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

February 2, 2013

Logical Equivalence a Structural Congruence

Theorem

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

1. $\neg p \equiv \neg p'$
2. $p \wedge q \equiv p' \wedge q'$
3. $p \vee q \equiv p' \vee q'$
4. $p \Rightarrow q \equiv p' \Rightarrow q'$
5. $p \Leftrightarrow q \equiv p' \Leftrightarrow q'$

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. $\mathcal{I}_v(p) = \mathrm{true}$ iff $\mathcal{I}_v(p') = \mathrm{true}$ and $\mathcal{I}_v(q) = \mathrm{true}$ iff $\mathcal{I}_v(q') = \mathrm{true}$
- 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 $\mathcal{I}_v(p' \Rightarrow q') = \mathrm{true}$
- Fix v
- Need to show if $\mathcal{I}_v(p \Rightarrow q) = \mathrm{true}$ then $\mathcal{I}_v(p' \Rightarrow q') = \mathrm{true}$, and if $\mathcal{I}_v(p' \Rightarrow q') = \mathrm{true}$ then $\mathcal{I}_v(p \Rightarrow q) = \mathrm{true}$

$\square$

Logical Equivalence a Structural Congruence

Proof.

- $(\Longrightarrow)$
  - Assume $\mathcal{I}_v(p \Rightarrow q) = \mathrm{true}$
  - By closure property of inductive definition of $\mathcal{I}$, either $\mathcal{I}_v(q) = \mathrm{true}$ or $\mathcal{I}_v(p) = \mathrm{false}$.
  - Therefore, by **Hyp**, either $\mathcal{I}_v(q') = \mathrm{true}$ or $\mathcal{I}_v(p') = \mathrm{false}$
    - since $\mathcal{B}$ has only two elements, and $\mathcal{I}_v$ total (proof?)
  - By $\mathcal{I}$ def, have $\mathcal{I}_v(p' \Rightarrow q')$
- $(\Longleftarrow)$ Proof same, swapping primed for unprimed $\square$

Non-standard Model of Propositional Logic

Other models possible
Example:

- $\mathcal{C} = \{\text{true}, \text{false}, \perp\}$
- Valuations w assign values in $\mathcal{C}$ to propositional atoms
- If $\mathcal{J}_w(p) = \perp$ then $\mathcal{J}_w(\neg p) = \perp$, otherwise same as for $\mathcal{I}$
- $\mathcal{J}_w(p) = \perp$ or $\mathcal{J}_w(q) = \perp$ then $\mathcal{J}_w(\neg p) = \perp$, $\mathcal{J}_w(p \wedge q) = \perp$, $\mathcal{J}_w(p \vee q) = \perp$, $\mathcal{J}_w(p \Rightarrow q) = \perp$, and $\mathcal{J}_w(p \Leftrightarrow q) = \perp$; otherwise same as for $\mathcal{I}$
- Note: $A \vee \neg A \not\equiv \mathbf{T}$

Proofs in Propositional Logic

- Natural Deduction proofs are trees with nodes that are inference rules
- Inference rule has hypotheses and conclusion
- Conclusion a single proposition
- Hypotheses zero or more propositions, possibly with hypotheses
- Two main kinds of inference rules:
  - Introduction – says how to conclude proposition made from connective is true
  - Eliminations – says how to use a proposition made from connective to prove result
- Inference rules associated with connectives
- Rule with no hypotheses called an axiom

Introduction Rules

Truth Introduction:

$$\frac{}{\mathbf{T}}\ \mathbf{T}\ \mathbf{I}$$

And Introduction:

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

Or Introduction:

$$\frac{A}{A \vee B}\ \text{Or}_L\ \text{I} \qquad \frac{B}{A \vee B}\ \text{Or}_R\ \text{I}$$

Not Introduction:

$$\frac{\begin{array}{c} A \\ \vdots \\ \mathbf{F} \end{array}}{\neg A}\ \text{Not I}$$

Implication Introduction:

$$\frac{\begin{array}{c} A \\ \vdots \\ B \end{array}}{A \Rightarrow B}\ \text{Imp I}$$

No False Introduction

Example Proof 1

$$\frac{}{A \Rightarrow (B \Rightarrow (A \wedge B))}$$

Example Proof 1

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

Example Proof 1

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

Example Proof 1

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

Example Proof 1

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

- All assumptions discharged; proof complete

Example Proof 2

$$\frac{}{B \Rightarrow (A \wedge B)}$$

Example Proof 2

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

Example Proof 2

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

Example Proof 2

$$\dfrac{\dfrac{{\color{red}A?} \quad B}{A \wedge B}\,\text{And I}}{B \Rightarrow (A \wedge B)}\,\text{Imp I}$$

Example Proof 2

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

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

Discharging Hypothesis

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

Discharging Hypothesis

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

Discharging Hypothesis

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

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

Discharging Hypothesis

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

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

Discharging Hypothesis

$$\cfrac{\cfrac{A \quad A}{A \wedge A}\,\text{And I}}{A \Rightarrow (A \wedge A)}\,\text{Imp I} \qquad\qquad \cfrac{\cfrac{\color{red}{A}}{B \Rightarrow A}\,\text{Imp I}}{\color{red}{A} \Rightarrow (B \Rightarrow A)}\,\color{red}{\text{Imp I}}$$

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

Discharging Hypothesis

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

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

Discharging Hypothesis

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

- 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

$$\frac{}{A \Rightarrow (A \vee B)}$$

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

False Elimination:

$$\frac{\mathbf{F}}{C}\ \mathbf{F}\text{ E}$$

Not Elimination:

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

And Elimination:

$$\frac{A \wedge B \qquad \begin{array}{c} A \\ \vdots \\ C \end{array}}{C}\ \text{And}_L\text{ E}
\qquad\qquad
\frac{A \wedge B \qquad \begin{array}{c} B \\ \vdots \\ C \end{array}}{C}\ \text{And}_R\text{ E}$$

Or Elimination:

$$\frac{A \vee B \qquad \begin{array}{c} A \\ \vdots \\ C \end{array} \qquad \begin{array}{c} B \\ \vdots \\ C \end{array}}{C}\ \text{Or E}$$

Implication Elimination:

$$\frac{A \Rightarrow B \quad A \qquad \begin{array}{c} B \\ \vdots \\ C \end{array}}{C}\ \text{Imp E}$$

Example Proof 4

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

Example Proof 4

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

Example Proof 4

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

Example Proof 4

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

Example Proof 4

$$
\cfrac{\cfrac{\cfrac{\cfrac{A \Rightarrow B \quad A \qquad \cfrac{}{C}}{C}\;\text{Imp E}}{A \Rightarrow C}\;\text{Imp I}}{(B \Rightarrow C) \Rightarrow (A \Rightarrow C)}\;\text{Imp I}}{(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}\;\text{Imp I}
$$

Example Proof 4

$$\dfrac{\dfrac{\dfrac{A \Rightarrow B \quad A \quad \dfrac{}{C}}{C}\,\text{Imp E}}{A \Rightarrow C}\,\text{Imp I}}{\dfrac{(B \Rightarrow C) \Rightarrow (A \Rightarrow C)}{(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}\,\text{Imp I}}\,\text{Imp I}$$

Example Proof 4

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

Example Proof 4

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

Example Proof 4

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

Example Proof 4

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

Example Proof 4

$$
\dfrac{\dfrac{\dfrac{\dfrac{A \Rightarrow B \quad A \qquad \dfrac{B \Rightarrow C \quad B \quad C}{C}\,\text{Imp E}}{C}\,\text{Imp E}}{A \Rightarrow C}\,\text{Imp I}}{(B \Rightarrow C) \Rightarrow (A \Rightarrow C)}\,\text{Imp I}}{(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))}\,\text{Imp I}
$$

Some Well-Known Derived Rules

Modus Ponens

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

Left Conjunct

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

Right Conjunct

$$\frac{A \wedge B}{B}\ \text{AndR} \qquad\qquad \frac{A \wedge B \quad A}{A}\ \text{And}_R\ \text{E}$$

Your Turn

$$\frac{}{(A \wedge B) \Rightarrow (A \vee B)}$$

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) and
  - A proposition (called conclusion of sequent)
- More generally (not here), allow set of hypotheses and set of conclusions

Nat. Ded. Introduction Sequent Rules

Γ is set of propositions (assumptions/hypotheses)

Hypothesis Introduction:

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

Truth Introduction:

$$\frac{}{\Gamma \vdash \mathbf{T}}\ \mathbf{T}\ \text{I}$$

And Introduction:

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

Or Introduction:

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \text{Or}_L\ \text{I} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \text{Or}_R\ \text{I}$$

Not Introduction:

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

Implication Introduction:

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

Nat. Ded. Elimination Sequent Rules

Γ is set of propositions (assumptions/hypotheses)

Not Elimination:

$$\frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash C}\ \text{Not E}$$

Implication Elimination:

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

And Elimination:

$$\frac{\Gamma \vdash A \wedge B \quad \Gamma \cup \{A\} \vdash C}{\Gamma \vdash C}\ \text{And}_L\ \text{E} \qquad \frac{\Gamma \vdash A \wedge B \quad \Gamma \cup \{B\} \vdash C}{\Gamma \vdash C}\ \text{And}_R\ \text{E}$$

False Elimination:

$$\frac{\Gamma \vdash \mathbf{F}}{\Gamma \vdash C}\ \mathbf{F}\ \text{E}$$

Or Elimination:

$$\frac{\Gamma \vdash A \vee B \quad \Gamma \cup \{A\} \vdash C \quad \Gamma \cup \{B\} \vdash C}{\Gamma \vdash C}\ \text{Or E}$$

Example Proof 4, Revisited