Lecture 7 - January 31

Model Checking

Practical Knowledge about Parsing
Operator Precedence
Drawing Parse Trees
Left-Most Derivation (LMD)

Announcement

- Lab1 Part 2 tutorial videos released
  - + Help: Scheduled Office Hours & flexible TA hours
  - + ≈ 2 hours
    - * debugging using labels, error trace, state graph
    - * PlusCal vs. Auto-Translated TLA+ Predicates
- Optional Textbook for Model Checking and Program Verification

  Logic in Computer Science:

  Modelling and reasoning about systems

  by M. Huth and M. Ryan
- Written Test 1 approaching...

  ↳ WSC ① EECS login → lab computer

  ② PPY login → eClass

Parsing: Some Practical Knowledge

context-free grammar

start variable

base cases/terminals

non-terminals

↳ goal in derivation is to "get rid of" all non-terminals

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]

the set of strings derivable from g

$F(p \Rightarrow q) \in \mathcal{L}(g)$

string of LTL formula

language

grammar of LTL

no completion in-between

$p\ F(\neg q) \notin \mathcal{L}(g)$

$p\ U\ F(\neg q) \in \mathcal{L}(g)$

Assumption: Operator precedence considered first before the CFG.

Interpreting a Formula: Parse Trees (1)

top down:
root → leaves

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]
	|	$(\mathbf{X}\,\phi)$	[neXt state]
	|	$(\mathbf{F}\,\phi)$	[some Future state]
	|	$(\mathbf{G}\,\phi)$	[all future states (Globally)]
	|	$(\phi\,\mathbf{U}\,\phi)$	[Until]
	|	$(\phi\,\mathbf{W}\,\phi)$	[Weak-until]
	|	$(\phi\,\mathbf{R}\,\phi)$	[Release]

root.

p, q, r

c > 0, $p^2 > 4$

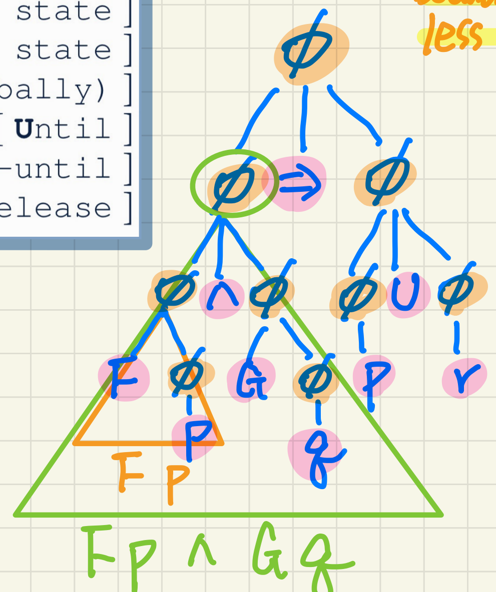
not = a keyword !

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

logical
↓
bounds less tightly

temporal op

atom



Interpreting a Formula: Parse Trees (1)

top down:
root → leaves

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]

root.

p, q, r

$c > 0,\ p^2 > 4$

not = a keyword !

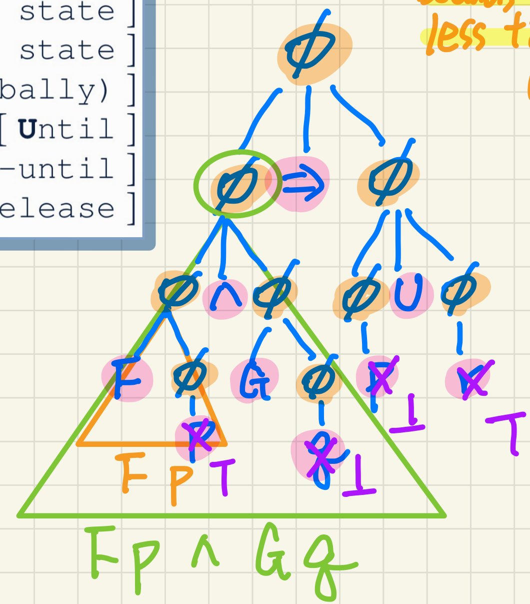
$$\boxed{\boxed{\mathbf{F}\,\cancel{p}} \wedge \boxed{\mathbf{G}\,\cancel{q}}} \Rightarrow \boxed{\boxed{\cancel{p}\,\mathbf{U}\,\cancel{r}}}$$

$\top$ $\bot$ $\bot$ $\top$

logical → bounds less tightly

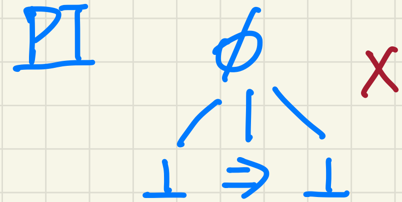
temporal op

atom



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]

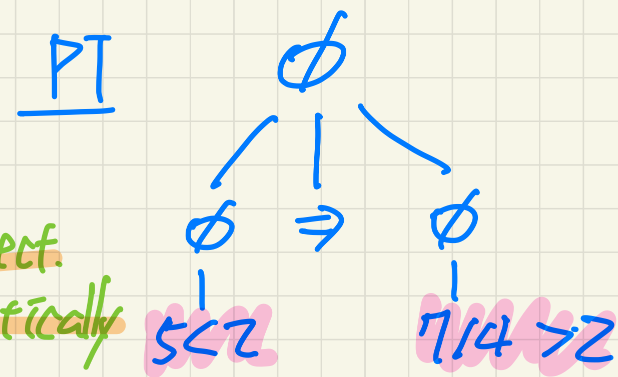
$5 < 2 \Rightarrow 7/4 > 2$



(no evaluation should be done)

- syntax
- $\boxed{\text{semantics}}$

↳ only makes sense if the formula is correct syntactically

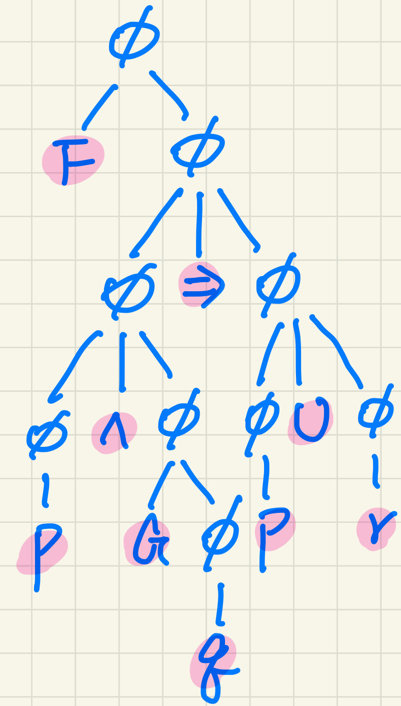


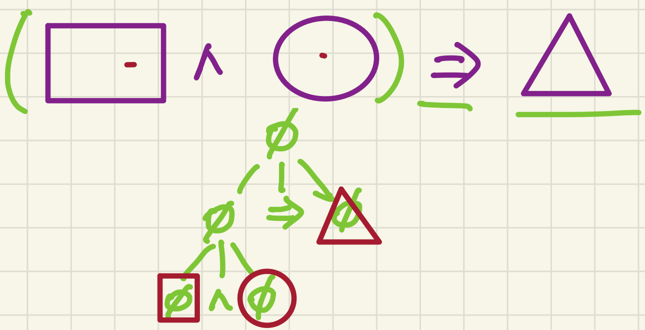
Interpreting a Formula: Parse Trees (2)

Q. $p \Rightarrow q \Rightarrow r$?

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]

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





$p \wedge q \equiv q \wedge p$ but different PTs.

Given two formula strings f1 and f2

different spellings.

(1) If $\boxed{f1 \neq f2}$, but f1 and f2 have the same parse tree, f1 and f2 are considered as semantically equivalent.

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

$(F \; p) \wedge (G \; q) \Rightarrow (p \; U \; r)$

① part of the input string to force some order of interpretation.

② parentheses are omitted in PTs.

(optional) (2) If f1 = f2, but f1 and f2 have different PTs, this means the grammar is ambiguous.

Interpreting a Formula: Parse Trees (3)

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

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

Interpreting a Formula: Parse Trees (4)

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

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

Interpreting a Formula: LMD (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]

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

is derived to

ϕ → left-most non-terminal

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

left-most non-terminal

Implication

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

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

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

(to be continued ...).