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 27, 2018

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:

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

Proof implies Truth

Theorem (Soundness)

Suppose $\{H_1, \ldots, H_n\} \vdash P$ is provable. Then, for every valuation v, if for every i we have $v \models H_i$, then $v \models P$.

Proof.

- Fix a proof of $\{H_1, \ldots, H_n\} \vdash P$

Proof implies Truth

Theorem (Soundness)

Suppose $\{H_1, \ldots, H_n\} \vdash P$ is provable. Then, for every valuation v, if for every i we have $v \models H_i$, then $v \models P$.

Proof.

- Fix a proof of $\{H_1, \ldots, H_n\} \vdash P$
- Proceed by induction on the structure of the proof tree of $\{H_1, \ldots, H_n\} \vdash P$.

Proof implies Truth

Theorem (Soundness)

Suppose $\{H_1, \ldots, H_n\} \vdash P$ is provable. Then, for every valuation v, if for every i we have $v \models H_i$, then $v \models P$.

Proof.

- Fix a proof of $\{H_1, \ldots, H_n\} \vdash P$
- Proceed by induction on the structure of the proof tree of $\{H_1, \ldots, H_n\} \vdash P$.
- Ind Hyp: We may assume that, for every subproof of the proof of $\{H_1, \ldots, H_n\} \vdash P$, if v satisfies all the hypotheses of the result of the subproof, then v satisfies the consequent of the result of the subproof.

Proof implies Truth

Theorem (Soundness)

Suppose $\{H_1, \ldots, H_n\} \vdash P$ *is provable. Then, for every valuation* v, *if for every* i *we have* $v \models H_i$, *then* $v \models P$.

Proof.

- Fix a proof of $\{H_1, \ldots, H_n\} \vdash P$
- Proceed by induction on the structure of the proof tree of $\{H_1, \ldots, H_n\} \vdash P$.
- Ind Hyp: We may assume that, for every subproof of the proof of $\{H_1, \ldots, H_n\} \vdash P$, if v satisfies all the hypotheses of the result of the subproof, then v satisfies the consequent of the result of the subproof.
- Proceed by case analysis on the last rule used in the proof.

Proof implies Truth

Theorem (Soundness)

Suppose $\{H_1, \ldots, H_n\} \vdash P$ *is provable. Then, for every valuation* v, *if for every* i *we have* $v \models H_i$, *then* $v \models P$.

Proof.

- Fix a proof of $\{H_1, \ldots, H_n\} \vdash P$
- Proceed by induction on the structure of the proof tree of $\{H_1, \ldots, H_n\} \vdash P$.
- Ind Hyp: We may assume that, for every subproof of the proof of $\{H_1, \ldots, H_n\} \vdash P$, if v satisfies all the hypotheses of the result of the subproof, then v satisfies the consequent of the result of the subproof.
- Proceed by case analysis on the last rule used in the proof.
- Case: Hyp

Proof implies Truth

Theorem (Soundness)

Suppose $\{H_1, \ldots, H_n\} \vdash P$ *is provable. Then, for every valuation* v, *if for every* i *we have* $v \models H_i$, *then* $v \models P$.

Proof.

- Fix a proof of $\{H_1, \ldots, H_n\} \vdash P$
- Proceed by induction on the structure of the proof tree of $\{H_1, \ldots, H_n\} \vdash P$.
- Ind Hyp: We may assume that, for every subproof of the proof of $\{H_1, \ldots, H_n\} \vdash P$, if v satisfies all the hypotheses of the result of the subproof, then v satisfies the consequent of the result of the subproof.
- Proceed by case analysis on the last rule used in the proof.
- Case: Hyp
  - The P is among the H_i, so by assumption $v \models P$.

Proof implies Truth

Proof.

- Case: **T** I

Proof implies Truth

Proof.

- Case: **T** I
  - Then $P = \mathbf{T}$ and $v \models \mathbf{T}$ always.

Proof implies Truth

Proof.

- Case: **T** I
  - Then $P = \mathbf{T}$ and $v \models \mathbf{T}$ always.
- Case: And I

Proof implies Truth

Proof.

- Case: **T** I
  - Then $P = \mathbf{T}$ and $v \models \mathbf{T}$ always.
- Case: And I
  - Then there exist A and B s.t. $P = A \wedge B$ and $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n\} \vdash B$ are provable by subproofs of the proof of $\{H_1, \ldots, H_n\} \vdash P$.

Proof implies Truth

Proof.

- Case: **T** I
  - Then $P = \mathbf{T}$ and $v \models \mathbf{T}$ always.
- Case: And I
  - Then there exist A and B s.t. $P = A \wedge B$ and $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n\} \vdash B$ are provable by subproofs of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A$ and $v \models B$.

Proof implies Truth

Proof.

- Case: **T** I
  - Then $P = \mathbf{T}$ and $v \models \mathbf{T}$ always.
- Case: And I
  - Then there exist A and B s.t. $P = A \wedge B$ and $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n\} \vdash B$ are provable by subproofs of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A$ and $v \models B$.
  - Thus $v \models A \wedge B$ so $v \models P$.

Proof implies Truth

Proof.

- Case: **T** I
  - Then $P = \mathbf{T}$ and $v \models \mathbf{T}$ always.
- Case: And I
  - Then there exist A and B s.t. $P = A \wedge B$ and $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n\} \vdash B$ are provable by subproofs of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A$ and $v \models B$.
  - Thus $v \models A \wedge B$ so $v \models P$.
- Case Or_L I

Proof implies Truth

Proof.

- Case: **T** I
  - Then $P = \mathbf{T}$ and $v \models \mathbf{T}$ always.
- Case: And I
  - Then there exist A and B s.t. $P = A \wedge B$ and $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n\} \vdash B$ are provable by subproofs of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A$ and $v \models B$.
  - Thus $v \models A \wedge B$ so $v \models P$.
- Case Or_L I
  - Then there exist A and B s.t. $P = A \vee B$ and $\{H_1, \ldots, H_n\} \vdash A$ is provable by a subproof of $\{H_1, \ldots, H_n\} \vdash P$.

Proof implies Truth

Proof.

- Case: **T** I
  - Then $P = \mathbf{T}$ and $v \models \mathbf{T}$ always.
- Case: And I
  - Then there exist A and B s.t. $P = A \wedge B$ and $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n\} \vdash B$ are provable by subproofs of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A$ and $v \models B$.
  - Thus $v \models A \wedge B$ so $v \models P$.
- Case Or_L I
  - Then there exist A and B s.t. $P = A \vee B$ and $\{H_1, \ldots, H_n\} \vdash A$ is provable by a subproof of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A$.

Proof implies Truth

Proof.

- Case: $\mathbf{T}$ I
  - Then $P = \mathbf{T}$ and $v \models \mathbf{T}$ always.
- Case: And I
  - Then there exist A and B s.t. $P = A \wedge B$ and $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n\} \vdash B$ are provable by subproofs of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A$ and $v \models B$.
  - Thus $v \models A \wedge B$ so $v \models P$.
- Case Or_L I
  - Then there exist A and B s.t. $P = A \vee B$ and $\{H_1, \ldots, H_n\} \vdash A$ is provable by a subproof of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A$.
  - Thus $v \models A \vee B$ so $v \models P$.

Proof implies Truth

Proof.

- Case: $\mathbf{T}$ I
  - Then $P = \mathbf{T}$ and $v \models \mathbf{T}$ always.
- Case: And I
  - Then there exist A and B s.t. $P = A \wedge B$ and $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n\} \vdash B$ are provable by subproofs of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A$ and $v \models B$.
  - Thus $v \models A \wedge B$ so $v \models P$.
- Case Or_L I
  - Then there exist A and B s.t. $P = A \vee B$ and $\{H_1, \ldots, H_n\} \vdash A$ is provable by a subproof of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A$.
  - Thus $v \models A \vee B$ so $v \models P$.
- Case Or_R I same.

Proof implies Truth

Proof.

- Case: Not I

Proof implies Truth

Proof.

- Case: Not I
  - Then there exists A s.t. $P = \neg A$ and $\{H_1, \ldots, H_n, A\} \vdash \mathbf{F}$ is provable by a subproof of the proof of $\{H_1, \ldots, H_n\} \vdash P$.

Proof implies Truth

Proof.

- Case: Not I
  - Then there exists A s.t. $P = \neg A$ and $\{H_1, \ldots, H_n, A\} \vdash \mathbf{F}$ is provable by a subproof of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - Have $v \models H_i$ for $i = 1 \ldots n$, but not $v \models \mathbf{F}$.

Proof implies Truth

Proof.

- Case: Not I
  - Then there exists A s.t. $P = \neg A$ and $\{H_1, \ldots, H_n, A\} \vdash \mathbf{F}$ is provable by a subproof of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - Have $v \models H_i$ for $i = 1 \ldots n$, but not $v \models \mathbf{F}$.
  - By Ind. Hyp. must have $v \not\models A$

Proof implies Truth

Proof.

- Case: Not I
  - Then there exists A s.t. $P = \neg A$ and $\{H_1, \ldots, H_n, A\} \vdash \mathbf{F}$ is provable by a subproof of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - Have $v \models H_i$ for $i = 1 \ldots n$, but not $v \models \mathbf{F}$.
  - By Ind. Hyp. must have $v \not\models A$
  - Thus $v \models \neg A$.

Proof implies Truth

Proof.

- Case: Not I
  - Then there exists A s.t. $P = \neg A$ and $\{H_1, \ldots, H_n, A\} \vdash \mathbf{F}$ is provable by a subproof of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - Have $v \models H_i$ for $i = 1 \ldots n$, but not $v \models \mathbf{F}$.
  - By Ind. Hyp. must have $v \not\models A$
  - Thus $v \models \neg A$.
- Case: Imp I

Proof implies Truth

Proof.

- Case: Not I
  - Then there exists A s.t. $P = \neg A$ and $\{H_1, \ldots, H_n, A\} \vdash \mathbf{F}$ is provable by a subproof of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - Have $v \models H_i$ for $i = 1 \ldots n$, but not $v \models \mathbf{F}$.
  - By Ind. Hyp. must have $v \not\models A$
  - Thus $v \models \neg A$.
- Case: Imp I
  - Then there exist A and B s.t. $P = A \Rightarrow B$ and $\{H_1, \ldots, H_n, A\} \vdash B$ is provable by a subproof of the proof of $\{H_1, \ldots, H_n\} \vdash P$.

Proof implies Truth

Proof.

- Case: Not I
  - Then there exists A s.t. $P = \neg A$ and $\{H_1, \ldots, H_n, A\} \vdash \mathbf{F}$ is provable by a subproof of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - Have $v \models H_i$ for $i = 1 \ldots n$, but not $v \models \mathbf{F}$.
  - By Ind. Hyp. must have $v \not\models A$
  - Thus $v \models \neg A$.
- Case: Imp I
  - Then there exist A and B s.t. $P = A \Rightarrow B$ and $\{H_1, \ldots, H_n, A\} \vdash B$ is provable by a subproof of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, if $v \models A$ then $v \models B$, so either have have $v \models B$ or $v \not\models A$.

Proof implies Truth

Proof.

- Case: Not I
  - Then there exists A s.t. $P = \neg A$ and $\{H_1, \ldots, H_n, A\} \vdash \mathbf{F}$ is provable by a subproof of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - Have $v \models H_i$ for $i = 1 \ldots n$, but not $v \models \mathbf{F}$.
  - By Ind. Hyp. must have $v \not\models A$
  - Thus $v \models \neg A$.
- Case: Imp I
  - Then there exist A and B s.t. $P = A \Rightarrow B$ and $\{H_1, \ldots, H_n, A\} \vdash B$ is provable by a subproof of the proof of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, if $v \models A$ then $v \models B$, so either have have $v \models B$ or $v \not\models A$.
  - Thus $v \models A \Rightarrow B$ so $v \models P$.

Proof implies Truth

Proof.

- Case Not E

Proof implies Truth

Proof.

- Case Not E
  - Then there exist A s.t. $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n\} \vdash A$ are provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.

Proof implies Truth

Proof.

- Case Not E
  - Then there exist A s.t. $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n\} \vdash A$ are provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A$ and $v \models \neg A$, which is imposible.

Proof implies Truth

Proof.

- Case Not E
  - Then there exist A s.t. $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n\} \vdash A$ are provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A$ and $v \models \neg A$, which is imposible.
  - Thus either the last rule is not Not E or for some i we have $v \not\models H_i$, contradicting theorem assumption.

Proof implies Truth

Proof.

- Case Not E
  - Then there exist A s.t. $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n\} \vdash A$ are provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A$ and $v \models \neg A$, which is imposible.
  - Thus either the last rule is not Not E or for some i we have $v \not\models H_i$, contradicting theorem assumption.
- Case: Imp E

Proof implies Truth

Proof.

- Case Not E
  - Then there exist A s.t. $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n\} \vdash A$ are provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A$ and $v \models \neg A$, which is imposible.
  - Thus either the last rule is not Not E or for some i we have $v \not\models H_i$, contradicting theorem assumption.
- Case: Imp E
  - Then there exist A and B s.t. $\{H_1, \ldots, H_n\} \vdash A \Rightarrow B$ and $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n, B\} \vdash P$ are provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.

Proof implies Truth

Proof.

- Case Not E
  - Then there exist A s.t. $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n\} \vdash A$ are provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A$ and $v \models \neg A$, which is imposible.
  - Thus either the last rule is not Not E or for some i we have $v \not\models H_i$, contradicting theorem assumption.
- Case: Imp E
  - Then there exist A and B s.t. $\{H_1, \ldots, H_n\} \vdash A \Rightarrow B$ and $\{H_1, \ldots, H_n\} \vdash A$ and $\{H_1, \ldots, H_n, B\} \vdash P$ are provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A \Rightarrow B$ and $v \models A$.

Proof implies Truth

Proof.

- Case Not E
  - Then there exist A s.t. $\{H_1,\ldots,H_n\} \vdash A$ and $\{H_1,\ldots,H_n\} \vdash A$ are provable by subproofs of $\{H_1,\ldots,H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1\ldots n$, have $v \models A$ and $v \models \neg A$, which is imposible.
  - Thus either the last rule is not Not E or for some i we have $v \not\models H_i$, contradicting theorem assumption.
- Case: Imp E
  - Then there exist A and B s.t. $\{H_1,\ldots,H_n\} \vdash A \Rightarrow B$ and $\{H_1,\ldots,H_n\} \vdash A$ and $\{H_1,\ldots,H_n,B\} \vdash P$ are provable by subproofs of $\{H_1,\ldots,H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1\ldots n$, have $v \models A \Rightarrow B$ and $v \models A$.
  - Therefore $v \models B$.

Proof implies Truth

Proof.

- Case Not E
  - Then there exist A s.t. $\{H_1,\ldots,H_n\} \vdash A$ and $\{H_1,\ldots,H_n\} \vdash A$ are provable by subproofs of $\{H_1,\ldots,H_n\} \vdash P$.
  - By inductive hypothesis, since $v \models H_i$ for $i = 1\ldots n$, have $v \models A$ and $v \models \neg A$, which is imposible.
  - Thus either the last rule is not Not E or for some i we have $v \not\models H_i$, contradicting theorem assumption.
- Case: Imp E
  - Then there exist A and B s.t. $\{H_1,\ldots,H_n\} \vdash A \Rightarrow B$ and $\{H_1,\ldots,H_n\} \vdash A$ and $\{H_1,\ldots,H_n,B\} \vdash P$ are provable by subproofs of $\{H_1,\ldots,H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1\ldots n$, have $v \models A \Rightarrow B$ and $v \models A$.
  - Therefore $v \models B$.
  - Again by Ind. Hyp, $v \models P$.

Proof implies Truth

Proof.

- Case: And$_L$ E

□

Proof implies Truth

Proof.

- Case: And$_L$ E
  - Then there exist A and B s.t. $\{H_1,\ldots,H_n\} \vdash A \wedge B$ and $\{H_1,\ldots,H_n,A\} \vdash P$ are provable by subproofs of $\{H_1,\ldots,H_n\} \vdash P$.

□

Proof implies Truth

Proof.

- Case: And$_L$ E
  - Then there exist A and B s.t. $\{H_1,\ldots,H_n\} \vdash A \wedge B$ and $\{H_1,\ldots,H_n,A\} \vdash P$ are provable by subproofs of $\{H_1,\ldots,H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1\ldots n$, have $v \models A \wedge B$ and $v \models A$ (and $v \models B$).

□

Proof implies Truth

Proof.

- Case: And$_L$ E
  - Then there exist A and B s.t. $\{H_1,\ldots,H_n\} \vdash A \wedge B$ and $\{H_1,\ldots,H_n,A\} \vdash P$ are provable by subproofs of $\{H_1,\ldots,H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1\ldots n$, have $v \models A \wedge B$ and $v \models A$ (and $v \models B$).
  - Again by Ind. Hyp, $v \models P$.

□

Proof implies Truth

Proof.

- Case: And$_L$ E
  - Then there exist A and B s.t. $\{H_1, \ldots, H_n\} \vdash A \wedge B$ and $\{H_1, \ldots, H_n, A\} \vdash P$ are provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A \wedge B$ and $v \models A$ (and $v \models B$).
  - Again by Ind. Hyp, $v \models P$.
- Case: And$_R$ E same.

Proof implies Truth

Proof.

- Case: And$_L$ E
  - Then there exist A and B s.t. $\{H_1, \ldots, H_n\} \vdash A \wedge B$ and $\{H_1, \ldots, H_n, A\} \vdash P$ are provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A \wedge B$ and $v \models A$ (and $v \models B$).
  - Again by Ind. Hyp, $v \models P$.
- Case: And$_R$ E same.
- Case: **F** E

Proof implies Truth

Proof.

- Case: And$_L$ E
  - Then there exist A and B s.t. $\{H_1, \ldots, H_n\} \vdash A \wedge B$ and $\{H_1, \ldots, H_n, A\} \vdash P$ are provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A \wedge B$ and $v \models A$ (and $v \models B$).
  - Again by Ind. Hyp, $v \models P$.
- Case: And$_R$ E same.
- Case: **F** E
  - Then $\{H_1, \ldots, H_n\} \vdash \mathbf{F}$ is provable by a subproof of $\{H_1, \ldots, H_n\} \vdash P$.

Proof implies Truth

Proof.

- Case: And$_L$ E
  - Then there exist A and B s.t. $\{H_1, \ldots, H_n\} \vdash A \wedge B$ and $\{H_1, \ldots, H_n, A\} \vdash P$ are provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A \wedge B$ and $v \models A$ (and $v \models B$).
  - Again by Ind. Hyp, $v \models P$.
- Case: And$_R$ E same.
- Case: **F** E
  - Then $\{H_1, \ldots, H_n\} \vdash \mathbf{F}$ is provable by a subproof of $\{H_1, \ldots, H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1 \ldots n$, have $v \models \mathbf{F}$, which is impossible.

Proof implies Truth

Proof.

- Case: And$_L$ E
  - Then there exist A and B s.t. $\{H_1, \ldots, H_n\} \vdash A \wedge B$ and $\{H_1, \ldots, H_n, A\} \vdash P$ are provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A \wedge B$ and $v \models A$ (and $v \models B$).
  - Again by Ind. Hyp, $v \models P$.
- Case: And$_R$ E same.
- Case: **F** E
  - Then $\{H_1, \ldots, H_n\} \vdash \mathbf{F}$ is provable by a subproof of $\{H_1, \ldots, H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1 \ldots n$, have $v \models \mathbf{F}$, which is impossible.
  - Therefore, either last rule in proof not **F** E, or $v \neg \models H_i$, which violates theorem assumption.

Proof implies Truth

Proof.

- Case: Or E
  - Then there exist A and B s.t. $\{H_1, \ldots, H_n\} \vdash A \vee B$ and $\{H_1, \ldots, H_n, A\} \vdash P$ and $\{H_1, \ldots, H_n, B\} \vdash P$ are all provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.

Proof implies Truth

Proof.

- Case: Or E
  - Then there exist A and B s.t. $\{H_1, \ldots, H_n\} \vdash A \vee B$ and $\{H_1, \ldots, H_n, A\} \vdash P$ and $\{H_1, \ldots, H_n, B\} \vdash P$ are all provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A \vee B$.

□

Proof implies Truth

Proof.

- Case: Or E
  - Then there exist A and B s.t. $\{H_1, \ldots, H_n\} \vdash A \vee B$ and $\{H_1, \ldots, H_n, A\} \vdash P$ and $\{H_1, \ldots, H_n, B\} \vdash P$ are all provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A \vee B$.
  - Have at least one of $v \models A$ or $v \models B$.

□

Proof implies Truth

Proof.

- Case: Or E
  - Then there exist A and B s.t. $\{H_1, \ldots, H_n\} \vdash A \vee B$ and $\{H_1, \ldots, H_n, A\} \vdash P$ and $\{H_1, \ldots, H_n, B\} \vdash P$ are all provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A \vee B$.
  - Have at least one of $v \models A$ or $v \models B$.
  - Case: $v \models A$

□

Proof implies Truth

Proof.

- Case: Or E
  - Then there exist A and B s.t. $\{H_1, \ldots, H_n\} \vdash A \vee B$ and $\{H_1, \ldots, H_n, A\} \vdash P$ and $\{H_1, \ldots, H_n, B\} \vdash P$ are all provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A \vee B$.
  - Have at least one of $v \models A$ or $v \models B$.
  - Case: $v \models A$
    - Ind. Hyp. implies $v \models P$.

□

Proof implies Truth

Proof.

- Case: Or E
  - Then there exist A and B s.t. $\{H_1, \ldots, H_n\} \vdash A \vee B$ and $\{H_1, \ldots, H_n, A\} \vdash P$ and $\{H_1, \ldots, H_n, B\} \vdash P$ are all provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A \vee B$.
  - Have at least one of $v \models A$ or $v \models B$.
  - Case: $v \models A$
    - Ind. Hyp. implies $v \models P$.
  - Case: $v \models B$

□

Proof implies Truth

Proof.

- Case: Or E
  - Then there exist A and B s.t. $\{H_1, \ldots, H_n\} \vdash A \vee B$ and $\{H_1, \ldots, H_n, A\} \vdash P$ and $\{H_1, \ldots, H_n, B\} \vdash P$ are all provable by subproofs of $\{H_1, \ldots, H_n\} \vdash P$.
  - By Ind. Hyp., since $v \models H_i$ for $i = 1 \ldots n$, have $v \models A \vee B$.
  - Have at least one of $v \models A$ or $v \models B$.
  - Case: $v \models A$
    - Ind. Hyp. implies $v \models P$.
  - Case: $v \models B$
    - Again by Ind. Hyp, $v \models P$.

□

Truth does not imply Proof . . .

- For given rules, can not prove $A \vee \neg A$
- Need an axiom.

Model Checking for Propositions

- Problem: Would like an efficient way to answer for a given proposition P:
  - Is P a tautology?
  - Is P satisfiable?
    - Note: A general algorithm to answer the first can be used to answer the second and vice versa.
  - Does a given valuation satisfy P?
- Difficulty: Answering if P is satisfiable is NP-complete
- Algorithms exist with good performance in general practice
- BDDs are one such

Binary Decision Trees

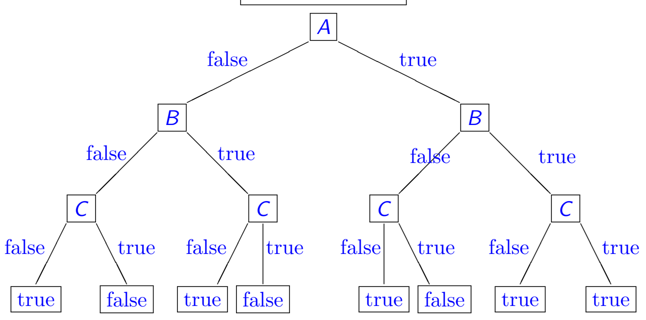
- Binary decision tree is a (rooted, directected) edge and vertex labeled tree with two types of verices – internal nodes, and leaves – such that:
  - Internal nodes have exactly two out edges
  - Leaves have no out edges
  - Internal nodes are labeled by atomic propositions (variables)
  - Leaves are labeled by true or false.
  - Left edges labeled false and right edges labeled true.
  - For each path (branch) in the tree, each atomic proposition may label at most one vertex of that path.

Binary Decision Trees

- Binary decision trees can record the set of all models (and non-models) of a proposition
  - Path records a valuation: out edge label gives value for variable labeling an internal
  - Any variable not on path can have any value
  - Leaf label says whether a valuation assigning those values to those variables
    - Is a model (true, the tree accepts the valuation)
    - Or not a model (false, the tree)
  - Each valuation matches exactly one branch
  - More than one valuation may (will) match a given branch

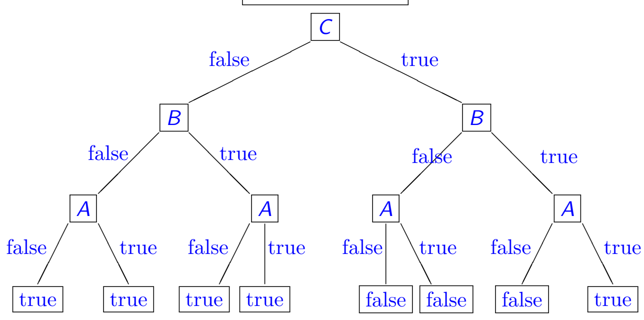
Example:

$\boxed{(A \wedge B) \vee (\neg C)}$



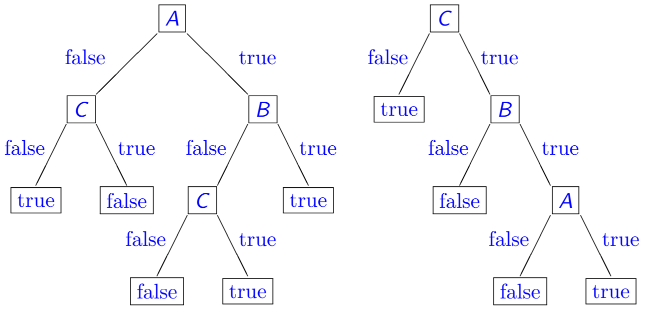
Example: Different Variable Ordering - Different Tree

$\boxed{(A \wedge B) \vee (\neg C)}$



Example: Many Logically Equivalent Trees

$\boxed{(A \wedge B) \vee (\neg C)}$



Alternate Syntax for Propositional Logic

- Still have constants $\{\mathbf{T}, \mathbf{F}\}$
- Still have countable set AP of propositional variables a.k.a. atomic propositions
- Only one ternary connective: the conditional if_then_else_
  - First argument only a variable
  - Second and third arguments propositions

Translating Original Propositions into if_then_else

- Start with proposition P_0 with variables $v_1, \ldots v_n$
- $P[c/v]$ is the proposition resulting from replacing all occurrences of variable v with constant c
- Let $\overline{P}$ be the result of evaluating every subexpression of P containing no variables
- Let $P_1 = \mathit{if}\ \ v_1\ \ \mathit{then}\ \overline{P_0[\mathbf{T}/v_1]}\ \mathit{else}\ \overline{P_0[\mathbf{F}/v_1]}$
- Let $P_i = \mathit{if}\ \ v_i\ \ \mathit{then}\ P_{i-1}[\mathbf{T}/v_i]\ \mathit{else} P_{i-1}[\mathbf{F}/v_i]$
- P_n is logically equivalent to P, but only uses if_then_else_.
  - Valuation satisfies P if and only if it satisfies P_n
  - P_n depends on the order of variables $v_1, \ldots v_n$
  - P_n directly corresponds to a binary decision tree

Example:

$P = (A \wedge B) \vee (\neg C)$, variables $\{A,\ B,\ C\}$

$P_0 = (A \wedge B) \vee (\neg C)$

Example:

$P = (A \wedge B) \vee (\neg C)$, variables $\{A,\ B,\ C\}$

$P_0 = (A \wedge B) \vee (\neg C)$
$P_1 = \mathit{if}\ \ A\ \ \mathit{then}\ (\mathbf{T}\ \wedge\ B) \vee (\neg C)\ \mathit{else}\ (\mathbf{F}\ \wedge\ B) \vee (\neg C)$

Example:

$P = (A \wedge B) \vee (\neg C)$, variables $\{A,\ B,\ C\}$

$P_0 = (A \wedge B) \vee (\neg C)$
$P_1 = \mathit{if}\ \ A\ \ \mathit{then}\ (\mathbf{T}\ \wedge\ B) \vee (\neg C)\ \mathit{else}\ (\mathbf{F}\ \wedge\ B) \vee (\neg C)$
$P_2' = \mathit{if}\ \ B\ \ \mathit{then}\ (\mathit{if}\ \ A\ \ \mathit{then}\ (\mathbf{T}\ \wedge\ \mathbf{T}) \vee (\neg C)\ \mathit{else}\ (\mathbf{F}\ \wedge\ \mathbf{T}) \vee (\neg C))$
$\qquad \mathit{else}\ (\mathit{if}\ \ A\ \ \mathit{then}\ (\mathbf{T}\ \wedge\ \mathbf{F}) \vee (\neg C)\ \mathit{else}\ (\mathbf{F}\ \wedge\ \mathbf{F}) \vee (\neg C))$

Example:

$P = (A \wedge B) \vee (\neg C)$, variables $\{A,\ B,\ C\}$

$$
\begin{aligned}
P_0 &= (A \wedge B) \vee (\neg C)\\
P_1 &= \textit{if } A \textit{ then } (\mathbf{T} \wedge B) \vee (\neg C) \textit{ else } (\mathbf{F} \wedge B) \vee (\neg C)\\
P_2' &= \textit{if } B \textit{ then } (\textit{if } A \textit{ then } (\mathbf{T} \wedge \mathbf{T}) \vee (\neg C) \textit{ else } (\mathbf{F} \wedge \mathbf{T}) \vee (\neg C))\\
&\qquad \textit{else } (\textit{if } A \textit{ then } (\mathbf{T} \wedge \mathbf{F}) \vee (\neg C) \textit{ else } (\mathbf{F} \wedge \mathbf{F}) \vee (\neg C))\\
P_2 &= \textit{if } B \textit{ then } (\textit{if } A \textit{ then } \mathbf{T} \vee (\neg C) \textit{ else } \mathbf{F} \vee (\neg C))\\
&\qquad \textit{else } (\textit{if } A \textit{ then } \mathbf{F} \vee (\neg C) \textit{ else } \mathbf{F} \vee (\neg C))
\end{aligned}
$$

Example:

$P = (A \wedge B) \vee (\neg C)$, variables $\{A,\ B,\ C\}$

$$
\begin{aligned}
P_0 &= (A \wedge B) \vee (\neg C)\\
P_1 &= \textit{if } A \textit{ then } (\mathbf{T} \wedge B) \vee (\neg C) \textit{ else } (\mathbf{F} \wedge B) \vee (\neg C)\\
P_2' &= \textit{if } B \textit{ then } (\textit{if } A \textit{ then } (\mathbf{T} \wedge \mathbf{T}) \vee (\neg C) \textit{ else } (\mathbf{F} \wedge \mathbf{T}) \vee (\neg C))\\
&\qquad \textit{else } (\textit{if } A \textit{ then } (\mathbf{T} \wedge \mathbf{F}) \vee (\neg C) \textit{ else } (\mathbf{F} \wedge \mathbf{F}) \vee (\neg C))\\
P_2 &= \textit{if } B \textit{ then } (\textit{if } A \textit{ then } \mathbf{T} \vee (\neg C) \textit{ else } \mathbf{F} \vee (\neg C))\\
&\qquad \textit{else } (\textit{if } A \textit{ then } \mathbf{F} \vee (\neg C) \textit{ else } \mathbf{F} \vee (\neg C))\\
P_3' &= \textit{if } C \textit{ then } (\textit{if } B \textit{ then } (\textit{if } A \textit{ then } \mathbf{T} \vee (\neg \mathbf{T}) \textit{ else } \mathbf{F} \vee (\neg \mathbf{T}))\\
&\qquad\qquad \textit{else } (\textit{if } A \textit{ then } \mathbf{F} \vee (\neg \mathbf{T}) \textit{ else } \mathbf{F} \vee (\neg \mathbf{T})))\\
&\qquad \textit{else } (\textit{if } B \textit{ then } (\textit{if } A \textit{ then } \mathbf{T} \vee (\neg \mathbf{F}) \textit{ else } \mathbf{F} \vee (\neg \mathbf{F}))\\
&\qquad\qquad \textit{else } (\textit{if } A \textit{ then } \mathbf{F} \vee (\neg \mathbf{F}) \textit{ else } \mathbf{F} \vee (\neg \mathbf{F})))
\end{aligned}
$$

Example:

$P = (A \wedge B) \vee (\neg C)$, variables $\{A,\ B,\ C\}$

$$
\begin{aligned}
P_0 &= (A \wedge B) \vee (\neg C)\\
P_1 &= \textit{if } A \textit{ then } (\mathbf{T} \wedge B) \vee (\neg C) \textit{ else } (\mathbf{F} \wedge B) \vee (\neg C)\\
P_2' &= \textit{if } B \textit{ then } (\textit{if } A \textit{ then } (\mathbf{T} \wedge \mathbf{T}) \vee (\neg C) \textit{ else } (\mathbf{F} \wedge \mathbf{T}) \vee (\neg C))\\
&\qquad \textit{else } (\textit{if } A \textit{ then } (\mathbf{T} \wedge \mathbf{F}) \vee (\neg C) \textit{ else } (\mathbf{F} \wedge \mathbf{F}) \vee (\neg C))\\
P_2 &= \textit{if } B \textit{ then } (\textit{if } A \textit{ then } \mathbf{T} \vee (\neg C) \textit{ else } \mathbf{F} \vee (\neg C))\\
&\qquad \textit{else } (\textit{if } A \textit{ then } \mathbf{F} \vee (\neg C) \textit{ else } \mathbf{F} \vee (\neg C))\\
P_3' &= \textit{if } C \textit{ then } (\textit{if } B \textit{ then } (\textit{if } A \textit{ then } \mathbf{T} \vee (\neg \mathbf{T}) \textit{ else } \mathbf{F} \vee (\neg \mathbf{T}))\\
&\qquad\qquad \textit{else } (\textit{if } A \textit{ then } \mathbf{F} \vee (\neg \mathbf{T}) \textit{ else } \mathbf{F} \vee (\neg \mathbf{T})))\\
&\qquad \textit{else } (\textit{if } B \textit{ then } (\textit{if } A \textit{ then } \mathbf{T} \vee (\neg \mathbf{F}) \textit{ else } \mathbf{F} \vee (\neg \mathbf{F}))\\
&\qquad\qquad \textit{else } (\textit{if } A \textit{ then } \mathbf{F} \vee (\neg \mathbf{F}) \textit{ else } \mathbf{F} \vee (\neg \mathbf{F})))\\
P_3 &= \textit{if } C \textit{ then } (\textit{if } B \textit{ then } (\textit{if } A \textit{ then } \mathbf{T} \textit{ else } \mathbf{F})\\
&\qquad\qquad \textit{else } (\textit{if } A \textit{ then } \mathbf{F} \textit{ else } \mathbf{F}))\\
&\qquad \textit{else } (\textit{if } B \textit{ then } (\textit{if } A \textit{ then } \mathbf{T} \textit{ else } \mathbf{T})\\
&\qquad\qquad \textit{else } (\textit{if } A \textit{ then } \mathbf{T} \textit{ else } \mathbf{T}))
\end{aligned}
$$

Example, cont.

$$
\begin{aligned}
P_3 &= \textit{if } C \textit{ then } (\textit{if } B \textit{ then } (\textit{if } A \textit{ then } \mathbf{T} \textit{ else } \mathbf{F})\\
&\qquad\qquad \textit{else } (\textit{if } A \textit{ then } \mathbf{F} \textit{ else } \mathbf{F}))\\
&\qquad \textit{else } (\textit{if } B \textit{ then } (\textit{if } A \textit{ then } \mathbf{T} \textit{ else } \mathbf{T})\\
&\qquad\qquad \textit{else } (\textit{if } A \textit{ then } \mathbf{T} \textit{ else } \mathbf{T}))
\end{aligned}
$$

P_3 corresponds to second binary decision tree given earlier

- Any proposition in strict if_then_else_ form corresponds directly to a binary decision tree that accepts exactly the valuations that satisfy (model) the proposition.

Binary Decision Diagram

- Binary decision trees may contain (much) redundancy
- Binary Decision Diagram (BDD): Replace trees by (rooted) directed acyclic graphs
- Require all other conditions still hold
- Generalization of binary decision trees
- Allows for sharing of common subtrees.
- Accepts / rejects valuations as with binary decision trees.

Example

Reduced Ordered Binary Decision Diagrams

- Problem: given proposition may correspond to many different BDDs
- How to create a (compact) canonical BDD for a proposition such that two different propositions are logically equivalent if and only if they have the same (isomorphic) canonical BDD
- Start: order propositional variables $v_i < v_j$.
- Bryant showed you can obtain such a canonical BDD by requiring
  - Variables should appear in order on each path for root to leaf
  - No distinct duplicate (isomorphic) subtrees (including leaves)

Achieving Canonical Form

- Start with an Ordered BDD (all edges in correct order)
- Repeat following until none apply
- Remove duplicate leaves: Eliminate all but one leaf with a given label and redirect all edges to the eliminated leaves to the remaining one
- Remove duplicate nonterminals: If node n and m have the same variable label, their left edges point to the same node and their right edges point to the same node, remove one and redirect edges that pointed to it to the other
- Remove redundant tests: If both out edges node of n point to node m, eliminate n and redirect all edges coming into n to m
- Bryant gave procedure to do the above that terminates in linear time

Example