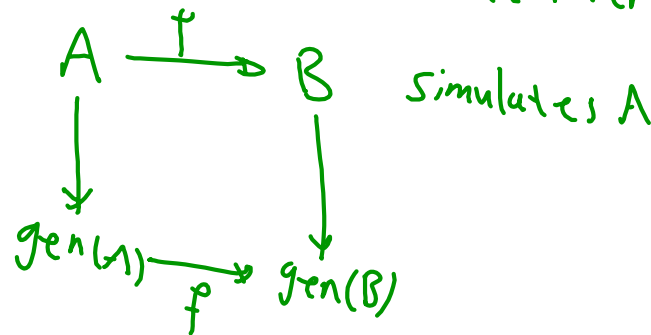


Simulation Relations:

Ex 23.3.3 (timeout automaton)

Ex 23.3.4 (Two-task Race)

→ a timeout occurs in the interval $[k_1, k_2 + 1]$



$gen(A) \rightarrow S$
 $gen(B) \rightarrow u$

↓ Properties of \mathcal{P}

1. $S.now = u.now$

2. $S.status = u.status$

3. $u.last(timeout) \geq$

$$\left\{ \begin{array}{l} S.last(dec) + (S.count - 1)l_2 + l \\ S.last(timeout) \end{array} \right.$$

$S.count > 0$

$S.count = 0$

4. $u.first(timeout) \leq$

$$\left\{ \begin{array}{l} S.first(dec) + (S.count - 1)l_1 + 0 \\ S.first(timeout) \end{array} \right.$$

$S.count > 0$

$S.count = 0$

Assertion 23.3.4 (P, 76s)

$k = s.\text{count} > 0 \Rightarrow 1, 2, 3, 4$ hold

1. $s.\text{now} = u.\text{now}$

2. $s.\text{status} = u.\text{status}$

3. $u.\text{last}(\text{timeout}) \xrightarrow{\text{by def B}} = kl_2 + l$

$\underbrace{s.\text{last}(\text{der})}_{l_2} + (k - 1)l_2 + l$

4.

Step condition:

$$(s, \pi, s') \in \text{trans}(\text{gen}(A))$$

$$\pi = \text{dec}$$

$$\pi = \nu(1)$$

⋮

$$\pi = \text{timeout}$$

Assm: $u \in f(s)$

prove: $u' \in f(s')$

$u = u'$
we need $u \in f(s)$ to prove

$$s.\text{count} > c$$

$$1. s'.\text{now} = s.\text{now} = u.\text{now}$$

$$s.\text{now} + l \leq$$

$$2. s'.\text{status} = \dots \text{ by assump } \geq s.\text{last}(\text{dec}) + l$$

$$3. u.\text{last}(\text{timeout}) \geq \underbrace{s.\text{now}}_{= s.\text{now}} \left\{ \begin{array}{l} s'.\text{last}(\text{dec}) + (s'.\text{count} - 1)l_2 + l \\ s'.\text{last}(\text{timeout}) \end{array} \right.$$

$$s'.\text{count} > c$$

$$s'.\text{last}(\text{dec}) \leq \underbrace{s'.\text{now} + l_2}_{= s.\text{now} + l}$$

$$s'.\text{last}(\text{timeout}) \leq s'.\text{now} + l = s.\text{now} + l$$

$$s'.\text{count} = c$$

Race automation
(P. 741)

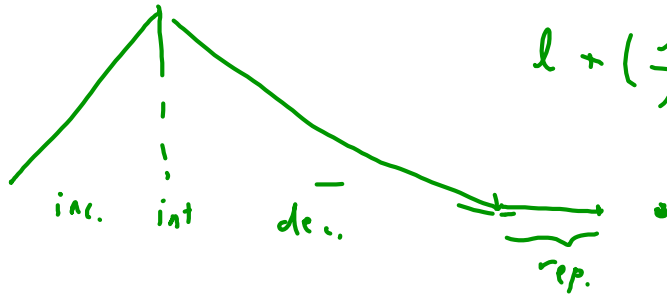
B' automaton (P. 767)

main = { inc., dec., rep. } [l₁, l₂]

int = { set }, [0, l)

flag = false

$\lfloor \frac{l}{l_1} \rfloor + 1$

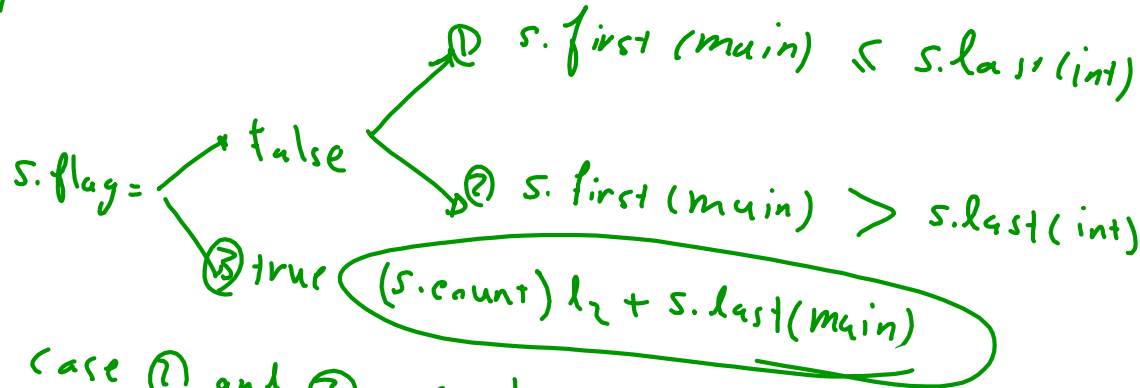


$$l + \left(\frac{l}{l_1}\right) l_2 + l_2 = l + k l + l_2$$

$$k = l_2 / l_1$$

$$\begin{aligned}
 & \text{1. } u.\text{now} - s.\text{now} \\
 & \text{2. } u.\text{reported} = s.\text{reported} \\
 & \text{3. } u.\text{last}(\text{rep.}) \geq \begin{cases} s.\text{last}(\text{int}) + \left[\frac{s.\text{last}(\text{int}) - s.\text{first}(\text{main})}{l_1} \right] l_2 + l_2 \\
 s.\text{last}(\text{main}) + (s.\text{count}) l_2 \end{cases} \\
 & \left(\frac{T}{l_1} + 1 \right) l_2
 \end{aligned}$$

if case ①
otherwise



case ② and ③ are the same

if you don't have time to inc. then you don't inc.