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

February 6, 2020

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
  - Example

    if C then if B then if A then **T** *else* **F** *else* **F** *else* **T**

  - Represents the last tree above

Semantics for Conditional Propositional Logic

- Define when a valuation v satisfies a conditional proposition by

  $v \models \mathbf{T}$
  $v \not\models \mathbf{F}$
  $v \models$ *if A then* P_t *else* P_f iff
  $v(A) = \mathrm{true}$ and $v \models P_t$ or
  $v(A) = \mathrm{false}$ and $v \models P_f$

- Example: let $v = \{A \mapsto \mathrm{true},\ B \mapsto \mathrm{true}, C \mapsto \mathrm{true}\}$

  $v \models$ *if C then if B then if A then* **T** *else* **F** *else* **F** *else* **T**

Semantics for Conditional Propositional Logic

- Define when a valuation v satisfies a conditional proposition by

  $v \models \mathbf{T}$
  $v \not\models \mathbf{F}$
  $v \models$ *if A then* P_t *else* P_f iff
  $v(A) = \mathrm{true}$ and $v \models P_t$ or
  $v(A) = \mathrm{false}$ and $v \models P_f$

- Example: let $v = \{A \mapsto \mathrm{true},\ B \mapsto \mathrm{true}, C \mapsto \mathrm{true}\}$

  $v \models$ *if C then if B then if A then* **T** *else* **F** *else* **F** *else* **T** since
  $v(C) = \mathrm{true}$ and
  $v \models$ *if B then if A then* **T** *else* **F** *else* **F**

Semantics for Conditional Propositional Logic

- Define when a valuation v satisfies a conditional proposition by

  $v \models \mathbf{T}$
  $v \not\models \mathbf{F}$
  $v \models$ *if A then* P_t *else* P_f iff
  $v(A) = \mathrm{true}$ and $v \models P_t$ or
  $v(A) = \mathrm{false}$ and $v \models P_f$

- Example: let $v = \{A \mapsto \mathrm{true},\ B \mapsto \mathrm{true}, C \mapsto \mathrm{true}\}$

  $v \models$ *if C then if B then if A then* **T** *else* **F** *else* **F** *else* **T** since
  $v(C) = \mathrm{true}$ and

  $v \models$ *if B then if A then* **T** *else* **F** *else* **F** since
  $v(B) = \mathrm{true}$ and
  $v \models$ *if A then* **T** *else* **F**

Semantics for Conditional Propositional Logic

- Define when a valuation v satisfies a conditional proposition by

  $v \models \mathbf{T}$
  $v \not\models \mathbf{F}$
  $v \models$ *if A then* P_t *else* P_f iff
  $v(A) = \mathrm{true}$ and $v \models P_t$ or
  $v(A) = \mathrm{false}$ and $v \models P_f$

- Example: let $v = \{A \mapsto \mathrm{true},\ B \mapsto \mathrm{true}, C \mapsto \mathrm{true}\}$

  $v \models$ *if C then if B then if A then* **T** *else* **F** *else* **F** *else* **T** since
  $v(C) = \mathrm{true}$ and
  $v \models$ *if B then if A then* **T** *else* **F** *else* **F** since
  $v(B) = \mathrm{true}$ and

  $v \models$ *if A then* **T** *else* **F** since
  $v(A) = \mathrm{true}$ and$v \models \mathbf{T}$

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 $P_1 = \textit{if}\ v_1\ \textit{then}\ \overline{P_0[\mathbf{T}/v_1]}\ \textit{else}\ \overline{P_0[\mathbf{F}/v_1]}$
- Let $P_i = \textit{if}\ v_i\ \textit{then}\ P_{i-1}[\mathbf{T}/v_i]\ \textit{else}\ P_{i-1}[\mathbf{F}/v_i]$
- 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 $\{A, B, C\}$, $A < B < C$

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

Example:

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

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

Example:

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

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

Example:

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

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

Example:

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

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

Example:

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

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

Example, cont.

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

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 of node 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