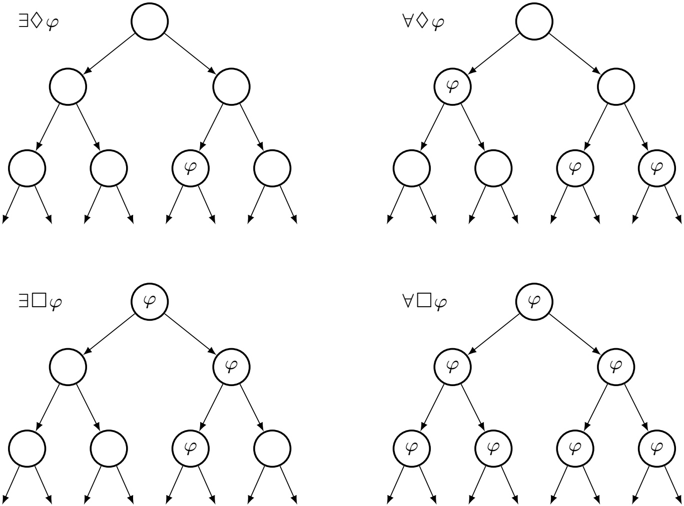
Computational Tree Logic (CTL)



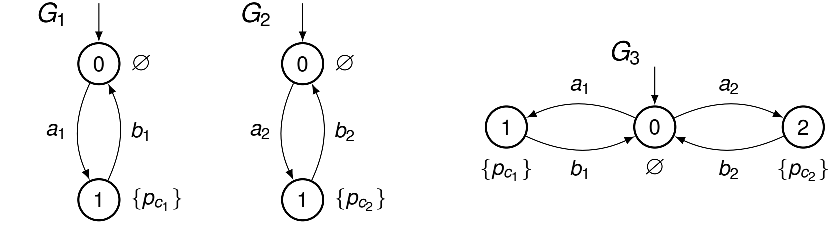
Safety

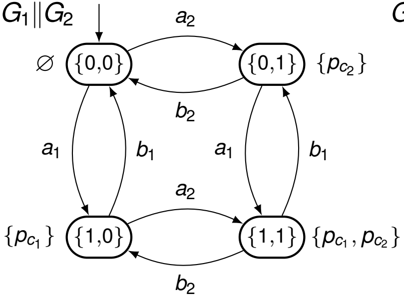
Safety specifications: Nothing bad will ever happen.

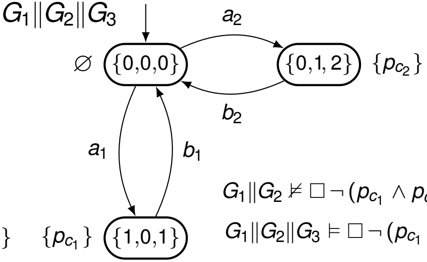
- Invariant: $\Box\, Temp_1 \leq temp \leq Temp_2)$,
- Invariant: $\Box\, 0 \leq \#parts \leq BufferSize)$,
- Mutual exlusion: $\Box \neg(p_{c_1} \wedge p_{c_2})$

  p_{c_k} = state label for task k in critical (mutual exclusion) zone.

Mutual Exclusion







$G_1 \| G_2 \nvDash \Box \neg (p_{c_1} \wedge p_{c2})$

$G_1 \| G_2 \| G_3 \vDash \Box \neg (p_{c_1} \wedge p_{c_2})$

Liveness

Liveness specifications: Something good will eventually happen.

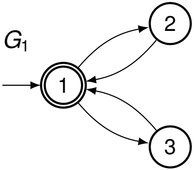
- p_r = request state label,
- p_e = execution state label,
- p_n = non-marked state label,
- $\varphi_m = \neg p_n$ = state label expression for a marked state.

Examples of liveness specifications:

- $\Diamond \varphi_m$ - A marked state will eventually be reached at least one time
- $\Box \Diamond \varphi_m$ - A marked state will eventually be reached infinitely many times,
- $p_r \rightarrow \Diamond p_e$ - A request in initial state will eventually be executed,
- $\Box (p_r \rightarrow \Diamond p_e)$ - A request at any state will eventually be executed.

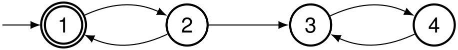
Liveness

G_1



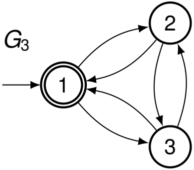
$G_1 \models \Box \Diamond \, \varphi_m$

G_2



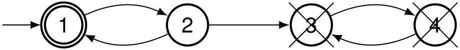
$G_2 \not\models \Box \Diamond \, \varphi_m$

G_3



$G_3 \not\models \Box \Diamond \, \varphi_m$

G_4

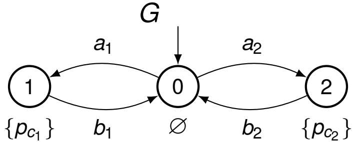


$G_4 \models \Box \Diamond \, \varphi_m$

Fairness

Fairness specifications: Guarantee that all alternative paths will be execetuded.

Typical application: mutual exclusion of shared resources.



Unconditional fairness specification:

$$\Box\Diamond\, p_{c_1} \wedge \Box\Diamond\, p_{c_2}$$

The states with labels p_{c_1} and p_{c_2} will both be reached infinitely many times.

Specifications Including Next and Until

Three state temperature model, $x_1 \leftrightarrow T \leq T_1$, $x_2 \leftrightarrow T_1 < T \leq T_2$ and $x_3 \leftrightarrow T > T_2$

$$\Box(x_1 \rightarrow \neg \bigcirc x_3)$$
$$\Box(x_2 \rightarrow \bigcirc(x_1 \vee x_3))$$

An elevator does not change direction before completing its current task

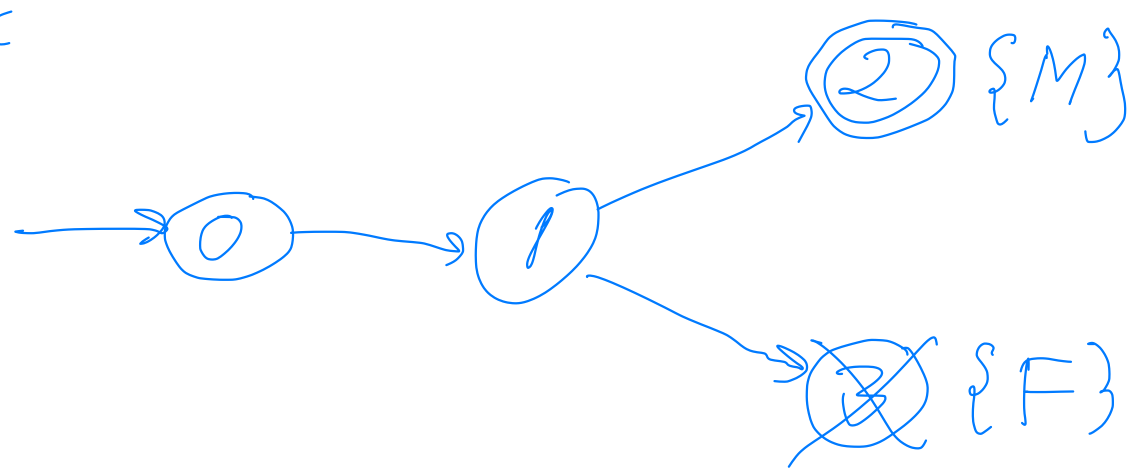
$$\Box(\mathit{floor} = 2 \wedge \mathit{buttonFloor5} \wedge \mathit{direction} = \mathit{up} \\ \rightarrow (\mathit{direction} = \mathit{up}\ U\ \mathit{floor} = 5))$$

9 (cont) Temporal Logic

state labels in automata

An automaton including also state labels is called a *transition system*

Ex



AP = set of atomic propositions. In this example $AP = \{M, F\}$.

Labeling function $\lambda : \Sigma \to 2^{AP}$

set of states

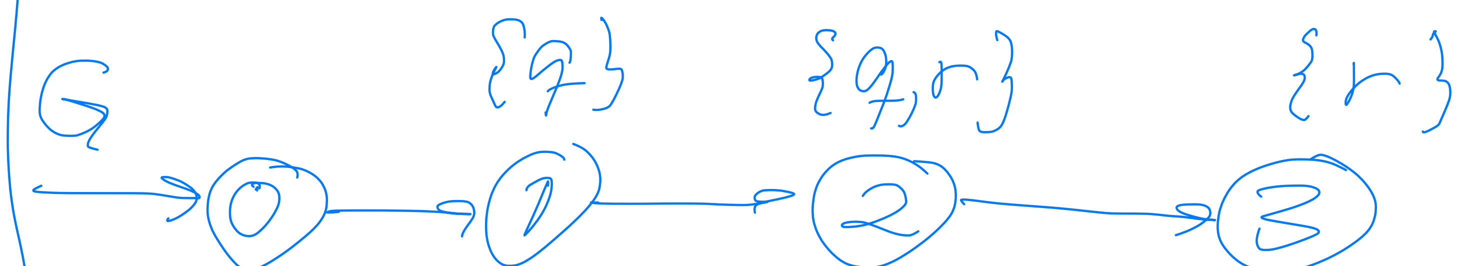
$\lambda(2) = \{M\}$ $\quad \lambda(3) = \{F\}$

$\lambda(0) = \lambda(1) = \emptyset$ (default)

More generally

$AP = \{p, q, r, \ldots\}$

Ex



$[\![q]\!]$ = set of states including label q $= \{1, 2\}$

$[\![r]\!] = \{2, 3\}$

An algorithm will now be presented where $[\![\exists \Diamond q]\!]$ is computed

Note that $[\![\exists \Diamond q]\!] = \{0, 1, 2\}$

μ-calculus

A tool to generate algorithms for analyzing in which states a temporal logic formula is valid. This includes both LTL, CTL and CTL*.

Ex Expansion law for

$$\exists \Diamond q \equiv q \vee \exists \circ (\exists \Diamond q)$$

Introduce a logical variable $y = \exists \Diamond q \Rightarrow$ The expansion law can be expressed as

$$y = q \vee \exists \circ y$$

This expression will be iterated until a fixed point is reached.

μ-calculus is a logic that includes fixed point operators.

Syntax for μ-calculus

$\varphi ::= p \mid y \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid f(\varphi) \mid \mu y.\varphi$

$p \in AP$

f = function including the next modality + quantifier either

$\exists\bigcirc$ or $\forall\bigcirc$,

$\mu y.\varphi$ is the least fixed point

$\nu y.\varphi$ is the greatest fixed point

semantics of μ-calculus

Given a transition system

$G = \langle X, \Sigma, T, I, AP, \lambda \rangle$

the set of states $[\![\varphi]\!]$ where the μ-calculus formula φ holds is defined as follows:

$[\![p]\!] = \{x \mid p \in \lambda(x)\}$

$[\![y]\!] = Y \in 2^X$

$[\![\neg\varphi]\!] = \sim[\![\varphi]\!] = X \setminus [\![\varphi]\!]$

$[\![\varphi_1 \wedge \varphi_2]\!] = [\![\varphi_1]\!] \cap [\![\varphi_2]\!]$

$[\![f(\varphi)]\!] = \mathrm{Pre}^f([\![\varphi]\!])$

$[\![\mu y.\varphi]\!] = \mu Y.\,\underline{\Psi}(Y) =$ least fixed point for $Y =$

$= \bigcap \{Y \in 2^X \mid Y = \Psi(Y)\}$

$[\![\nu y . \Psi]\!] = \nu Y . \Psi(Y) =$

= greatest fixed point

for $Y = \bigcup \{ Y \in 2^{\Sigma} \mid Y = \Psi(Y) \}$

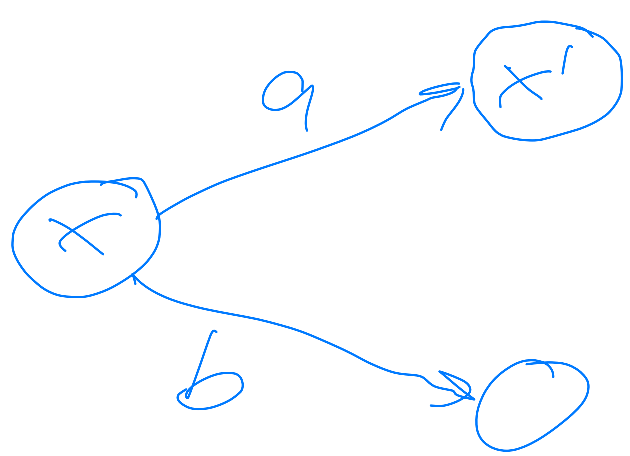
where $\Psi(Y) = \Psi([\![y]\!]) =$

$= [\![\Psi(y)]\!]$

$\delta(x,a)$ = transition function

$\Sigma(x)$ = active event set

= possible events defined in state x



$x' = \delta(x,a)$

$\Sigma(x) = \{a, b\}$

$Pre^{\exists}(Y) = [\![\exists \circ y]\!] =$

$= \{x \mid \exists a \in \Sigma(x) : \delta(x,a) \subseteq Y\}$

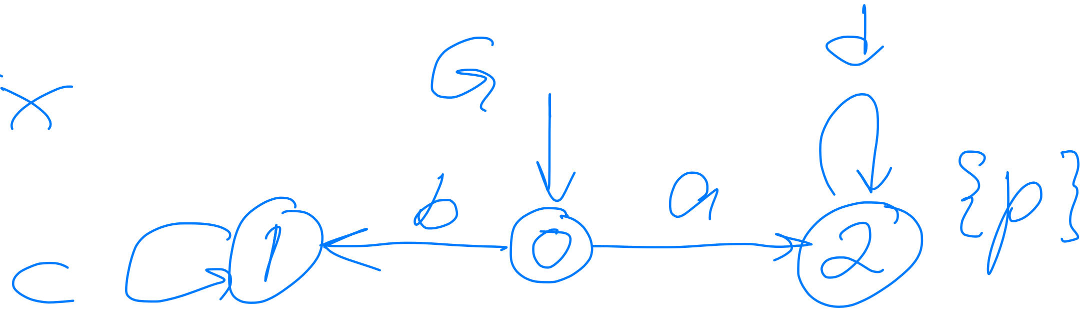
For at least one event a, $x' = \delta(x,a) \in Y \Leftrightarrow$ coreachability one step backward.

$Pre^{\forall}(Y) = [\![\forall \circ y]\!] =$

$= \{x \mid \forall a \in \Sigma(x) : \delta(x,a) \subseteq Y\}$

All target states from x must belong to Y

Ex

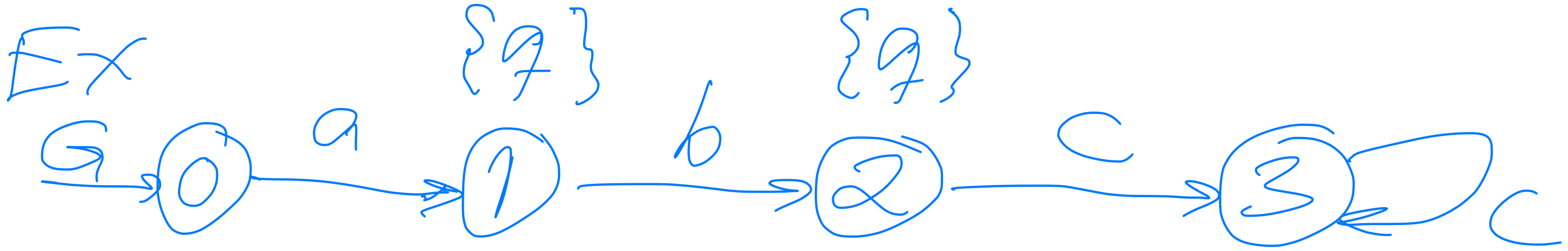


$$Pre^{\exists}([\![p]\!]) = Pre^{\exists}(\{2\}) = \{0,2\}$$

$$Pre^{\forall}([\![p]\!]) = Pre^{\forall}(\{2\}) = \{2\}$$

state 0 is not included since state 1 is missing in $Pre^{\forall}(\{2\})$

Ex



$[\![\exists\Diamond q]\!]$?

$\exists\Diamond q \longleftrightarrow$ μ-calculus formula

$$\mu y.\ \underbrace{q \vee \exists\bigcirc y}_{\psi(y)}$$

$$[\![\exists\Diamond q]\!] = [\![\mu y.\ \psi(y)]\!] =$$

$= \mu Y.\ \underline{\Psi}(Y)$ where

$$\underline{\Psi}(Y) = [\![\psi(y)]\!] = [\![q \vee \exists\bigcirc y]\!]$$

$$= [\![q]\!] \cup [\![\exists\bigcirc y]\!] = [\![q]\!] \cup Pre^{\exists}(Y)$$

where $Y = [\![y]\!]$

The least fixed point of $Y = \Psi(Y)$ is obtained by iterating $Y_{i+1} = \Psi(Y_i)$ for $i = 0, 1, 2, \ldots$ with $Y_0 = \emptyset$ until $Y_{i+1} = Y_i$

$Y_1 = \Psi(Y_0) = [\![q]\!] \cup Pre^{\exists}(Y_0)$

$= \{1,2\} \cup \underbrace{Pre^{\exists}(\emptyset)}_{\emptyset} = \{1,2\}$

$Y_2 = \Psi(Y_1) = [\![q]\!] \cup Pre^{\exists}(Y_1)$

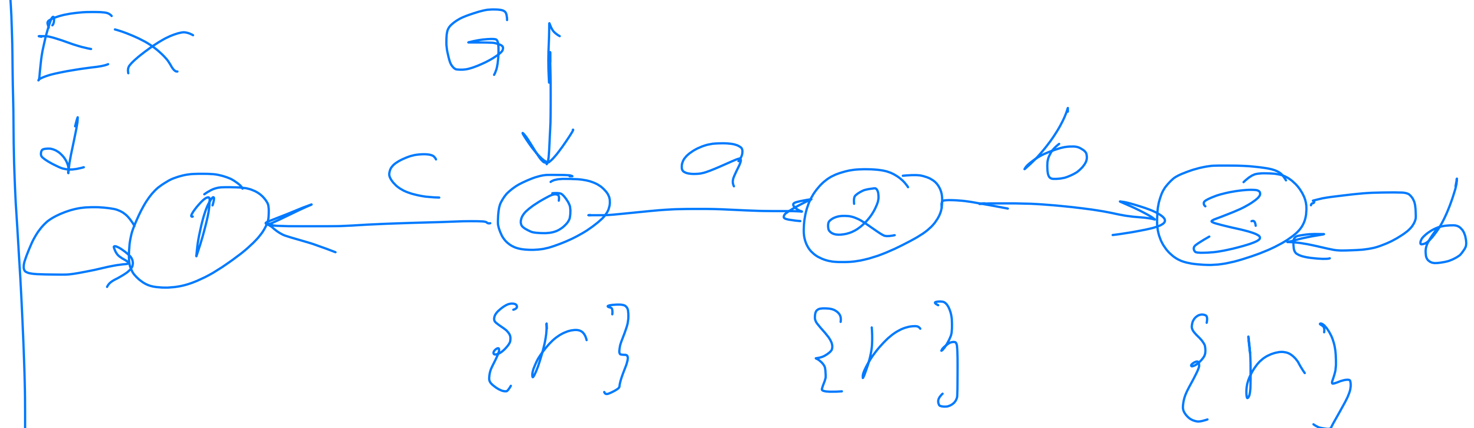
$= \{1,2\} \cup \{0,1\} = \{0,1,2\}$

$Y_3 = \Psi(Y_2) = \{1,2\} \cup \underbrace{Pre^{\exists}(\{0,1,2\})}_{\{0,1\}}$

$= \{0,1,2\} = Y_2 = Y_\omega$

$[\![\exists \Diamond q]\!] = \{0,1,2\}$

Ex



$\forall \Box r \leftrightarrow \nu y. \underbrace{r \wedge \forall \circ y}_{\psi(y)}$

$[\![\forall \Box r]\!] = \nu Y. \Psi(Y)$ where

$\Psi(Y) = [\![r \wedge \forall \circ y]\!] = [\![r]\!] \cap Pre^{\forall}(Y)$

Greatest fixed point is obtained by iterating $Y_{i+1} = \Psi(Y_i)$ with $Y_0 = \Sigma = \{0,1,2,3\}$

$Y_1 = \Psi(Y_0) = \underbrace{\{0,2,3\}}_{[\![r]\!]} \cap \underbrace{Pre^{\forall}(\Sigma)}_{\Sigma} =$

$= \{0, 2, 3\}$

$Y_2 = \Psi(Y_1) = [\![r]\!] \cap Pre^{\forall}(\{0, 2, 3\}) = \{2, 3\}$

state 0 not included since the target state 1 from state 0 is not included in Y in

$Pre^{\forall}(Y) \quad Y = \{0, 2, 3\}$

$Y_3 = [\![r]\!] \cap \underbrace{Pre^{\forall}(\{2, 3\})}_{\{2,3\}} = Y_2 = Y_\omega$

fixed point

$[\![\forall \Box r]\!] = Y_\omega = \{2, 3\}$