L Gunter 2112 SC, UIUC

egunter@illinois.edu

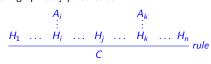
http://courses.engr.illinois.edu/cs477

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

January 30, 2014

Proofs in Propositional Logic

- Natural Deduction proofs are
 - trees with nodes that are inference rules
 - and a discharge function
- Inference rule has hypotheses and conclusion
- Conclusion: a single proposition
- Hypotheses: zero or more propositions, each possibly with hypotheses
 - Rule with no hypotheses called an axiom
- Inference rule graphically presents as



- Discharge function: maps proof tree leaves with node (induction rule) introducing it
- Instance of inference rule above may discharge A_i and A_j in a proof using rule

Elsa L Gunter ()

Inference Rules

- Inference rules associated with connectives
- Two main kinds of (non-axiom) inference rules:
 - Introduction says how to conclude proposition made from connective is true
 - Proposition below the line is instance of the connective
 - Hypotheses are (some of) connective components
 - Eliminations says how to use a proposition made from connective to prove result
 - Conclusion: propositional atom (i.e. any conclusion can be instance)
 - Hypotheses:
 - One that is instance of connective
 - Zero or more with proposition as conclusion, but some connective component as its hypotheses

Introduction Rules

Truth Introduction: And Introduction:

$$\frac{1}{T}$$
TT

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

Or Introduction:

$$\frac{A}{A \vee B} \operatorname{Or}_{L} \operatorname{I} \qquad \qquad \frac{B}{A \vee B} \operatorname{Or}_{R} \operatorname{I}$$

$$\frac{B}{A \vee B} \operatorname{Or}_R$$

Not Introduction:

Implication Introduction:



No False Introduction

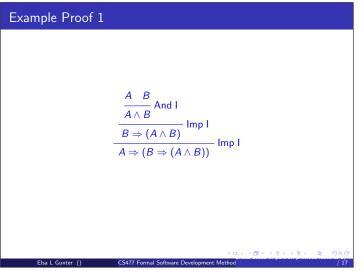
Example Proof 1

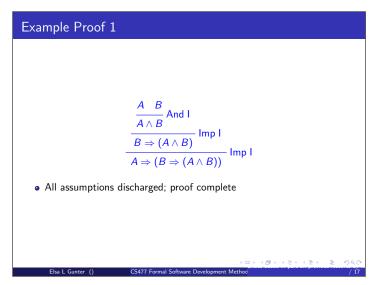
 $A \Rightarrow (B \Rightarrow (A \land B))$

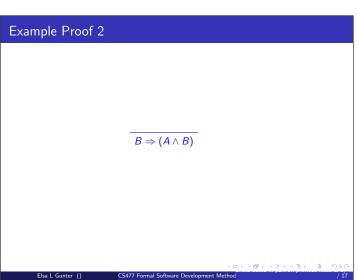
Example Proof 1

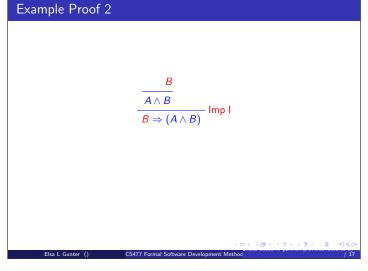
$$\frac{B \Rightarrow (A \land B)}{A \Rightarrow (B \Rightarrow (A \land B))} \text{Imp}$$

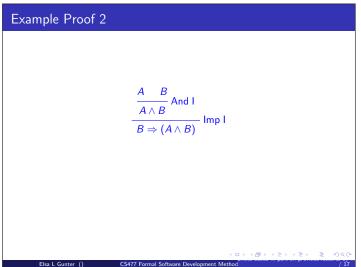
Example Proof 1 $\frac{A \quad B}{A \wedge B} \quad || \text{Imp I}| \\ B \Rightarrow (A \wedge B) \quad || \text{Imp I}| \\ A \Rightarrow (B \Rightarrow (A \wedge B)) \quad || \text{Imp I}|$











Example Proof 2

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

Elsa L Gunter (

CS477 Formal Software Development Method

Example Proof 2

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

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

lea I Gunter ()

5477 Formal Software Development Method

(불) 불 위익(연 / 17

Discharging Hypothesis

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

Elsa L Gunter (

S477 Formal Software Development Method

Discharging Hypothesis

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

Elsa L Gunter

S477 Formal Software Development Meti

/ 17

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

<□> < □ > < □ > < ≧ > < ≧ > < ≥ < > ○< ○

Discharging Hypothesis

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

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

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

lsa L Gunter ()

477 Formal Software Development Method

/ 1

Discharging Hypothesis

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

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

$$A \Rightarrow (B \Rightarrow A) \operatorname{Imp}$$

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

Discharging Hypothesis

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

$$\frac{A \rightarrow (A \wedge A)}{A \rightarrow (A \wedge A)} \text{Imp} \mid$$

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

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

Discharging Hypothesis

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

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

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

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

Your Turn

 $A \Rightarrow (A \lor B)$

Elimination Rules

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
 - Generally needs additional hypotheses

 $\frac{A \lor B \quad C \quad C}{C} \text{ Or E}$

Not Elimination:

 $\frac{\neg A \quad A}{C}$ Not E

And Elimination:

Or Elimination:

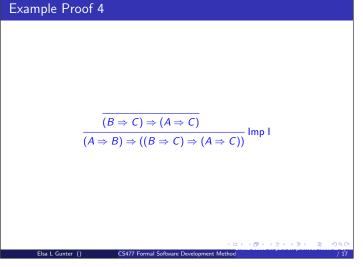
False Elimination:

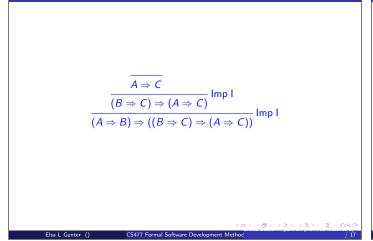
 $\begin{array}{ccc}
 & A \\
\vdots \\
 & A \land B & C \\
\hline
 & C & And_L E
\end{array}$

 $\frac{A \land B \quad C}{C} \quad And_R \; E$

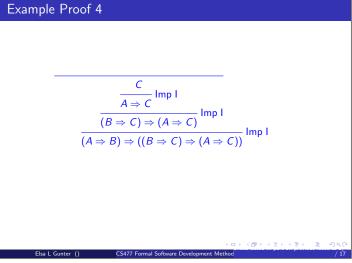
Implication Elimination:

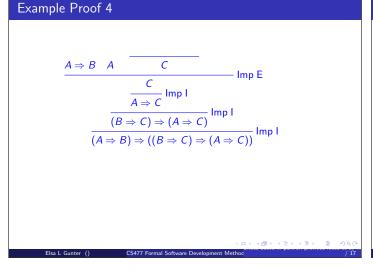
Example Proof 4 $\overline{(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}$

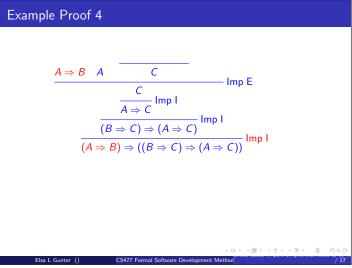




Example Proof 4







Example Proof 4

$$\frac{A \Rightarrow B \quad A \qquad C}{\frac{C}{A \Rightarrow C} \text{Imp I}}$$

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

Example Proof 4

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

$$\frac{\frac{C}{A \Rightarrow C} \operatorname{Imp I}}{\frac{(B \Rightarrow C) \Rightarrow (A \Rightarrow C)}{(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))} \operatorname{Imp I}$$

Example Proof 4

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

$$\frac{(B \Rightarrow C) \Rightarrow (A \Rightarrow C)}{(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))} \operatorname{Imp I}$$

Example Proof 4

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

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

$$\frac{(B \Rightarrow C) \Rightarrow (A \Rightarrow C)}{(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))} \operatorname{Imp I}$$

Example Proof 4

$$\frac{A \Rightarrow B \quad A}{C} \frac{B \Rightarrow C \quad B \quad C}{C} \text{Imp E}$$

$$\frac{C}{A \Rightarrow C} \text{Imp I}$$

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

Some Well-Known Derived Rules

Modus Ponens

$$A \Rightarrow B \quad A$$
 \longrightarrow

MF

 $\frac{A \Rightarrow B \quad A}{B} \text{ MP} \qquad \qquad \frac{A \Rightarrow B \quad A \quad B}{B} \text{ Imp E}$

Left Conjunct

$$\frac{A \wedge B}{\longrightarrow}$$
 And L

 $\frac{A \wedge B}{A} \text{AndL} \qquad \frac{A \wedge B \quad A}{A} \text{And}_{L} \text{ E}$

Right Conjunct

$$\frac{A \wedge B}{B}$$
 And F

 $\frac{A \wedge B}{R}$ And R $\frac{A \wedge B}{A}$ And R E

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

Assumptions in Natural Deduction

- Problem: Keeping track of hypotheses and their discharge in Natural Deduction is HARD!
- Solution: Use sequents to track hypotheses
- A sequent is a pair of
 - A set of propositions (called assumptions, or hypotheses of sequent)
 - A proposition (called conclusion of sequent)
- More generally (not here), allow set of hypotheses and set of conclusions

Nat. Ded. Introduction Sequent Rules

 □ is set of propositions (assumptions/hypotheses) Hypothesis Introduction:

$$\frac{}{\Gamma \cup \{A\} \vdash A}$$
 Hyp

Truth Introduction:

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \land B} \text{ And } I$$

Or Introduction:

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \lor P} \operatorname{Or}_{L}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \lor B} \operatorname{Or}_{L} \operatorname{I} \qquad \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \lor B} \operatorname{Or}_{R} \operatorname{I}$$

Not Introduction:

Implication Introduction:

$$\frac{\Gamma \cup \{A\} \vdash \mathbf{F}}{\Gamma \vdash \neg A} \mathsf{\,Not\,\,} \mathsf{I}$$

$$\frac{\Gamma \cup \{A\} \vdash B}{\Gamma \vdash A \Rightarrow B} \operatorname{Imp} I$$

Nat. Ded. Elimination Sequent Rules

Γ is set of propositions (assumptions/hypotheses) Not Elimination: Implication Elimination:

$$\frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash C} \text{ Not E} \qquad \frac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash A \quad \Gamma \cup \{B\} \vdash C}{\Gamma \vdash C} \text{ Imp E}$$

$$\frac{\Gamma \vdash A \land B \quad \Gamma \cup \{A\} \vdash C}{\Gamma \vdash C} \operatorname{And}_{L} \mathsf{E} \qquad \frac{\Gamma \vdash A \land B \quad \Gamma \cup \{B\} \vdash C}{\Gamma \vdash C} \operatorname{And}_{R} \mathsf{E}$$

False Elimination:

Or Elimination:

$$\frac{\Gamma \vdash \mathbf{F}}{\Gamma \vdash C} \mathbf{F} \mathsf{E} \qquad \frac{\Gamma \vdash A \lor B \quad \Gamma \cup \{A\} \vdash C \quad \Gamma \cup \{B\} \vdash C}{\Gamma \vdash C} \mathsf{Or} \, \mathsf{E}$$

Example Proof 4, Revisited

$$\frac{}{\{\}\vdash (A\Rightarrow B)\Rightarrow ((B\Rightarrow C)\Rightarrow (A\Rightarrow C))}$$

Example Proof 4, Revisited

$$\frac{ A \Rightarrow B \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}{\{\} \vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C)\}} \text{Imp I}$$

Example Proof 4, Revisited

$$\frac{\overline{\{A \Rightarrow B, B \Rightarrow C\} \vdash A \Rightarrow C}}{\{A \Rightarrow B\} \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)} \operatorname{Imp} I$$

$$\{ \} \vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C)) \operatorname{Imp} I$$

Example Proof 4, Revisited

$$\Gamma_3 = \{A \Rightarrow B, B \Rightarrow C, A\}$$

$$\frac{\{A \Rightarrow B, B \Rightarrow C, A\} \vdash C}{\{A \Rightarrow B, B \Rightarrow C\} \vdash A \Rightarrow C} \operatorname{Imp} I$$

$$\frac{\{A \Rightarrow B, B \Rightarrow C\} \vdash A \Rightarrow C}{\{A \Rightarrow B\} \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)} \operatorname{Imp} I$$

$$\{\} \vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))$$

Example Proof 4, Revisited

$$\Gamma_3 = \{A \Rightarrow B, B \Rightarrow C, A\}$$

$$\Gamma_4 = \{A \Rightarrow B, B \Rightarrow C, A, B\}$$

$$\frac{\{A \Rightarrow B, B \Rightarrow C, A\} \vdash C}{\{A \Rightarrow B, B \Rightarrow C\} \vdash A \Rightarrow C} \qquad \text{Imp I}$$

$$\frac{\{A \Rightarrow B, B \Rightarrow C\} \vdash A \Rightarrow C}{\{A \Rightarrow B\} \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)} \qquad \text{Imp I}$$

$$\frac{\{A \Rightarrow B\} \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}{\{\} \vdash (A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))} \qquad \text{Imp I}$$

Example Proof 4, Revisited

$$\Gamma_3 = \{ A \Rightarrow B, B \Rightarrow C, A \}$$

$$\Gamma_4 = \{ A \Rightarrow B, B \Rightarrow C, A, B \}$$

Tryp
$$\frac{\Gamma_3 \vdash A \Rightarrow B}{\Gamma_3 \vdash A} \qquad \Gamma_4 \vdash C$$

$$\frac{\{A \Rightarrow B, B \Rightarrow C, A\} \vdash C}{\{A \Rightarrow B, B \Rightarrow C\} \vdash A \Rightarrow C} \qquad \text{Imp I}$$

$$\frac{\{A \Rightarrow B, B \Rightarrow C\} \vdash A \Rightarrow C}{\{A \Rightarrow B\} \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)} \qquad \text{Imp I}$$

$$\frac{\{A \Rightarrow B\} \vdash (B \Rightarrow C) \Rightarrow (A \Rightarrow C)}{\{A \Rightarrow B\} \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))} \qquad \text{Imp I}$$

Example Proof 4, Revisited

$$\Gamma_3 = \{ A \Rightarrow B, \ B \Rightarrow C, \ A \}$$

$$\Gamma_4 = \{ A \Rightarrow B, \ B \Rightarrow C, \ A, \ B \}$$

Example Proof 4, Revisited

$$\begin{split} &\Gamma_3 = \{A \Rightarrow B, \ B \Rightarrow C, \ A\} \\ &\Gamma_4 = \{A \Rightarrow B, \ B \Rightarrow C, \ A, \ B\} \\ &\Gamma_5 = \{A \Rightarrow B, \ B \Rightarrow C, \ A, \ B, \ {\color{red}C}\} \end{split}$$

$$\frac{\text{Hyp}}{\Gamma_3 \vdash A \Rightarrow B} \quad \frac{\text{Hyp}}{\Gamma_3 \vdash A} \quad \frac{\overline{\Gamma_4 \vdash B} \Rightarrow C}{\Gamma_4 \vdash B} \quad \overline{\Gamma_5 \vdash C} \quad \text{Imp E}$$

$$\frac{\{A \Rightarrow B, B \Rightarrow C, A\} \vdash C}{\{A \Rightarrow B, B \Rightarrow C\} \vdash A \Rightarrow C} \quad \text{Imp I}$$

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

Example Proof 4, Revisited

$$\begin{split} &\Gamma_3 = \{A \Rightarrow B, \ B \Rightarrow C, \ A\} \\ &\Gamma_4 = \{A \Rightarrow B, \ B \Rightarrow C, \ A, \ B\} \\ &\Gamma_5 = \{A \Rightarrow B, \ B \Rightarrow C, \ A, \ B, \ C\} \end{split}$$

$$\frac{\text{Hyp}}{\Gamma_3 \vdash A \Rightarrow B} \quad \frac{\text{Hyp}}{\Gamma_3 \vdash A} \quad \frac{\frac{\text{Hyp}}{\Gamma_4 \vdash B \Rightarrow C} \quad \overline{\Gamma_4 \vdash B} \quad \overline{\Gamma_5 \vdash C}}{\Gamma_4 \vdash C} \quad \text{Imp E}$$

$$\frac{\{A \Rightarrow B, B \Rightarrow C, A\} \vdash C}{\{A \Rightarrow B, B \Rightarrow C\} \vdash A \Rightarrow C} \quad \text{Imp I}$$

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

CS477 Formal Software Development Meti

Example Proof 4, Revisited

$$\Gamma_3 = \{A \Rightarrow B, B \Rightarrow C, A\}$$

$$\Gamma_4 = \{A \Rightarrow B, B \Rightarrow C, A, B\}$$

$$\Gamma_5 = \{A \Rightarrow B, B \Rightarrow C, A, B, C\}$$

$$\frac{\text{Hyp}}{\Gamma_3 \vdash A \Rightarrow B} \quad \frac{\text{Hyp}}{\Gamma_3 \vdash A} \quad \frac{\frac{\text{Hyp}}{\Gamma_4 \vdash B \Rightarrow C} \quad \frac{\text{Hyp}}{\Gamma_4 \vdash B} \quad \overline{\Gamma_5 \vdash C}}{\Gamma_4 \vdash C} \quad \text{Imp E}$$

$$\frac{\{A \Rightarrow B, B \Rightarrow C, A\} \vdash C}{\{A \Rightarrow B, B \Rightarrow C\} \vdash A \Rightarrow C} \quad \text{Imp I}$$

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

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

Example Proof 4, Revisited

$$\begin{split} &\Gamma_3 = \{A \Rightarrow B, \ B \Rightarrow C, \ A\} \\ &\Gamma_4 = \{A \Rightarrow B, \ B \Rightarrow C, \ A, \ B\} \\ &\Gamma_5 = \{A \Rightarrow B, \ B \Rightarrow C, \ A, \ B, \ {\color{red}C}\} \end{split}$$

$$\Gamma_4 = \{A \Rightarrow B, B \Rightarrow C, A, B\}$$

 $\Gamma_5 = \{A \Rightarrow B, B \Rightarrow C, A, B, C\}$

$$\frac{\text{Hyp}}{\Gamma_3 \vdash A \Rightarrow B} \quad \frac{\text{Hyp}}{\Gamma_3 \vdash A} \quad \frac{\text{Hyp}}{\Gamma_4 \vdash B \Rightarrow C} \quad \frac{\text{Hyp}}{\Gamma_4 \vdash B} \quad \frac{\text{Hyp}}{\Gamma_5 \vdash C} \quad \text{Imp E}$$

$$\frac{\{A \Rightarrow B, B \Rightarrow C, A\} \vdash C}{\{A \Rightarrow B, B \Rightarrow C\} \vdash A \Rightarrow C} \quad \text{Imp I}$$

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

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