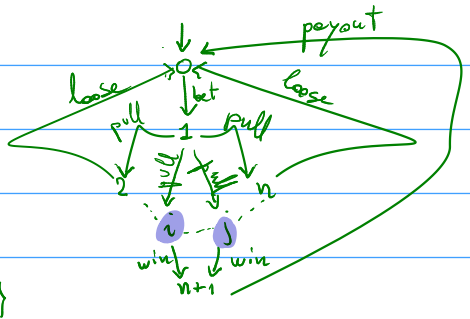
Example. A (simplified) 3-wheels slot machine



$S = \{0, \dots, n+1\}$ & $I = \{0\}$

$Act = \{bet, win, loose, pull, payout\}$

Fix an interval $W = [i,j]$ with $2 \le i \le j \le n$

$\to = \{(0, bet, 1)\} \cup \{1\} \times \{pull\} \times [2,n] \cup \{(n+1, payout, 0)\}$

$\cup\ W \times \{win\} \times \{n+1\} \cup S \setminus W \times \{loose\} \times \{0\}$

3-wheels machine $Z_{3,3}$

$AP = \bigcup_{i=1}^{3} \{w_i = f \mid f \in Fruits\} \cup \bigcup_{h \in W} \{price = h\}$ where $Fruits = \{apple, pear, bonus \dots\}$

$L : h \mapsto \bigcup_{i=1}^{3} \{w_i = c_i(h)\} \cup \{price = p(h)\}$

where $c_1, c_2, c_3 : S \to Fruit$ $\quad p : S \to \mathbb{N}$ s.t. $\forall h \in S : p(h) > 0 \iff h \in W$

Exercise: the cardinality of S should be much bigger than the cardinality of W for the TS above to be realistic. Why? (Hint: think of a possible implementation)

NON-DETERMINISM

is crucial modelling mechanism

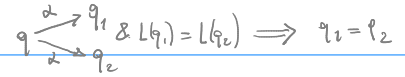
- under-specification
- to abstract away from low level details
- to model uncontrollable behaviour of the environment

(e.g. transitions from 1 in the slot machine)

Deterministic TS $|I| = 1$

- **action deterministic** $\forall q \in S, \alpha \in Act : |Post(q,\alpha)| \le 1$ $\quad (:= \{q' \in S : q \xrightarrow{\alpha} q'\})$

- **AP deterministic** $\forall q \in S, A \in 2^{AP} : |\{q' \in Post(q) \mid L(q') = A\}| \le 1$ $\quad (:= \bigcup_{\alpha \in Act} Post(q,\alpha))$



Executions & Traces

Execution fragment are sequences $\rho \in S(Act\,S)^* \cup S(Act\,S)^\omega$ (finite / infinite) s.t.

$\rho = q_0 \alpha_1 q_1 \alpha_2 q_2 \cdots \alpha_n q_n \cdots \Rightarrow q_i \xrightarrow{\alpha_{i+1}} q_{i+1}$ for all i

ρ **initial** if $q_0 \in I$

ρ **maximal** if ρ infinite or $\rho = q_0 \alpha_1 q_1 \alpha_2 q_2 \cdots \alpha_n q_n$ & $Post(q_n) = \emptyset$

An **execution** is an initial & maximal execution fragment

The set **Reach(TS)** of **reachable states of TS** is the set of states q of TS s.t. there is an initial execution fragment ending in q

A note inspired by Duncan Attard's question (ay 20/21)
"Why do we need both labelling & actions to express properties?":

Verification can be { action based / state based / action + state based (the most complex case)

Execution fragments are used for action-based verification; this approach is commonplace for modelling communication.

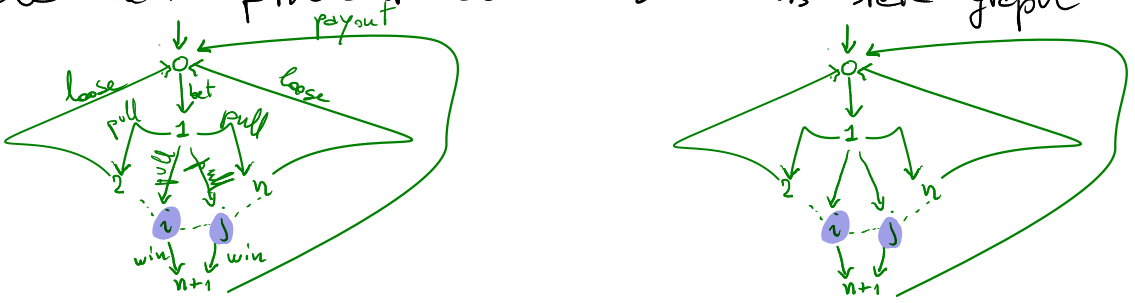
We now devote our attention to a state-based approach, where algorithms are oblivious of actions. Formally:

the state graph $G(TS)$ of $TS = (S, Act, \rightarrow, I, AP, L)$ is defined as

$$G(TS) = \langle S, \bigcup_{q \in S} \{q\} \times Post(q) \rangle$$

intuitively $G(TS)$ is obtained by "removing" the actions from the transitions of TS

Example: the TS of the slot machine & its state graph



notice that state labels do not "disappear" even though they are not explicitly represented

Notation: given a sequence $\sigma = \sigma_0 \sigma_1 \ldots \sigma_n \ldots$

- the lenght of σ is $|\sigma|$ (if σ is infinite, $|\sigma| = \infty$)
- the i-th element of σ is $\sigma[i]$
- the last element of σ is $last(\sigma)$, provided that σ is finite

From now on we assume TS fixed

LINEAR TIME BEH & PROPERTIES

A **PATH FRAGMENT** of TS is a path on its state graph

$\pi \in S^* \cup S^\omega$ s.t. $\forall\, 0 \le i \le |\pi| : \pi[i+1] \in Post(\pi[i])$

π maximal if $\pi \in S^* \wedge Post(last(\pi)) = \emptyset$ or $\pi \in S^\omega$

π initial if $\pi[0] \in I$

π path if initial & maximal

$\cup\, trace(\pi)$ $\{\, \pi \in path(TS) : \pi[0] = s \,\}$

TRACE of π $\{L(\pi[i])\}_{0 \le i \le |\pi|}$

$$Traces(TS) := \bigcup_{s \in I} traces(s)$$

An LT property (on AP) is an element P of $2^{(2^{AP})^\omega}$ i.e. $P \subseteq (2^{AP})^\omega$

Examples. Let $AP = \{r, g, y\}$ and P_{light} = "the traffic light is infinitely often r"

$P_{light} \ni \{r\}\{r,y\}\{g,y\}\{r\}\{r,y\}\{g,y\}$

$\not\ni \{r\}\{g\}\emptyset\emptyset\emptyset\ldots$

$\ni \{\{r\}\}^\omega$

$\ni X^\omega$ if $r \in X \subseteq AP$

$\ni \{X_i\}_{i \in \omega}$ if $r \in X_i \Leftrightarrow i$ prime

Let $AP = \{c_1, \ldots, c_n\}$

thread k is in the critical section

$$P_{mutex} = \{\{A_i\}_{i \in \omega} \in (2^{AP})^\omega \mid \forall i \ge 0,\ 1 \le h \le k \le n : \{c_h, c_k\} \subseteq A_i \Rightarrow h = k\}$$

$$\equiv \bigwedge_{1 \le h < k \le n} \{c_h, c_k\} \not\subseteq A_1 \wedge \ldots \wedge \bigwedge_{1 \le h < k \le n} \{c_h, c_k\} \not\subseteq A_n$$

Exercise: What does $P' = \{\{A_i\}_{i \ge 0} \in (2^{AP})^\omega \mid \forall i \ge 0\ \exists 1 \le h \le n.\ c_h \in A_i\}$ state? Give two different traces in P'

Exercise: Let P_{slot} : "always $(price = 0 \rightarrow$ eventually $\bigvee_{p \in [1,3]} price = p)$". Give an example of an element of P_{slot} and one of $(2^{AP})^\omega \setminus P_{slot}$

$$\begin{array}{ccccccccccc} TS & & \omega & & I & & s_i \xrightarrow{\alpha_i} s_{i+1} & & & & \\ \pi & = & s_0 & \alpha_1 & s_2 & \cdots & \alpha_n & s_n & \alpha_{n+1} & \cdots & \\ & & \downarrow & & \downarrow & & & \downarrow & & & \\ & & L(s_0) & & L(s_2) & \cdots & & L(s_n) & \cdots & \in & P \quad \text{LT property} \end{array}$$

$$TS \models P$$