Lecture 13 - February 26

Model Checking

Subformula
Labeled Transition System (LTS)
Paths, Path Suffixes

Announcements/Reminders

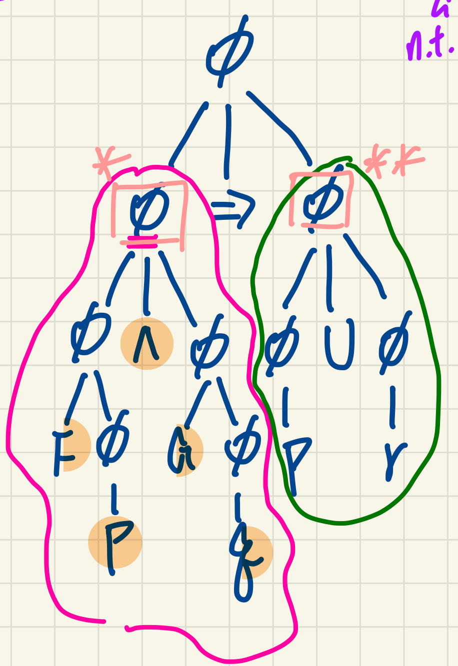
- WrittenTest1 guide & examples by the end of Friday
  - + All lectures materials up to and including today
  - + Lab1 and Lab2 (solutions & in-class discussion)
  - + Review Q&A (Zoom): 7:30pm on Monday, Mar 3
- Lab3 to be released next Wednesday
- Tomorrow's lab (9 to 10): office hour for your WT1
- This week's office hour: 3pm, Wed
- TA contact information (on-demand for labs) on eClass

$\phi \overset{①}{\Rightarrow} \phi \Rightarrow \phi \overset{②}{\Rightarrow} \phi \wedge \phi \Rightarrow \phi \overset{③}{\Rightarrow} \dots \overset{⑥}{\Rightarrow} Fp \wedge Gq \Rightarrow \phi \overset{⑦}{\Rightarrow} \dots$

Interpreting a Formula: PT vs. LMD vs. RMD

F p ∧ G q ⇒ p U r $\in L(g)$

Parse Tree



*LMD

ϕ

① $\Rightarrow \boxed{\phi} \Rightarrow \phi$

picked as leftmost n.t. by ②

②-⑥

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

ϕ

① $\Rightarrow \phi \Rightarrow \phi$

② $\Rightarrow \phi \Rightarrow \phi\ U\ \phi$

③ $\Rightarrow \phi \Rightarrow \phi\ U\ r$

④ $\Rightarrow \boxed{\phi} \Rightarrow p\ U\ r$

picked as right-most n.t. by ⑤

⑤ $\Rightarrow \phi \wedge \phi \Rightarrow p\ U\ r$

⑥ $\Rightarrow \phi \wedge G\,\phi \Rightarrow p\ U\ r$

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

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

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

⑤-⑨

Deriving Subformulas from a Parse Tree

Enumerate all subformulas of:

$\mathsf{F}\,(p \Rightarrow \mathsf{G}\ r) \vee ((\neg\ q)\ \mathsf{U}\ p)$

PT. How many subtrees in PT?

Q1. 10 subtrees

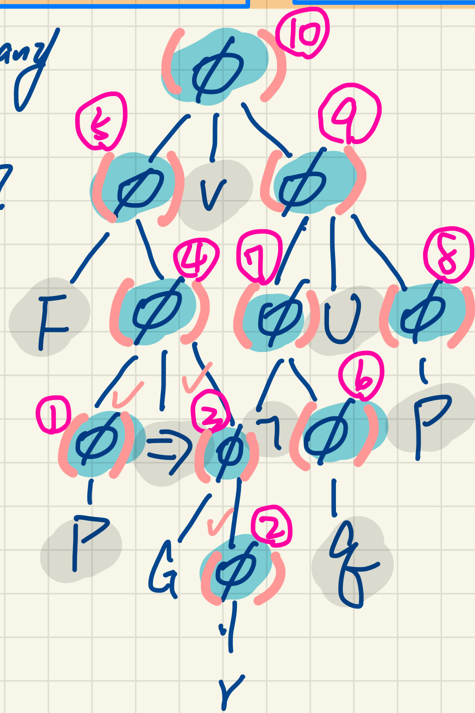
Q2. How many subformulas?

10

Q3. How many distinct subformulas?

9

(∵ ① and ⑧ are the same)



① p

② r

③ $\mathsf{G}(r)$

④ $(p) \Rightarrow (\mathsf{G}(r))$

⑤ $\mathsf{F}((p) \Rightarrow (\mathsf{G}(r)))$

⑥ q

⑦ $\neg(q)$

⑧ p

⑨ $(\neg(q))\ \mathsf{U}\ (p)$

⑩ $(⑤) \vee (⑨)$

formal model (specified as a LTS).

Labelled Transition System (LTS)

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

a set of atomic propositions (which evaluates to T or F)

a finite # of states

transition relation ↳ a set of pairs:
(cannot be a function: a state may be transitioned into more than one states)

$\longrightarrow \in S \leftrightarrow S$: set of all possible relations between S and S.

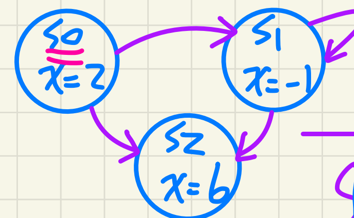
$s \curvearrowright s'$

* Labelling Function

$L \in S \rightarrow \mathbb{P}(P)$ ** — total function

** $\{\emptyset, \{x>0\}, \{x>4\}, \{x>0, x>4\}\}$

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



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

$L(s_0) = \{x>0\}$

$L(s_1) = \emptyset \quad \{\}$

$L(s_2) = \{x>0, x>4\}$

$\text{ran}(\{s_0\} \lhd \longrightarrow) = \text{ran}\{(s_0, s_1), (s_0, s_2)\} = \{s_1, s_2\}$

Q. Formulate **deadlock freedom**:

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

$\forall s \cdot s \in S \Rightarrow (\exists s' \cdot s' \in S \land$ ① $(s, s') \in \longrightarrow$ ② $s' \in \longrightarrow[\{s\}]$ ③ $s' \in \text{ran}(\{s\} \lhd \longrightarrow))$ ④ use range restriction

Labelled Transition System (LTS)

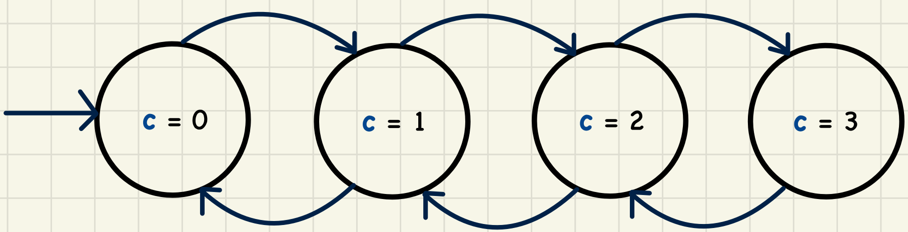
Exercises Consider the system with a counter c with the following assumption:

$$0 \leq c \leq 3$$

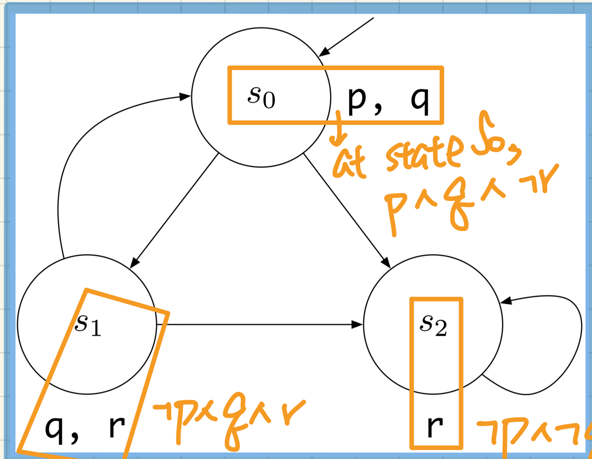
Say c is initialized 0 and may be incremented (via a transition *inc*, enabled when $c < 3$) or decremented (via a transition *dec*, enabled when $c > 0$).

- **Draw** a ***state graph*** of this system.
- **Formulate** the state graph as an ***LTS*** (via a triple $(S, \longrightarrow, L)$).

  Assume: Set P of atoms is: $\{ c \geq 1, c \leq 1 \}$



Labelled Transition System (LTS): Formulation & Paths



at state s_0, $p \wedge q \wedge \neg r$

$\neg p \wedge q \wedge r$

$\neg p \wedge \neg q \wedge r$

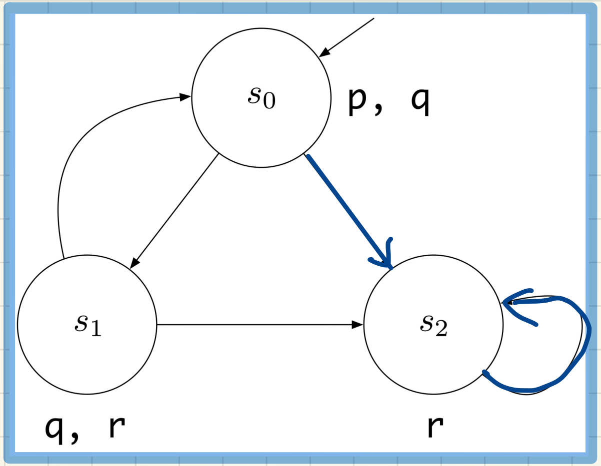
Assume: $\mathcal{P} = \{p, q, r\}$

$M = (S, \longrightarrow, L)$

$S = \{s_0, s_1, s_2\}$

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

$L = \{(s_0, \underline{\{p, q\}}), (s_1, \underline{\{q, r\}}), (s_2, \underline{\{r\}})\}$



name of state

Path : $\boxed{S_0} \to S_2 \to S_2 \to S_2 \to \cdots$

$\pi =$

notions of path components:

S_1 S_2 S_3 S_4

indices

Path Suffix

π^0 ✗

$\pi^1 = \pi$

$\pi^2 = S_2 \to S_2 \to \cdots$

$\pi = S_1 \to S_2 \to S_3 \to S_4 \to S_5$

$(\pi^2)^3 = S_4 \to S_5 \to \cdots$

$= \pi^4$