Lecture 8 - February 2

Model Checking

Comparison: Parse Trees, LMDs, RMDs
Deriving Subformulas
Labelled Transition System (LTS)

Interpreting a Formula: LMD (1)

$$
\begin{array}{lll}
\phi & ::= & \top \quad [\textit{true}] \\
& | & \bot \quad [\textit{false}] \\
& | & p \quad [\text{propositional atom}] \\
& | & (\neg\phi) \quad [\text{logical negation}] \\
& | & (\phi \wedge \phi) \quad [\text{logical conjunction}] \\
& | & (\phi \vee \phi) \quad [\text{logical disjunction}] \\
& | & (\phi \Rightarrow \phi) \quad [\text{logical implication}] \\
& | & (\mathbf{X}\phi) \quad [\text{neXt state}] \\
& | & (\mathbf{F}\phi) \quad [\text{some Future state}] \\
& | & (\mathbf{G}\phi) \quad [\text{all future states (Globally)}] \\
& | & (\phi \mathbf{U} \phi) \quad [\text{Until}] \\
& | & (\phi \mathbf{W} \phi) \quad [\text{Weak-until}] \\
& | & (\phi \mathbf{R} \phi) \quad [\text{Release}]
\end{array}
$$

each step of derivation is based on a rule in the grammar

$\mathbf{F}\,p \wedge \mathbf{G}\,q \Rightarrow p\,\mathbf{U}\,r$

$\phi \Rightarrow \phi$ is derived to $\phi \Rightarrow \phi$ by implication

ϕ → left-most non-terminal

left-most non-terminal

$\Rightarrow \phi \wedge \phi \Rightarrow \phi$

$\Rightarrow \mathbf{F}\phi \wedge \phi \Rightarrow \phi$

$\Rightarrow \mathbf{F}\,p \wedge \phi \Rightarrow \phi$

$\Rightarrow \mathbf{F}\,p \wedge \mathbf{G}\phi \Rightarrow \phi$

$\Rightarrow \mathbf{F}\,p \wedge \mathbf{G}\,q \Rightarrow \phi$

$\Rightarrow \mathbf{F}\,p \wedge \mathbf{G}\,q \Rightarrow \phi\,\mathbf{U}\,\phi$

$\Rightarrow \mathbf{F}\,p \wedge \mathbf{G}\,q \Rightarrow p\,\mathbf{U}\,\phi$

$\Rightarrow \mathbf{F}\,p \wedge \mathbf{G}\,q \Rightarrow p\,\mathbf{U}\,r$

when there's no non-terminal ⇒ done!

Interpreting a Formula: LMD (2)

$$
\begin{array}{lll}
\phi & ::= & \top \quad [\textit{true}] \\
 & | & \bot \quad [\textit{false}] \\
 & | & p \quad [\texttt{propositional atom}] \\
 & | & (\neg\phi) \quad [\texttt{logical negation}] \\
 & | & (\phi \wedge \phi) \quad [\texttt{logical conjunction}] \\
 & | & (\phi \vee \phi) \quad [\texttt{logical disjunction}] \\
 & | & (\phi \Rightarrow \phi) \quad [\texttt{logical implication}] \\
 & | & (\mathbf{X}\phi) \quad [\texttt{ne}\mathbf{X}\texttt{t state}] \\
 & | & (\mathbf{F}\phi) \quad [\texttt{some }\mathbf{F}\texttt{uture state}] \\
 & | & (\mathbf{G}\phi) \quad [\texttt{all future states (}\mathbf{G}\texttt{lobally)}] \\
 & | & (\phi\,\mathbf{U}\,\phi) \quad [\mathbf{U}\texttt{ntil}] \\
 & | & (\phi\,\mathbf{W}\,\phi) \quad [\mathbf{W}\texttt{eak-until}] \\
 & | & (\phi\,\mathbf{R}\,\phi) \quad [\mathbf{R}\texttt{elease}]
\end{array}
$$

$$\mathbf{F}\,(p \wedge \mathbf{G}\,q \Rightarrow p\,\mathbf{U}\,r)$$

Interpreting a Formula: LMD (3)

$$
\begin{array}{lcll}
\phi & ::= & \top & [\,\textit{true}\,] \\
 & | & \bot & [\,\textit{false}\,] \\
 & | & p & [\,\texttt{propositional atom}\,] \\
 & | & (\neg\phi) & [\,\texttt{logical negation}\,] \\
 & | & (\phi \wedge \phi) & [\,\texttt{logical conjunction}\,] \\
 & | & (\phi \vee \phi) & [\,\texttt{logical disjunction}\,] \\
 & | & (\phi \Rightarrow \phi) & [\,\texttt{logical implication}\,] \\
 & | & (\mathbf{X}\,\phi) & [\,\texttt{ne}\mathbf{X}\texttt{t state}\,] \\
 & | & (\mathbf{F}\,\phi) & [\,\texttt{some }\mathbf{F}\texttt{uture state}\,] \\
 & | & (\mathbf{G}\,\phi) & [\,\texttt{all future states (}\mathbf{G}\texttt{lobally)}\,] \\
 & | & (\phi\,\mathbf{U}\,\phi) & [\,\mathbf{U}\texttt{ntil}\,] \\
 & | & (\phi\,\mathbf{W}\,\phi) & [\,\mathbf{W}\texttt{eak-until}\,] \\
 & | & (\phi\,\mathbf{R}\,\phi) & [\,\mathbf{R}\texttt{elease}\,]
\end{array}
$$

$$\mathbf{F}\ p \wedge (\mathbf{G}\ q \Rightarrow p\ \mathbf{U}\ r)$$

Interpreting a Formula: LMD (4)

$$
\begin{array}{lll}
\phi & ::= & \top \quad [\textit{true}] \\
 & | & \bot \quad [\textit{false}] \\
 & | & p \quad [\texttt{propositional atom}] \\
 & | & (\neg\phi) \quad [\texttt{logical negation}] \\
 & | & (\phi \wedge \phi) \quad [\texttt{logical conjunction}] \\
 & | & (\phi \vee \phi) \quad [\texttt{logical disjunction}] \\
 & | & (\phi \Rightarrow \phi) \quad [\texttt{logical implication}] \\
 & | & (\mathbf{X}\phi) \quad [\texttt{neXt state}] \\
 & | & (\mathbf{F}\phi) \quad [\texttt{some Future state}] \\
 & | & (\mathbf{G}\phi) \quad [\texttt{all future states (Globally)}] \\
 & | & (\phi\,\mathbf{U}\,\phi) \quad [\texttt{Until}] \\
 & | & (\phi\,\mathbf{W}\,\phi) \quad [\texttt{Weak-until}] \\
 & | & (\phi\,\mathbf{R}\,\phi) \quad [\texttt{Release}]
\end{array}
$$

$$\mathbf{F}\ p \wedge ((\mathbf{G}\ q \Rightarrow p)\ \mathbf{U}\ r)$$

Interpreting a Formula: RMD (1)

ϕ	::=	$\top$	[*true*]
	|	$\bot$	[*false*]
	|	p	[propositional atom]
	|	$(\neg\phi)$	[logical negation]
	|	$(\phi \wedge \phi)$	[logical conjunction]
	|	$(\phi \vee \phi)$	[logical disjunction]
	|	$(\phi \Rightarrow \phi)$	[logical implication]
	|	$(\mathbf{X}\phi)$	[ne**X**t state]
	|	$(\mathbf{F}\phi)$	[some **F**uture state]
	|	$(\mathbf{G}\phi)$	[all future states (**G**lobally)]
	|	$(\phi\,\mathbf{U}\,\phi)$	[**U**ntil]
	|	$(\phi\,\mathbf{W}\,\phi)$	[**W**eak-until]
	|	$(\phi\,\mathbf{R}\,\phi)$	[**R**elease]

$$\mathbf{F}\,p \wedge \mathbf{G}\,q \Rightarrow p\,\mathbf{U}\,r$$

Interpreting a Formula: RMD (2)

ϕ	::=	$\top$	[*true*]
	|	$\bot$	[*false*]
	|	p	[propositional atom]
	|	$(\neg\phi)$	[logical negation]
	|	$(\phi \wedge \phi)$	[logical conjunction]
	|	$(\phi \vee \phi)$	[logical disjunction]
	|	$(\phi \Rightarrow \phi)$	[logical implication]
	|	$(\mathbf{X}\phi)$	[ne**X**t state]
	|	$(\mathbf{F}\phi)$	[some **F**uture state]
	|	$(\mathbf{G}\phi)$	[all future states (**G**lobally)]
	|	$(\phi\,\mathbf{U}\,\phi)$	[**U**ntil]
	|	$(\phi\,\mathbf{W}\,\phi)$	[**W**eak-until]
	|	$(\phi\,\mathbf{R}\,\phi)$	[**R**elease]

$$\mathbf{F}\,(p \wedge \mathbf{G}\,q \Rightarrow p\,\mathbf{U}\,r)$$

Interpreting a Formula: RMD (3)

$$
\begin{array}{lcll}
\phi & ::= & \top & [\,\textit{true}\,] \\
 & | & \bot & [\,\textit{false}\,] \\
 & | & p & [\,\texttt{propositional atom}\,] \\
 & | & (\neg\phi) & [\,\texttt{logical negation}\,] \\
 & | & (\phi \wedge \phi) & [\,\texttt{logical conjunction}\,] \\
 & | & (\phi \vee \phi) & [\,\texttt{logical disjunction}\,] \\
 & | & (\phi \Rightarrow \phi) & [\,\texttt{logical implication}\,] \\
 & | & (\mathbf{X}\,\phi) & [\,\texttt{ne}\mathbf{X}\texttt{t state}\,] \\
 & | & (\mathbf{F}\,\phi) & [\,\texttt{some }\mathbf{F}\texttt{uture state}\,] \\
 & | & (\mathbf{G}\,\phi) & [\,\texttt{all future states (}\mathbf{G}\texttt{lobally)}\,] \\
 & | & (\phi\,\mathbf{U}\,\phi) & [\,\mathbf{U}\texttt{ntil}\,] \\
 & | & (\phi\,\mathbf{W}\,\phi) & [\,\mathbf{W}\texttt{eak-until}\,] \\
 & | & (\phi\,\mathbf{R}\,\phi) & [\,\mathbf{R}\texttt{elease}\,]
\end{array}
$$

$$\mathbf{F}\ p \wedge (\mathbf{G}\ q \Rightarrow p\ \mathbf{U}\ r)$$

Interpreting a Formula: RMD (4)

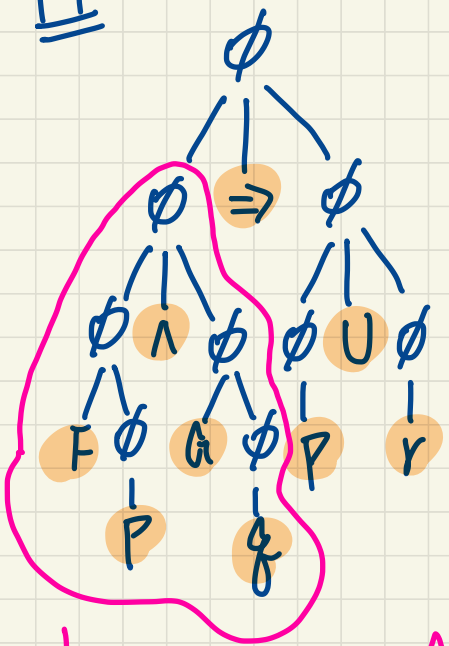
ϕ	::=	$\top$	[*true*]
	|	$\bot$	[*false*]
	|	p	[propositional atom]
	|	$(\neg\phi)$	[logical negation]
	|	$(\phi \wedge \phi)$	[logical conjunction]
	|	$(\phi \vee \phi)$	[logical disjunction]
	|	$(\phi \Rightarrow \phi)$	[logical implication]
	|	$(\mathbf{X}\phi)$	[ne**X**t state]
	|	$(\mathbf{F}\phi)$	[some **F**uture state]
	|	$(\mathbf{G}\phi)$	[all future states (**G**lobally)]
	|	$(\phi \mathbf{U} \phi)$	[**U**ntil]
	|	$(\phi \mathbf{W} \phi)$	[**W**eak-until]
	|	$(\phi \mathbf{R} \phi)$	[**R**elease]

$$\mathbf{F}\ p \wedge ((\mathbf{G}\ q \Rightarrow p)\ \mathbf{U}\ r)$$

Interpreting a Formula: PT vs. LMD vs. RMD

$F\,p \wedge G\,q \Rightarrow p\,U\,r$

PT



subtree: $F\,p \wedge G\,q$

LMD

① $\Rightarrow \phi \Rightarrow \phi$

② $\Rightarrow \phi \wedge \phi \Rightarrow \phi$

③ $\Rightarrow F\,\phi \wedge \phi \Rightarrow \phi$

④ $\Rightarrow F\,p \wedge \phi \Rightarrow \phi$

⑤ $\Rightarrow F\,p \wedge G\,\phi \Rightarrow \phi$

⑥ $\Rightarrow F\,p \wedge G\,q \Rightarrow \phi$

⑦ $\Rightarrow F\,p \wedge G\,q \Rightarrow \phi\,U\,\phi$

⑧ $\Rightarrow F\,p \wedge G\,q \Rightarrow p\,U\,\phi$

⑨ $\Rightarrow F\,p \wedge G\,q \Rightarrow p\,U\,r$

RMD

$\Rightarrow \phi \Rightarrow \phi$

$\Rightarrow \phi \Rightarrow \phi\,U\,\phi$

$\Rightarrow \phi \Rightarrow \phi\,U\,r$

$\Rightarrow \phi \Rightarrow p\,U\,r$

$\Rightarrow \phi \wedge \phi \Rightarrow p\,U\,r$

$\Rightarrow \phi \wedge G\,\phi \Rightarrow p\,U\,r$

$\Rightarrow \phi \wedge G\,q \Rightarrow p\,U\,r$

$\Rightarrow F\,\phi \wedge G\,q \Rightarrow p\,U\,r$

$\Rightarrow F\,p \wedge G\,q \Rightarrow p\,U\,r$

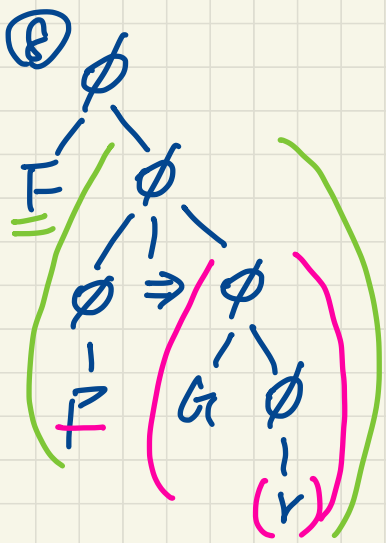
Deriving Subformulas from a Parse Tree

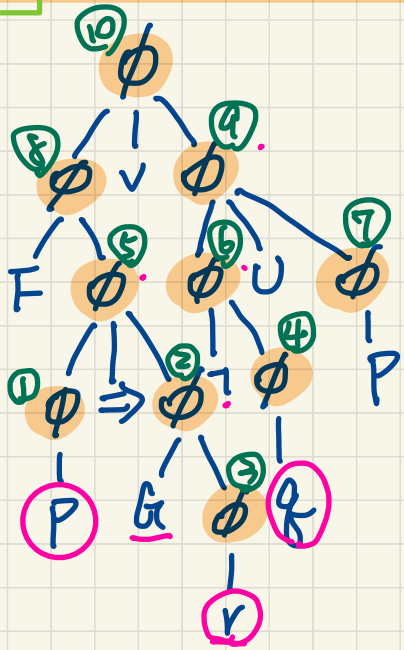
Instead, bracket strings obtained from subtrees.

Enumerate all subformulas of:

** $F\,(p \Rightarrow G\,r) \vee ((\neg q)\,U\,p)$

* and ** are not the same
∵ in ** F is applied last
in * F is applied first.





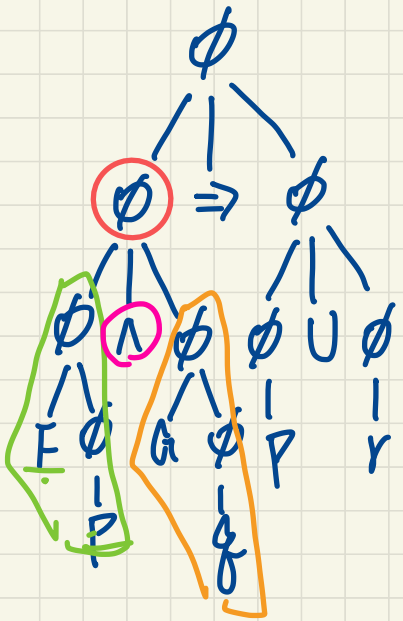
Q1: How many subformulas?
↳ Count how many ϕ's.

10

Q2. Enumerate all subformulas.

① p
② $G\,r$
③ r
④ q
⑤ $p \Rightarrow G\,r$
⑥ $\neg q$
⑦ p *
⑧ $F\,p \Rightarrow G\,r$
⑨ $(\neg q)\,U\,p$
⑩ $F(p \Rightarrow (G\,r)) \vee ((\neg q)\,U\,p)$

Given a PT:



Enumerate all subformulas:

$$(F(p)) \wedge (G(q))$$

Context-Free Grammar (CFG): Exercise

(optional)

dangling else

Is the following CFG ambiguous?

```
Statement  →  if Expr then Statement
           |  if Expr then Statement else Statement
           |  Assignment
           ...
```

Example:

if *Expr1* **then if** *Expr2* **then** *Assignment1* **else** *Assignment2*

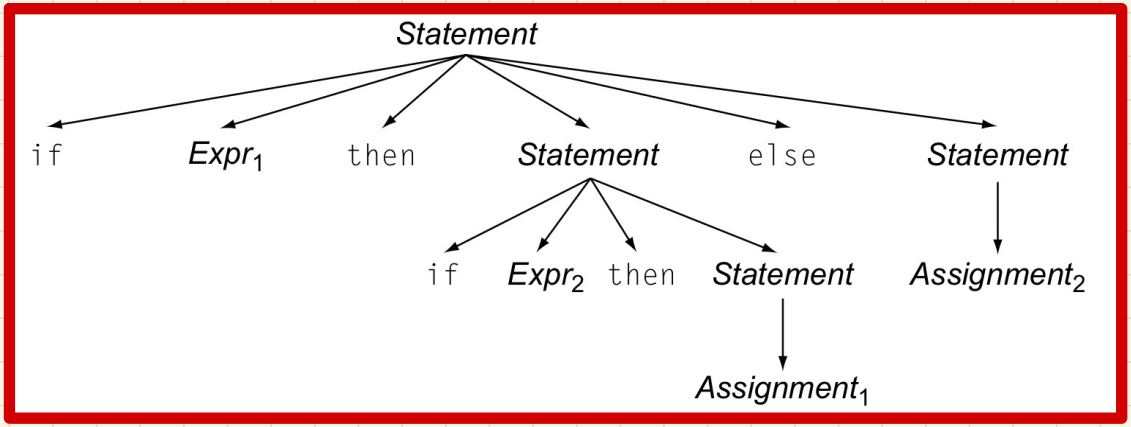
Context-Free Grammar (CFG): Exercise

Is the following CFG ambiguous?

```
Statement  →  if Expr then Statement
           |  if Expr then Statement else Statement
           |  Assignment
           ...
```

Example: A Possible **Semantic Interpretation**?

if *Expr1* **then** **if** *Expr2* **then** *Assignment1* **else** *Assignment2*



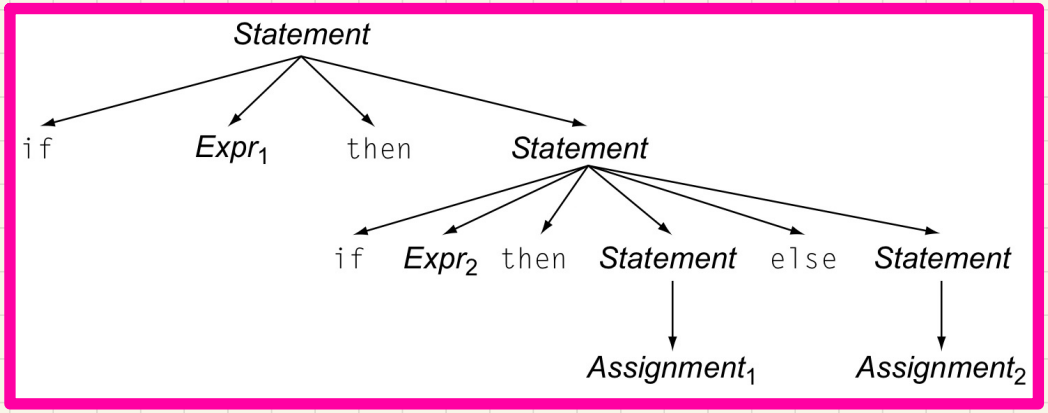
Context-Free Grammar (CFG): Exercise

Is the following CFG ambiguous?

```
Statement  →  if Expr then Statement
           |  if Expr then Statement else Statement
           |  Assignment
           ...
```

Example: A Possible **Semantic Interpretation**?

if *Expr1* **then** **if** *Expr2* **then** *Assignment1* **else** *Assignment2*



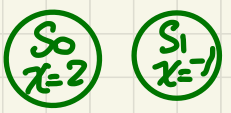
Labelled Transition System (LTS)

$$M = (S, \longrightarrow, L), \text{ given } P$$

- S: a finite set of states (↳ values of variables)
- $\longrightarrow \in S \leftrightarrow S$: transition relation ↳ set of pairs. — the set of all relations on states.
- $L \in S \to \mathbb{P}(P)$: labelling function — ↳ a set of atoms that are satisfied by the state
- P: a set of atomic propositions (which evaluate to T or F)

x
$L \in S \to P$ — given a state, return a member in P

e.g. $P = \{x > 0, x > 4\}$



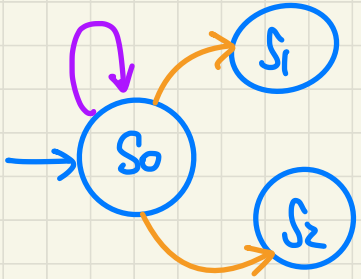
$L(S_0) = \{x > 0\}$
$L(S_1) = \{\}$
$L(S_2) = \{x > 0, x > 4\}$

Q. Formulate **deadlock freedom**:

From any state, it is always possible to make progress.

$\rightarrow \in S \leftrightarrow S$

$\rightarrow \in S \rightarrow S$



(s_0, s_0)

$\{ (s_0, s_1), (s_0, s_2) \}$

not a function,
a relation!