Lecture 9 - February 7

Model Checking

Examples: LTS Formulation
Paths, Unwinding All Possible Paths
Path Satisfaction: X, G, F

Announcements

- Lab2 released
- WrittenTest1 coming

  ↳ cover until and including today

  \+ some left-over examples

  (to be finished within first 20 min on Thursday).

Labelled Transition System (LTS)

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

labelling function

$L \in S \to \mathbb{P}(P)$

a set of atoms that are satisfied by the state

~~$L \in S \to P$~~

given a state, return a member in P

S: a finite set of states

↳ values of variables

$\longrightarrow$: transition relation

set of pairs.

$\longrightarrow \in \boxed{S \leftrightarrow S}$

the set of all relations on states.

P: a set of atomic propositions (which evaluate to T or F)

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

S_0 $x=2$ S_1 $x=-1$ S_2 $x=6$

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

Q. Formulate **deadlock freedom**:

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

$S.$ $S_1.$

$$\forall s \cdot s \in S \Rightarrow (\exists s' \cdot s' \in S \land \boxed{(s, s') \in \longrightarrow})$$

~~$L(S) \neq \emptyset$~~

Labelled Transition System (LTS)

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

$$0 \le c \le 3$$

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.
- $\boxed{\textbf{Formulate}}$ the state graph as an ***LTS*** (via a triple $(S, \longrightarrow, L)$).

  Assume: Set P of atoms is: $\{ \boxed{c \ge 1}, \boxed{c \le 1} \}$

Exercise

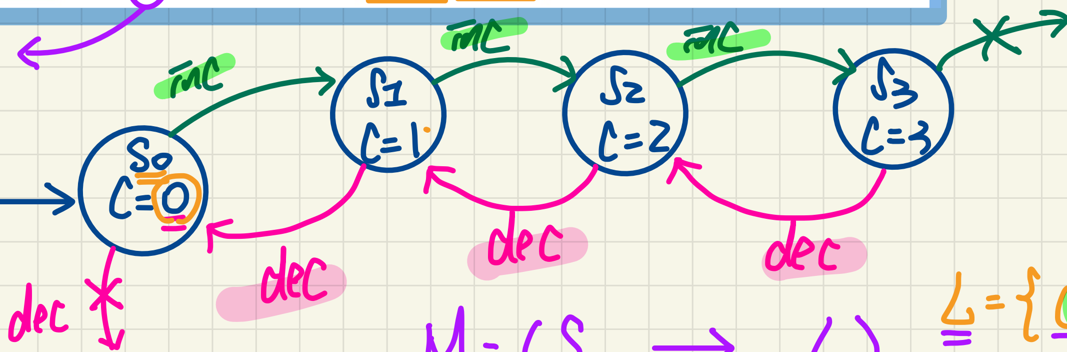
$0 < c_1 \le 2$ inc_1 dec_1

$3 \le c_2 \le 5$ inc_2 dec_2

init: $c_1 = 1$

$c_2 = 3$

properties that we're interested in verifying.



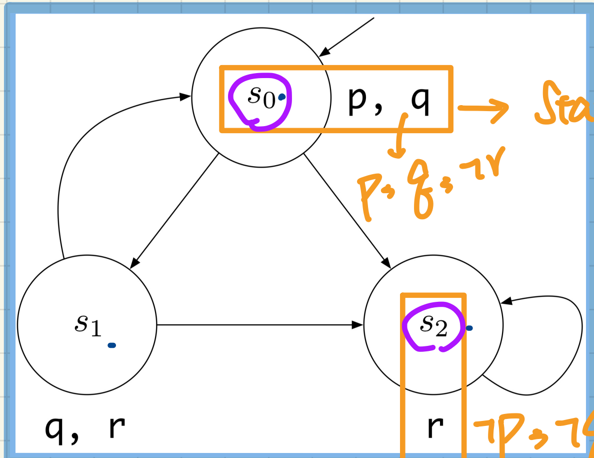
$S = \{s_0, s_1, s_2, s_3\}$

$\longrightarrow = \{(s_0, s_1), (s_1, s_2), (s_2, s_3), (s_3, s_2), (s_2, s_1), (s_1, s_0)\}$

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

$L = \{(s_0, \{c \le 1\}), (s_1, \{c \ge 1, c \le 1\}), (s_2, \{c \ge 1\}), (s_3, \{c \ge 1\})\}$

Labelled Transition System (LTS): Formulation & Paths



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

→ State s_0 satisfies p and q
(implicitly, r is not satisfied)

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

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

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

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

state names

Path: $\pi = s_0 \rightarrow s_2 \rightarrow s_2 \rightarrow s_2 \rightarrow \cdots$

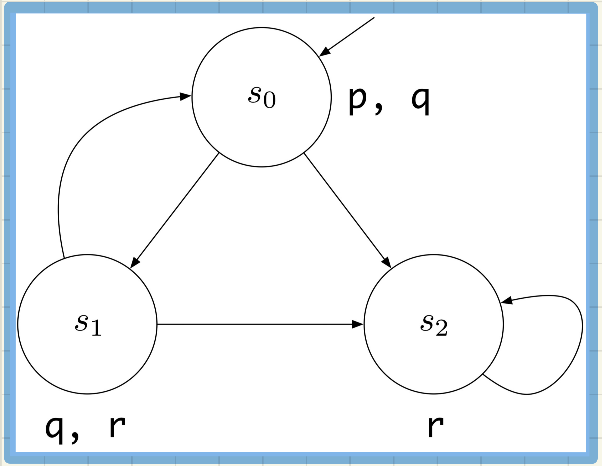
$s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow s_4 \rightarrow \cdots$

indices

1st state in path

2nd state in path

3rd state in path



$\pi^3 = s_0 \to s_1 \to s_0 \to s_1 \to \cdots$

$\pi = s_1 \to s_2 \to s_3 \to s_4 \to s_5 \to \cdots$

$(\pi^2)^3 = s_4 \to s_5 \to \cdots$

$= \pi^4$

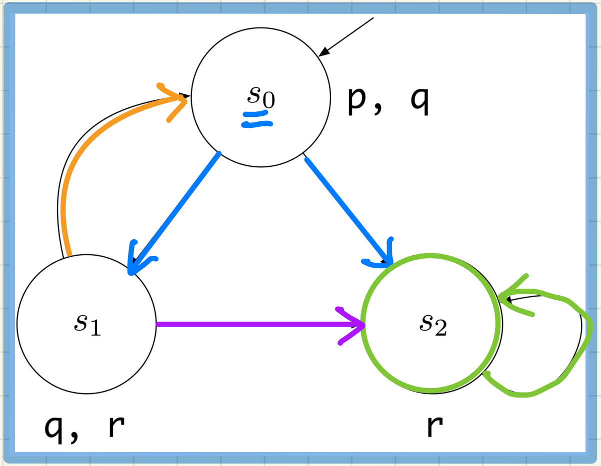
$\pi = s_0 \to s_1 \to s_0 \to s_1 \to s_0 \to s_1 \to \cdots$

Pattern: $s_1 \quad s_2 \quad s_3 \quad s_4 \quad s_5 \quad s_6$

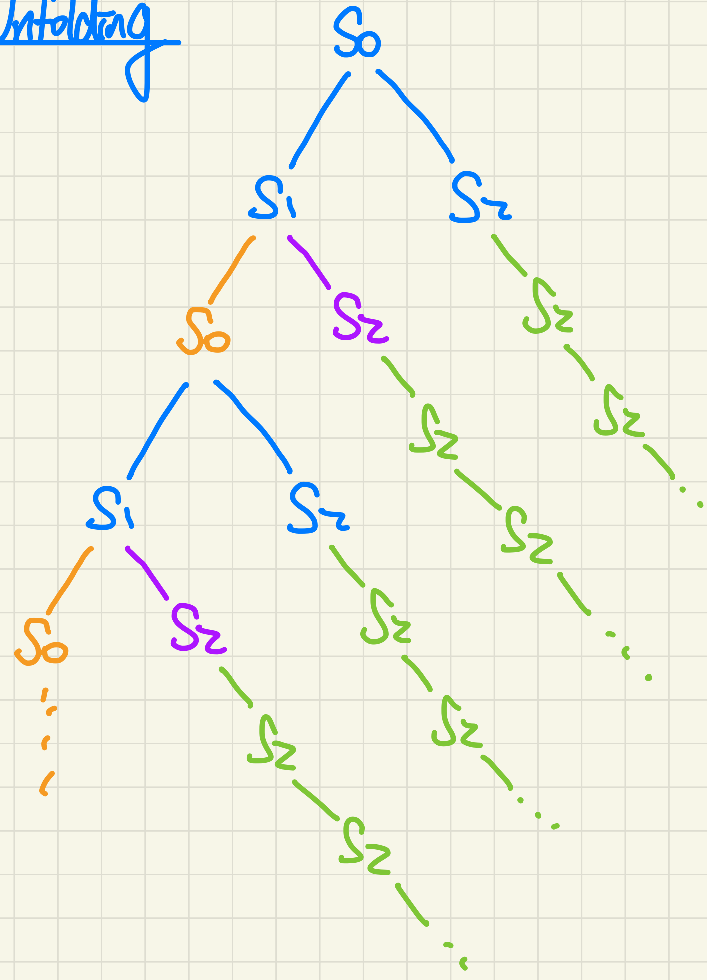
$\cancel{\pi^0}$

$\pi^1 = \pi$

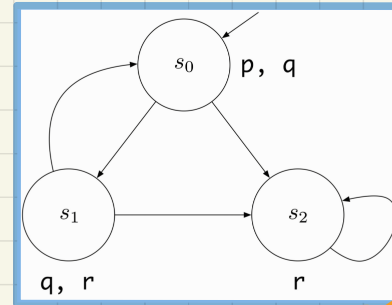
$\pi^2 = s_1 \to s_0 \to s_1 \to s_0 \to s_1 \to \cdots$



Unfolding



Path Satisfaction: Logical Operations



A **path** satisfies a **proposition** if its **initial state** ("**current state**") satisfies it.

first state in π

$$s_1 \to s_2 \to \cdots \to s_{i-1} \to s_i \to s_{i+1} \to \cdots$$

1st state

e.g. $\pi = s_0 \to s_2 \to s_2 \to \cdots$

$\pi \models p$

$\pi \not\models r$

$\pi \models p \iff p \in L(s_1)$ 1st state in path

$\pi \models \top$ ✓ 1st state satisfies $\top$ labelling function

$\pi \not\models \bot \iff \neg(\pi \models \bot)$

$\pi \models \neg\phi \iff \neg(\pi \models \phi)$

$\pi \models \phi 1 \wedge \phi 2 \iff \pi \models \phi_1 \wedge \pi \models \phi_2$

$\pi \models \phi 1 \vee \phi 2$

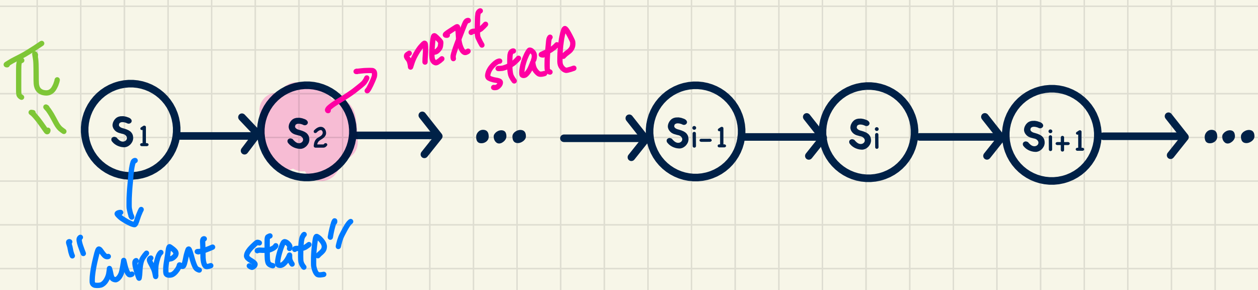
$\pi \models \phi 1 \Rightarrow \phi 2$

[redacted]

Path Satisfaction: Temporal Operations (1)

A **path** satisfies $X\phi$

if the **next state** (of the "current state") satisfies it.



Formulation (over a path)

$$\pi \models X\phi \iff \pi^2 \models \phi$$

*

Q. What is π^3 $\pi 3 \models X\, p$ checking?

Path Satisfaction: Temporal Operations (2)

Global

A **path** satisfies $G\phi$

if the every state satisfies it.

Formulation (over a path)

$$\pi \models G\phi \iff \forall i \cdot i \geq 1 \Rightarrow \boxed{\pi^i \models \phi}$$

Path Satisfaction: Temporal Operations (3)

Future

A **path** satisfies $F\phi$

if some future state satisfies it.

$$s_1 \to s_2 \to \cdots \to s_{i-1} \to s_i \to s_{i+1} \to \cdots$$

Formulation (over a path)

$$\pi \models F\phi \iff \exists i.\ i \geq 1 \wedge \boxed{\pi^i \models \phi}$$