Transformational Systems

Observable only at the beginning and the end of their execution ("black box")

input $\longrightarrow$ [system] output $\longrightarrow$

with no interaction with the environment.

- specified by

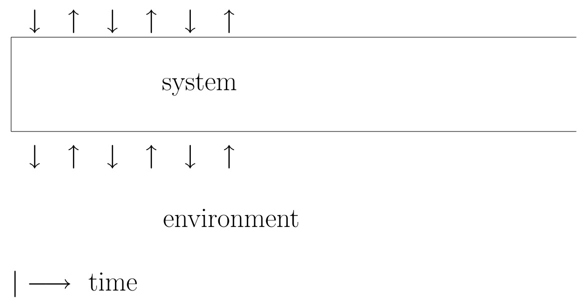
  input-output relations
  $\Downarrow$
  state formulas (assertions)
  First-Order Logic

- typically

  terminating sequential programs
  e.g., input $x \geq 0 \rightarrow$ output $z = \sqrt{x}$

Reactive Systems

Observable throughout their execution ("black cactus")



Interaction with the environment

- specified by

  their on-going behaviors
  (histories of interactions with their environment)
  $\Downarrow$
  sequence formulas
  Temporal Logic

- Typically
  - Airline reservation systems
  - Operating systems
  - Process control programs
  - Communication networks

SPL Semantics (Con't)

accessible configuration –
appears as value of π in some accessible state

```
Example:
```

$\left\{[\ell_0], [m_1]\right\}$ does not appear in any accessible state

Is a given configuration accessible?

Undecidable

The Mutual-Exclusion Problem

$$\textbf{loop forever do} \left[\begin{array}{l}\textbf{noncritical}\\ \cdots\cdots\cdots\\ \textbf{critical}\\ \cdots\cdots\cdots\end{array}\right] \quad \| \quad \textbf{loop forever do} \left[\begin{array}{l}\textbf{noncritical}\\ \cdots\cdots\cdots\\ \textbf{critical}\\ \cdots\cdots\cdots\end{array}\right]$$

Requirements:

- Exclusion

  While one of the processes is in its critical section, the other is not

- Accessibility

  Whenever a process is at the noncritical section exit, it must eventually reach its critical section

`Example:` mutual exclusion by semaphores Fig. 0.7

Expressibility

There are properties that cannot be specified by a quantifier-free temporal logic formula.

Example:

Specify the property
"x assumes the value 0 only, if ever, at even positions"
i.e., "at positions $0, 2, 4, \ldots$"

- cannot be expressed in quantifier-free TL
- can be expressed in (quantified) TL

  Quantifying over flexible boolean variable b:
  $\exists b[b \wedge \Box(b \leftrightarrow \neg \bigcirc b) \wedge \Box(x = 0 \rightarrow b)]$.
  $\forall b[b \wedge \Box(b \leftrightarrow \neg \bigcirc b) \rightarrow \Box(x = 0 \rightarrow b)]$.

  Why not

$$x = 0 \wedge \Box[x = 0 \rightarrow \bigcirc\bigcirc(x = 0)]?$$

Temporal vs First-Order

TL formula

$$\Box(p \rightarrow \Diamond[r \wedge \Diamond q])$$

can be transformed into FOL formula

$$(\forall t_1 \geq 0)\left[p(t_1) \rightarrow (\exists t_2)\left[\begin{array}{c} t_1 \leq t_2 \wedge r(t_2) \wedge \\ (\exists t_3)(t_2 \leq t_3 \wedge q(t_3)) \end{array} \right] \right]$$

where t_1, t_2, t_3 are integers.