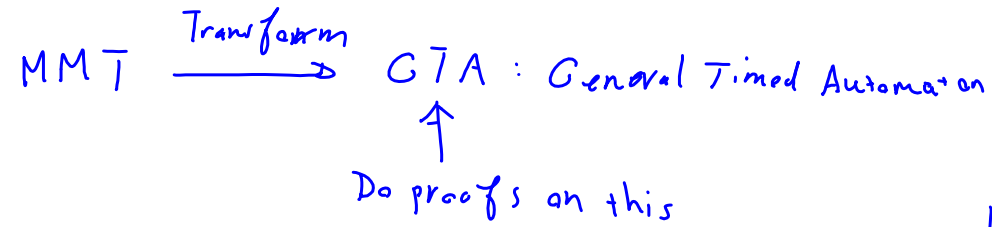


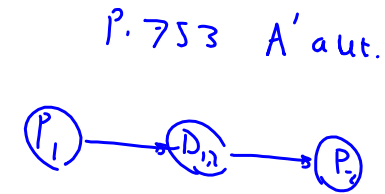
LPE Reading Group

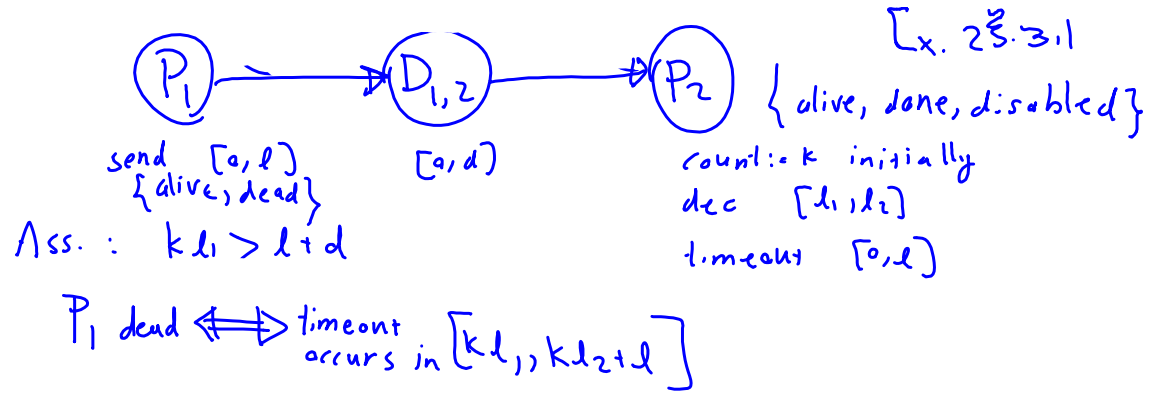
## 2.3 Proof Methods:

- invariant assertions: ~~→~~ Induction
- Simulation relations:



- Examples:
- 1) timeout automaton
    - invariant asser.
    - sim. rel.
  - 2) Race automaton → sim. rel.





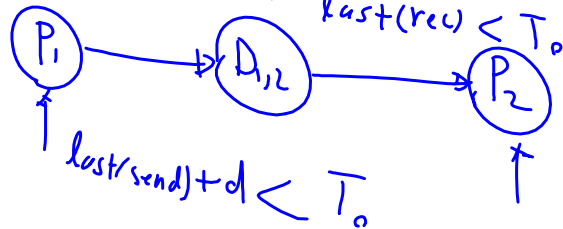
-

Assertion 23.3.3. In any reachable state of  $A$ , if  $status_1 = \text{alive}$ , then the following are true

1.  $count_2 > 0$

2. Either  $last(send) + d < \overbrace{first(dec) + (count_2 - 1)l_1}^{k \quad T_a \quad (k-1)l_1}$ , queue is nonempty or  $status_2 = \text{disabled}$ .  
earliest time that  $count_2 \rightarrow 0$

3. If queue is nonempty then either  $last(recv) < first(dec) + (count_2 - 1)l_1$ , or  $status_2 = \text{disabled}$ .



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

$\pi = dec.$   $(S, \pi, S') \in \text{trans}_1(\pi)$   $\mathbb{I}$   $1, 2, 3.$   
 $I(S_i)$  decrement  $I(S')$

$$S'.count_2 > 0$$

$$S.count_2 > 0 \quad S.count_2 = 1, \quad S'.count_2 = 0$$

$$2. \Rightarrow S.last(send) + d < S.first(dec)$$

$$3. \Rightarrow S.last(rec) < S.first(dec)$$

or ~~status\_2 disabled~~

$$\Rightarrow \max\{S.last(send), S.last(rec)\} < S.first(dec)$$

$$\Leftarrow S.now \Leftarrow \begin{matrix} S.last(send) \\ \text{or} \\ S.last(rec) \end{matrix} \Leftarrow (\min\{S.last+1, S.dwt\})$$