Temporal Logic

- A *logic* that talks about temporal relations beteween states

Formulas

- A temporal formula talks about a sequence of states

$$\sigma = s_0, s_1, s_2, \ldots$$

- The formula is relative to a given position i: *"now"*
- A *state predicate* p talks about "now"
- Temporal operators:

  $\Box P$ P holds *always* (from now)

  $\Diamond P$ P holds *eventually* (from now)
- Combinations:

  $\Box\Diamond P$ P holds *over and over again*

  $\Diamond\Box P$ P holds *eventually forever*

Some Temporal Laws

- $\neg\Box P \Leftrightarrow \Diamond\neg P$ $\quad$ $\Box(P \Rightarrow Q) \Rightarrow (\Box P \Rightarrow \Box Q)$

  $\Box P \Rightarrow P$ $\quad$ $\Box P \wedge \Diamond Q \Rightarrow \Diamond(P \wedge Q)$

  $P \Rightarrow \Diamond P$
- $\Box(P \wedge Q) \Leftrightarrow (\Box P \wedge \Box Q)$ $\quad$ $\Diamond\Box(P \wedge Q) \Leftrightarrow (\Diamond\Box P \wedge \Diamond\Box Q)$

  $\Diamond(P \vee Q) \Leftrightarrow (\Diamond P \vee \Diamond Q)$ $\quad$ $\Box\Diamond(P \vee Q) \Leftrightarrow (\Box\Diamond P \vee \Box\Diamond Q)$
- $\Box\Box P \Leftrightarrow \Box P$ $\quad$ $\Box\Diamond\Box P \Leftrightarrow \Diamond\Box P$

  $\Diamond\Diamond P \Leftrightarrow \Diamond P$ $\quad$ $\Diamond\Box\Diamond P \Leftrightarrow \Box\Diamond P$
- $\Box(P \vee Q) \Rightarrow (\Box P \vee \Diamond Q)$

The Leads-to Operator

Definition

- $P \leadsto Q \triangleq \Box(P \Rightarrow \Diamond Q)$ "P always leads to Q"

Some rules

- $\Box(P \Rightarrow Q) \Rightarrow (P \leadsto Q)$
- $(P \leadsto Q) \wedge (Q \leadsto R) \Rightarrow (P \leadsto R)$
- $(P \leadsto R) \wedge (Q \leadsto R) \Rightarrow ((P \vee Q) \leadsto R)$
- $(P \leadsto Q) \vee (P \leadsto R) \Rightarrow (P \leadsto (Q \vee R))$

Fair Scheduling

- A *schedule* determines the choices among enabled actions
- Given $a : \langle\, B \rightarrow S \,\rangle$ in some process P_i

Weak Fairness (WF)

- $\Box(\mathit{at}\ a \wedge B) \leadsto \mathit{after}\ a$
- Also known as *fair process exectution*
- Every process must be visited infinitely often
- Usually implemented by round-robin scheduling

Strong Fairness (SF)

- $\Box\Diamond(\mathit{at}\ a \wedge B) \leadsto \mathit{after}\ a$
- Can be implemented using WF + queues
- Hard to implement in general

Liveness Properties of Program Constructs

Basic progress examples

- $l\colon \langle\, x := e \,\rangle$ $\qquad$ $at\ l \leadsto after\ l$
- $l\colon$ **if** B **then** S_1 **else** S_2 $\qquad$ $at\ l \leadsto at\ S_1 \vee at\ S_2$

Derived rules

- For any S

$$in\ S \Rightarrow (\Box in\ S \vee \Diamond after\ S)$$

- For $l\colon (S_1; S_2)$

$$\frac{at\ S_1 \leadsto after\ S_1 \qquad at\ S_2 \leadsto after\ S_2}{at\ l \leadsto after\ l}$$

- For $w\colon$ **while** B **do** S

$$\frac{in\ S \leadsto after\ S}{in\ w \wedge \Box\neg B \leadsto after\ w}$$

Liveness of Critical Regions

- **Obligingness:**

$$in\ entry_i \wedge (\forall j \neq i : \Box in\ noncrit_j) \leadsto at\ crit_i$$

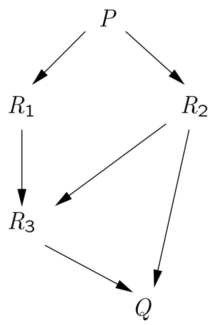
- **Resolution:**

$$(\exists i : in\ entry_i) \leadsto (\exists j : at\ crit_j)$$

- **Fairness:**

$$in\ entry_i \leadsto at\ crit_i$$

Proof Lattices

- 

represents the formulas
$$\left\{ \begin{array}{l} P \leadsto R_1 \lor R_2 \\ R_1 \leadsto R_3 \\ R_2 \leadsto Q \lor R_3 \\ R_3 \leadsto Q \end{array} \right.$$

Semaphore Properties

Safety

- Semaphore S represented by $s : integer$
- $\mathtt{P}(S)$: $\langle\, s > 0 \rightarrow s := s - 1 \,\rangle$
  $\mathtt{V}(S)$: $\langle\, s := s + 1 \,\rangle$

Liveness

- $at\ \mathtt{V}(S) \leadsto after\ \mathtt{V}(S)$
- *Weakly fair semaphore*
  $$(at\ \mathtt{P}(S) \land \Box s > 0) \leadsto after\ \mathtt{P}(S)$$
- Techniques: Busy-wait, semi busy-wait, wake-all
- *Strongly fair semaphore*
  $$(at\ \mathtt{P}(S) \land \Box\Diamond s > 0) \leadsto after\ \mathtt{P}(S)$$
- Techniques: FIFO, round-robin, aging