

# Stochastic Model Checking



UNIVERSITÄT  
DES  
SAARLANDES

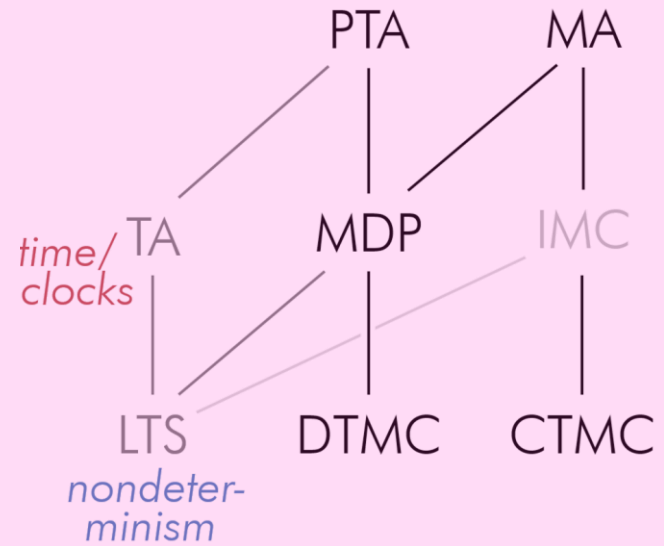
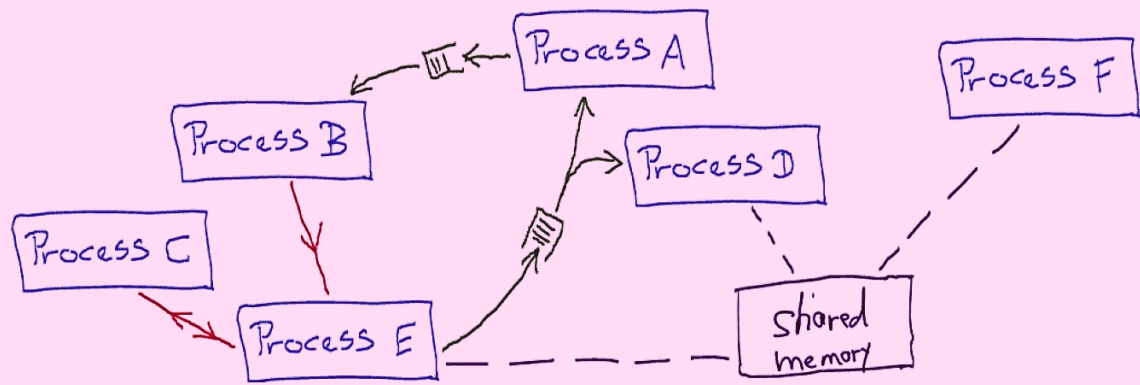
Arnd Hartmanns  
University of Twente – Enschede, the Netherlands

Holger Hermanns  
Saarland University – Saarbrücken, Germany  
Institute of Intelligent Software – Guangzhou, China

# Stochastic Model Checking

## Part One (contd.)

# What Did You See Yesterday?

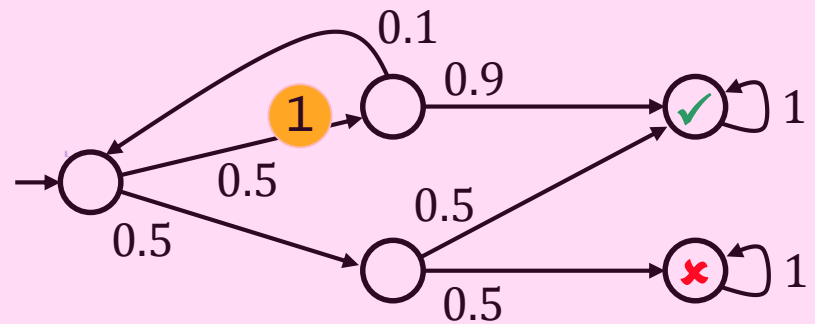


for  $\alpha \notin \text{Syn}$ :

$$\frac{s_1 \xrightarrow{\alpha}_1 s'_1}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s'_1, s_2 \rangle} \quad \frac{s_2 \xrightarrow{\alpha}_2 s'_2}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1, s'_2 \rangle}$$

for  $\alpha \in \text{Syn}$ :

$$\frac{s_1 \xrightarrow{\alpha}_1 s'_1 \wedge s_2 \xrightarrow{\alpha}_2 s'_2}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s'_1, s'_2 \rangle}$$

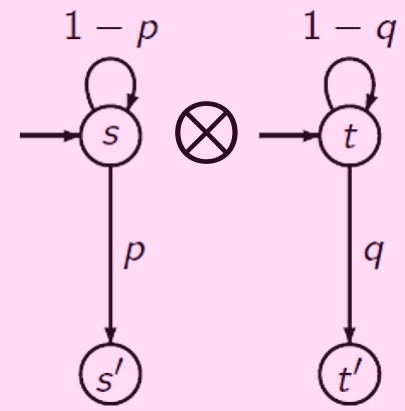


$$V_{\mathbb{E}}(s) = \sum_{s' \in S} P(s, s') \cdot (\text{cost}(s, s') + V_{\mathbb{E}}(s'))$$

# Composition Operators on Markov Chains

Only the synchronous product makes sense.

$$\frac{s_1 \xrightarrow{p} s'_1 \wedge s_2 \xrightarrow{q} s'_2}{\langle s_1, s_2 \rangle \xrightarrow{pq} \langle s'_1, s'_2 \rangle}$$



The MCs proceed in lock-step through discrete time.

What happens to the probabilities?

Synchronous Product

for parallel systems with fully synchronized processes

given TS  $\mathcal{T}_1 = (S_1, \text{Act}_1, \longrightarrow_1, \dots)$ ,  
 $\mathcal{T}_2 = (S_2, \text{Act}_2, \longrightarrow_2, \dots)$

$$\mathcal{T}_1 \otimes \mathcal{T}_2 = (S_1 \times S_2, \text{Act}, \longrightarrow, \dots)$$

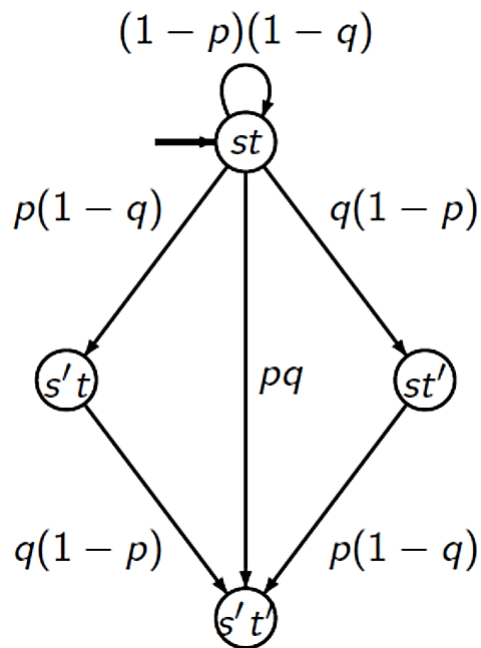
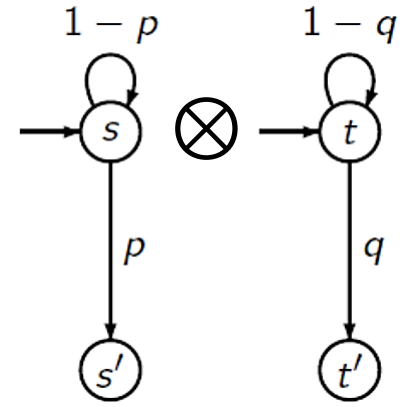
$$\frac{s_1 \xrightarrow{\alpha} s'_1 \wedge s_2 \xrightarrow{\beta} s'_2}{\langle s_1, s_2 \rangle \xrightarrow{\alpha * \beta} \langle s'_1, s'_2 \rangle}$$

$\text{Act}_1 \times \text{Act}_2 \longrightarrow \text{Act}$   
 $(\alpha, \beta) \mapsto \alpha * \beta$

# Composition Operators on Markov Chains

## Synchronous Composition of DTMCs

$$\frac{s_1 \xrightarrow{p} s'_1 \quad \wedge \quad s_2 \xrightarrow{q} s'_2}{\langle s_1, s_2 \rangle \xrightarrow{pq} \langle s'_1, s'_2 \rangle}$$



Synchronous Product

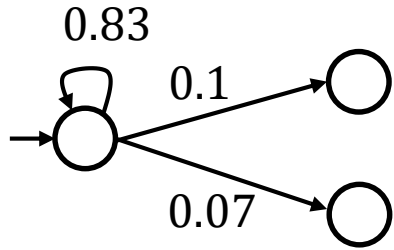
for parallel systems with fully synchronized processes

given TS  $\mathcal{T}_1 = (S_1, \text{Act}_1, \xrightarrow{1}, \dots)$ ,  
 $\mathcal{T}_2 = (S_2, \text{Act}_2, \xrightarrow{2}, \dots)$

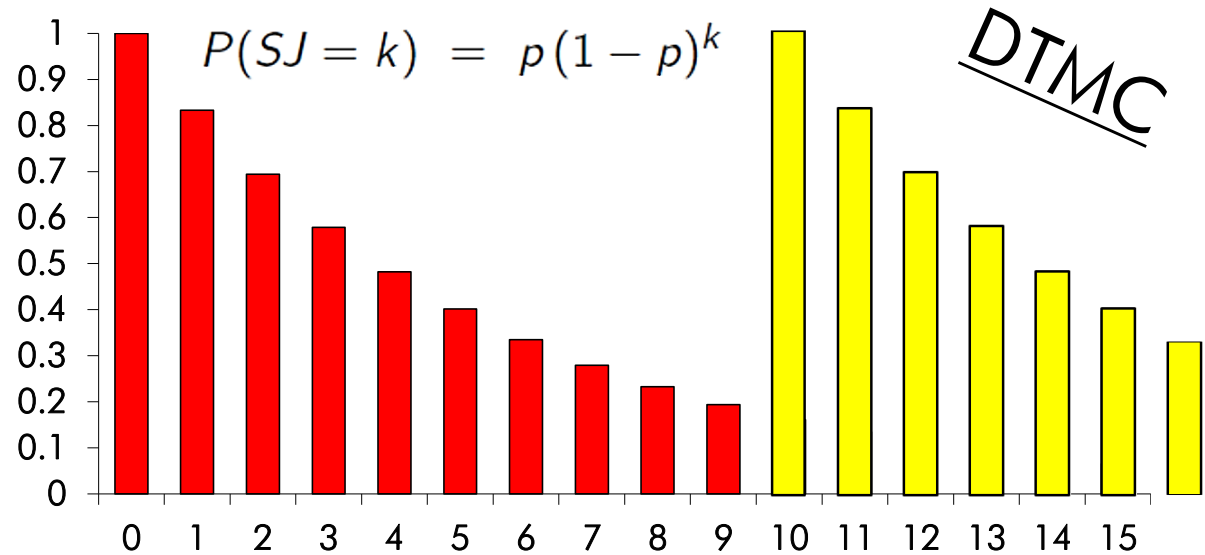
$$\mathcal{T}_1 \otimes \mathcal{T}_2 = (S_1 \times S_2, \text{Act}, \xrightarrow{\cdot}, \dots)$$

$$\frac{s_1 \xrightarrow{\alpha} s'_1 \quad \wedge \quad s_2 \xrightarrow{\beta} s'_2}{\langle s_1, s_2 \rangle \xrightarrow{\alpha * \beta} \langle s'_1, s'_2 \rangle} \quad \text{Act}_1 \times \text{Act}_2 \xrightarrow{(\alpha, \beta)} \text{Act}$$

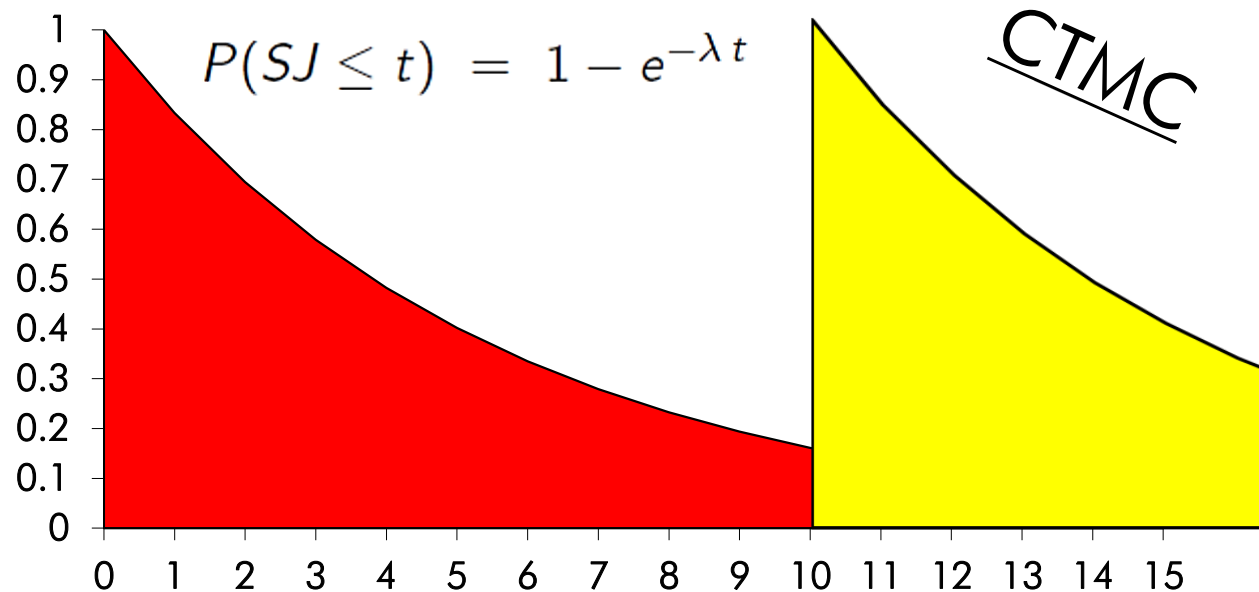
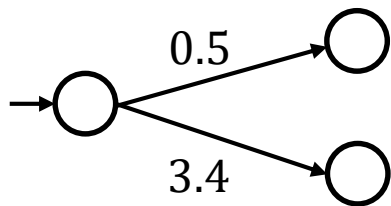
# Markov Chains in Discrete Time – and Beyond



Sojourn time distributions are geometric.



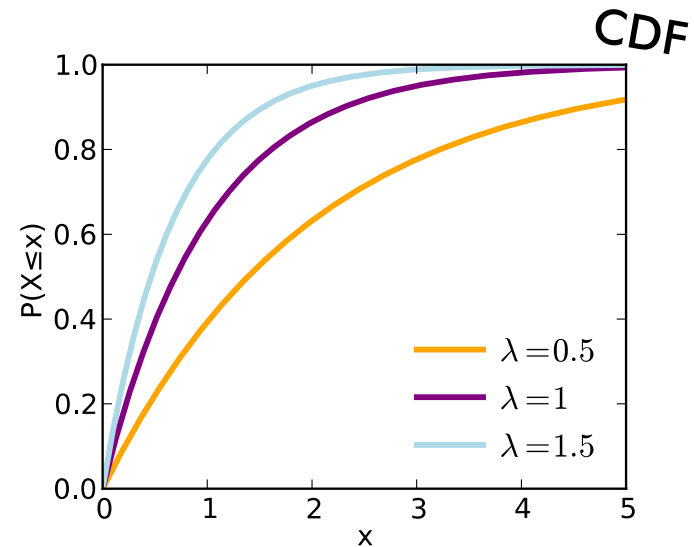
Sojourn time distributions are exponential.



# Continuous-Time Markov Chains

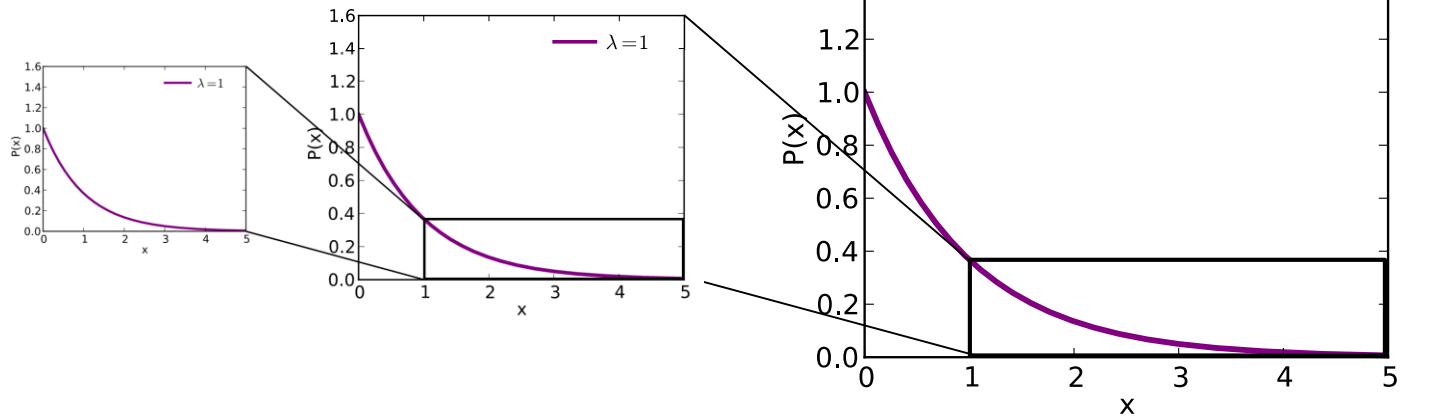
## The exponential distribution

- continuous, parameter: rate  $\lambda$
- mean:  $1/\lambda$
- CDF:  $F(x) = 1 - e^{-\lambda x}$

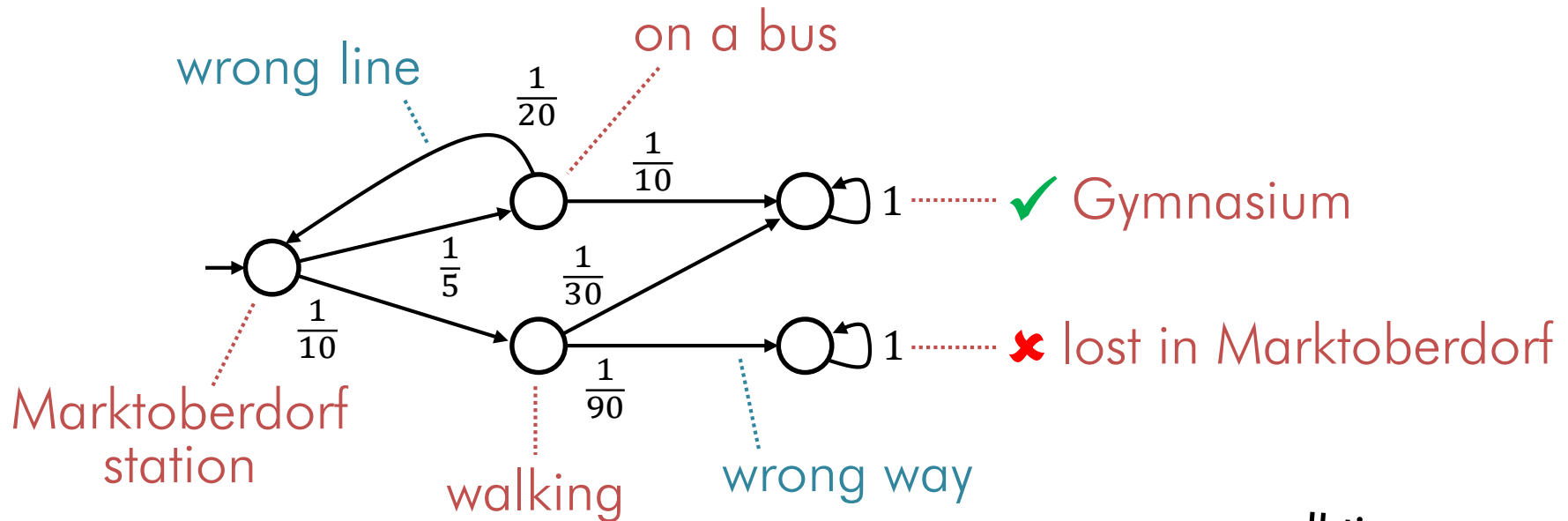


Memoryless property:

$$\mathbb{P}(X > x + t \mid X > x) = \mathbb{P}(X > t)$$



## Continuous-time Markov chains



Marktoberdorf station:

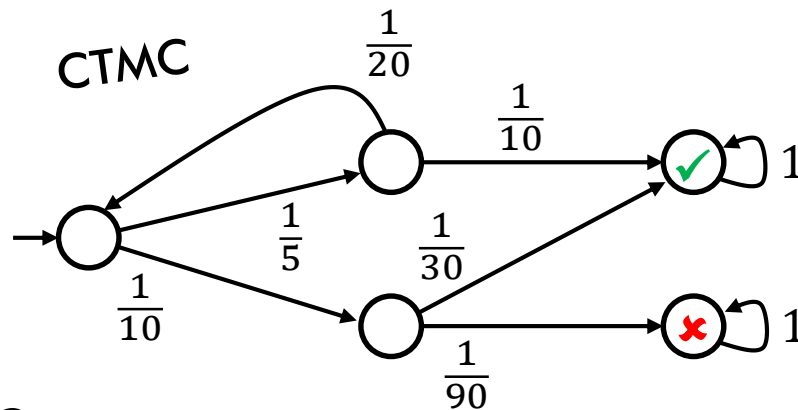
a bus every 5 minutes } race: bus comes } exit rate  $\frac{3}{10}$ :  
walk after 10 minutes } or decide to walk } stay  $3.\bar{3}$  min

⇒ race between  $\text{Exp}(\lambda)$  and  $\text{Exp}(\mu)$  follows  $\text{Exp}(\lambda + \mu)$

*all times are  
expected times!*

# Markov Chains

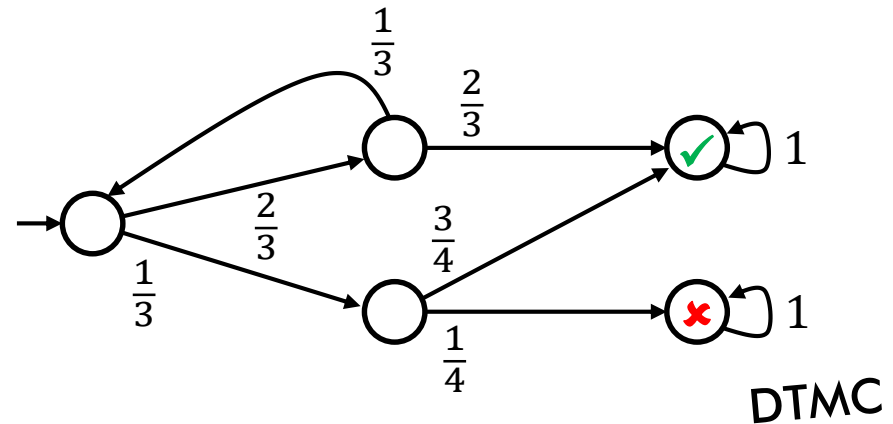
## Continuous-time Markov chains



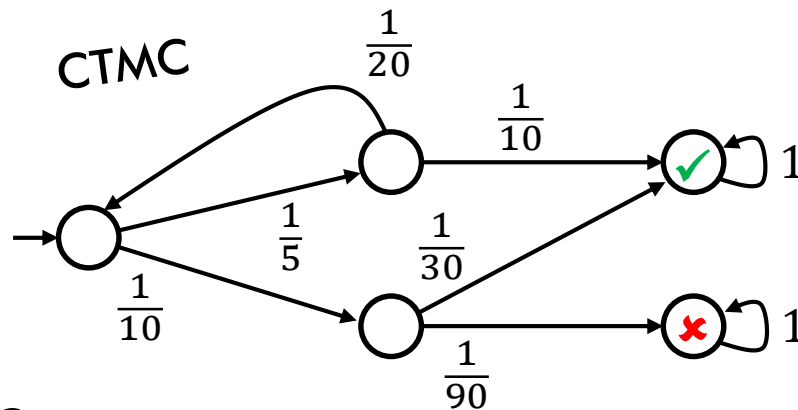
Probabilities:  
*normalised rates*

$\mathbb{P}(\diamond \checkmark)$ ?

⇒ check the  
embedded DTMC:



## Continuous-time Markov chains



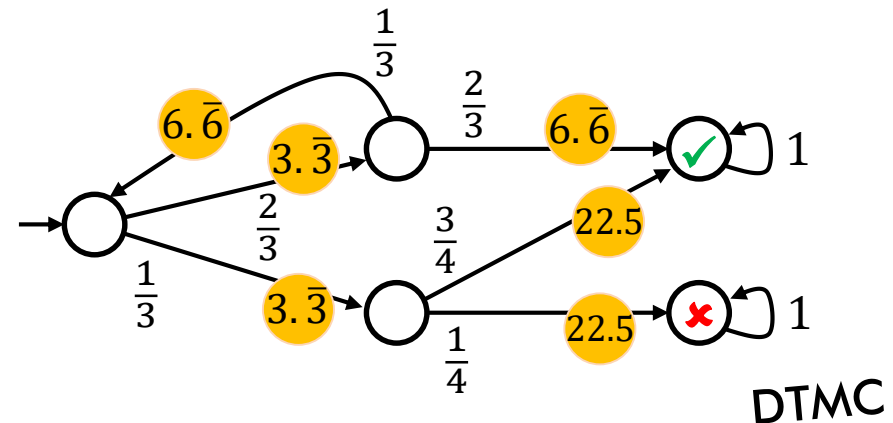
Probabilities:  
normalised rates

Costs for time:  
Sojourn time  
expectations  
per state

$$\mathbb{P}(\diamond \checkmark)?$$

$$\mathbb{E}(\text{🕒 to } \checkmark \vee \text{✗})?$$

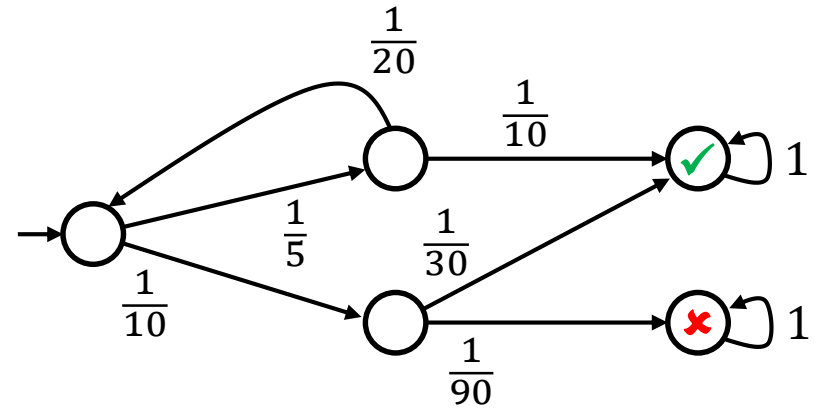
⇒ check the  
embedded DTMC:



# Markov Chains

## CTMC in Modest

```
property ETime =  
  Xmax(T, lost || arrived);  
  
do {  
  :: rate(1/5) tau;  
  alt {  
    :: rate(1/20) tau  
    :: rate(1/10) {= arrived = true =}; stop  
  }  
  :: rate(1/10) tau;  
  alt {  
    :: rate(1/30) tau {= arrived = true =}  
    :: rate(1/90) {= lost = true =}  
  }; stop  
}
```



⇒ Try it with  
mosta and  
mcsta!

# A bit of (branching-time) logic – CSL

“steady-state probability mass”

The probability mass

flowing along  $\phi$ -paths  
is a value in the interval  $J$ .

The long-run fraction of time  
spent in  $\Phi$ -states

is a value in the interval  $J$ .

State formulas:

$$\Phi := \text{true} \mid a \mid \Phi_1 \wedge \Phi_2 \mid \neg\Phi \mid \mathbb{P}_J(\phi) \mid \mathbb{L}_J(\Phi)$$

where  $a \in AP$ ,  $J \subseteq [0, 1]$  is an interval with rational bounds.

within a duration  
from time interval  $I$ .

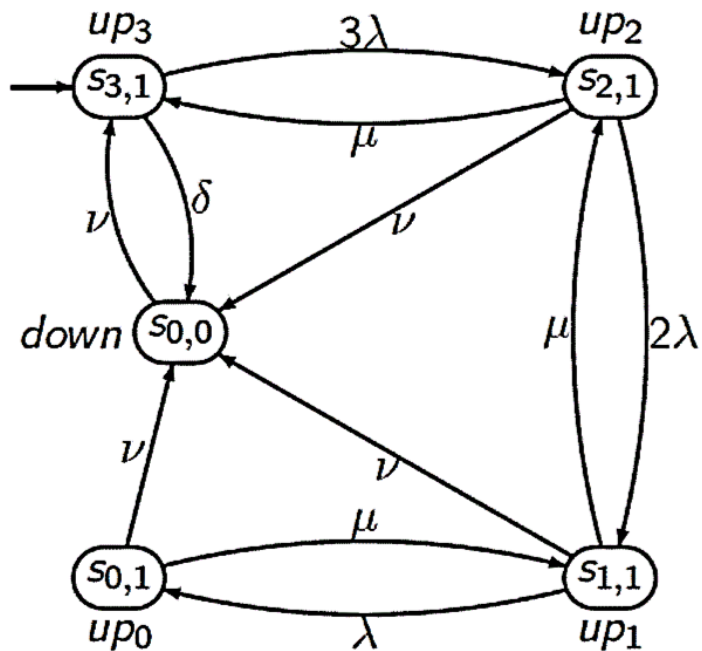
Path formulas:

$$\phi := \mathcal{X}^I\phi \mid \Phi_1 \mathcal{U}^I\Phi_2$$

where

$I \subseteq \mathbb{R}^{\geq 0}$  denotes an interval.

# A Triple-Modular Redundant System



- In the steady state, the probability that the system is in state  $s_{2,1}$  is at most  $p$ ,
- The transient probability at time  $t$  in state  $s'$  meets the bound  $> p$ ,
- The probability of reaching *down* state within 10 time units after having continuously operated with at least two processors is at most 0.01
- In steady state, with probability at least 0.9, the probability that the system will not go down within 10 time units is at least 0.8

- $\mathbb{L}_J(up)$ : steady-state availability
- $\mathbb{P}_J(\diamond^{[t,t]} up)$ : instantaneous availability at time  $t$
- $\mathbb{P}_J(\Phi \mathcal{U}^{[t,t]} up)$ : conditional instantaneous availability at time  $t$
- $\mathbb{P}_J(\square^{[t,t']} up)$ : interval availability,
- $\mathbb{L}_J(\mathbb{P}_J(\square^{[t,t']}))$ : steady-state interval availability
- $\mathbb{P}_J(\Phi \mathcal{U}^{[t,t']} \mathbb{L}_J(up))$ : conditional time-bounded steady-state availability

# CSL Model Checking – Numerical algorithm

- Can all be cast into fixpoint computations that juggle with matrices and vectors.
- Polynomial in size of model (cubic in practice).
- Linear in length of formula.
- Linear in largest rate occurring.
- Linear in largest interval bound occurring.

# Exponential Distributions – Unleashed

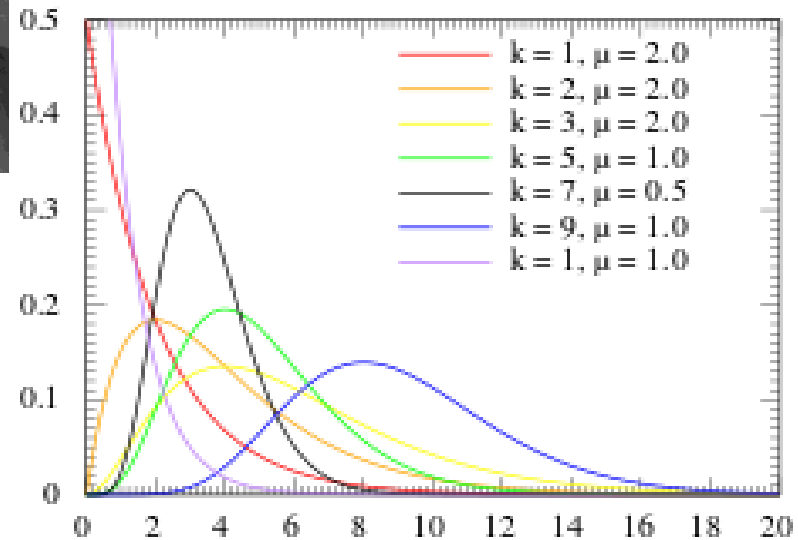
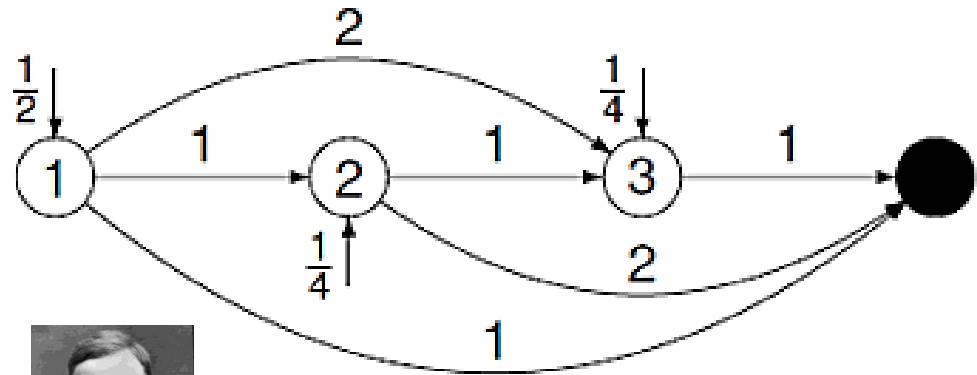
- Absorption time distribution in an absorbing CTMC

- Topologically dense

- Can approximate arbitrary distributions with arbitrary precision

- Effective fitting tools available

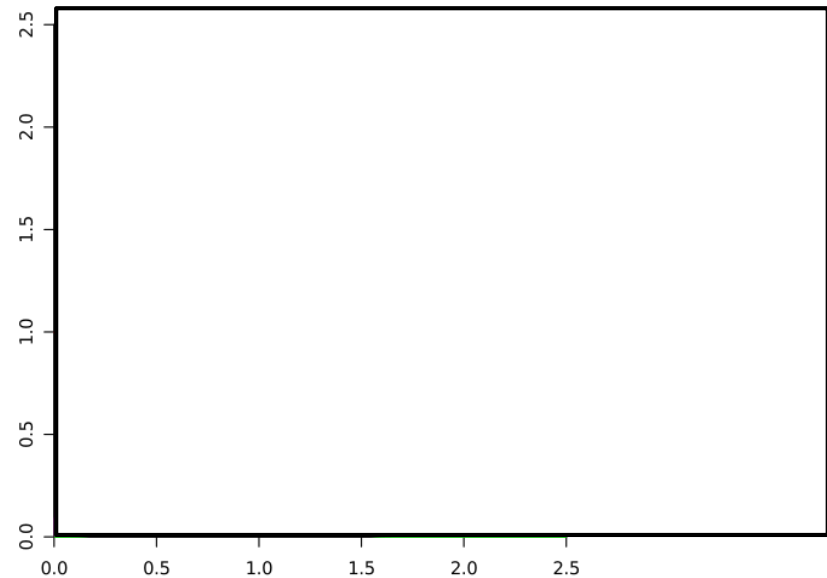
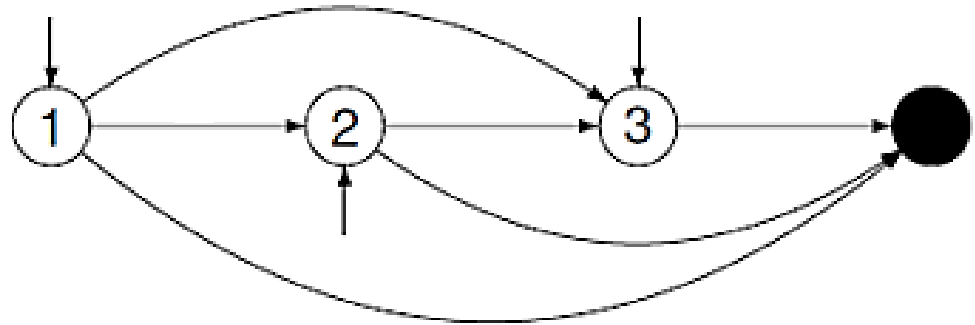
- “Phase-type Distributions”



- Closed under maximum, minimum, convolution

# What This Means

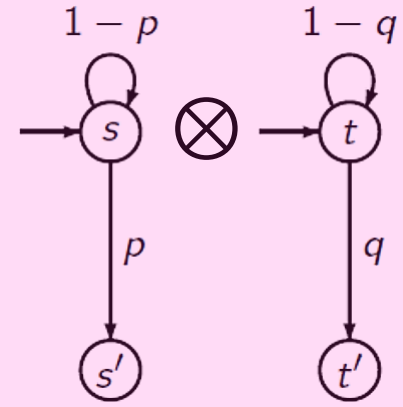
- Absorption time distribution in an absorbing CTMC
- Topologically dense
- Can approximate arbitrary distributions with arbitrary precision
- Effective fitting tools available
- “Phase-type Distributions”
- Closed under maximum, minimum, convolution



# Composition Operators on Discrete-Time Markov Chains

Only the synchronous product makes sense.

$$\frac{s_1 \xrightarrow{p} s'_1 \wedge s_2 \xrightarrow{q} s'_2}{\langle s_1, s_2 \rangle \xrightarrow{pq} \langle s'_1, s'_2 \rangle}$$



The MCs proceed in lock-step through discrete time.

What happens to the probabilities?

Synchronous Product

for parallel systems with fully synchronized processes

given TS  $\mathcal{T}_1 = (S_1, \text{Act}_1, \longrightarrow_1, \dots)$ ,  
 $\mathcal{T}_2 = (S_2, \text{Act}_2, \longrightarrow_2, \dots)$

$$\mathcal{T}_1 \otimes \mathcal{T}_2 = (S_1 \times S_2, \text{Act}, \longrightarrow, \dots)$$

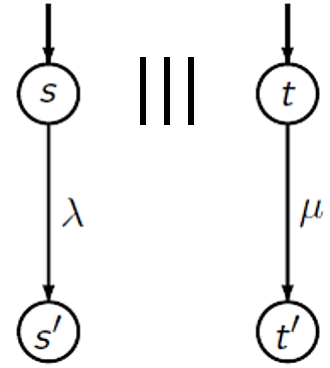
$$\frac{s_1 \xrightarrow{\alpha} s'_1 \wedge s_2 \xrightarrow{\beta} s'_2}{\langle s_1, s_2 \rangle \xrightarrow{\alpha * \beta} \langle s'_1, s'_2 \rangle}$$

$$\text{Act}_1 \times \text{Act}_2 \longrightarrow \text{Act}$$

$$(\alpha, \beta) \mapsto \alpha * \beta$$

# Composition of Continuous-Time Markov Chains

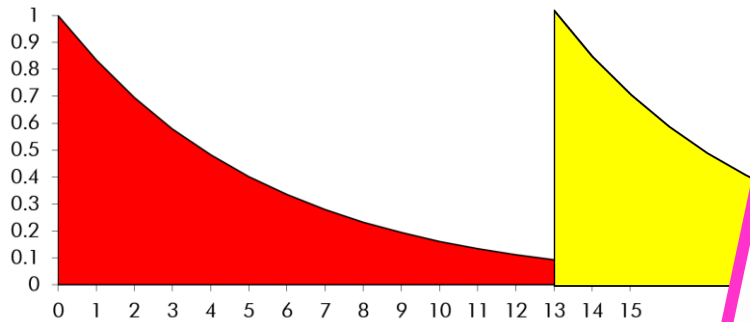
Only the interleaving operator makes sense.



$$\frac{s_1 \xrightarrow{\lambda} s'_1}{\langle s_1, s_2 \rangle \xrightarrow{\lambda} \langle s'_1, s_2 \rangle}$$

$$\frac{s_2 \xrightarrow{\mu} s'_2}{\langle s_1, s_2 \rangle \xrightarrow{\mu} \langle s_1, s'_2 \rangle}$$

The MCs proceed in independently through continuous time.



What happens to the rates?

Concurrency – Nondeterminism – Interleaving

$$\mathcal{T}_1 = (s_1, Act_1, \rightarrow_1, s_{0,1})$$

$$\mathcal{T}_2 = (s_2, Act_2, \rightarrow_2, s_{0,2})$$

$$\mathcal{T}_1 ||| \mathcal{T}_2 = (s_1 \times s_2, Act_1 \cup Act_2, \rightarrow, s_{0,1} \times s_{0,2})$$

where the transition relation  $\rightarrow$  is given by:

$$\frac{s_1 \xrightarrow{\alpha} s'_1}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s'_1, s_2 \rangle}$$

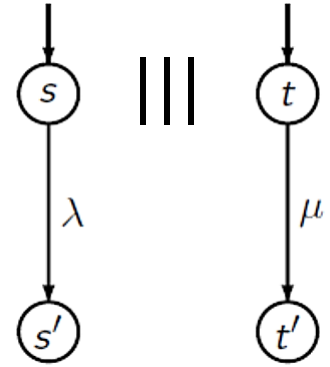
only  $\mathcal{T}_1$  moves

$$\frac{s_2 \xrightarrow{\alpha} s'_2}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1, s'_2 \rangle}$$

only  $\mathcal{T}_2$  moves

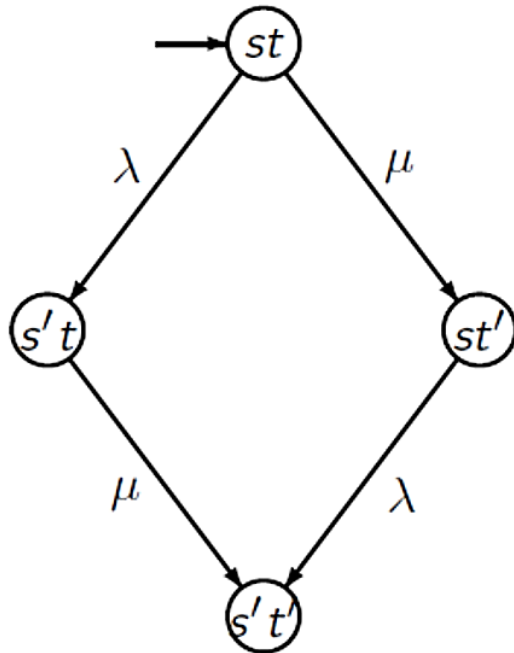
# Composition of Continuous-Time Markov Chains

Only the interleaving operator makes sense.



$$\frac{s_1 \xrightarrow{\lambda} s'_1}{\langle s_1, s_2 \rangle \xrightarrow{\lambda} \langle s'_1, s_2 \rangle}$$

$$\frac{s_2 \xrightarrow{\mu} s'_2}{\langle s_1, s_2 \rangle \xrightarrow{\mu} \langle s_1, s'_2 \rangle}$$



Concurrency – Nondeterminism – Interleaving

$$\mathcal{T}_1 = (S_1, Act_1, \xrightarrow{\cdot}_1, S_{0,1})$$

$$\mathcal{T}_2 = (S_2, Act_2, \xrightarrow{\cdot}_2, S_{0,2})$$

$$\mathcal{T}_1 ||| \mathcal{T}_2 = (S_1 \times S_2, Act_1 \cup Act_2, \xrightarrow{\cdot}, S_{0,1} \times S_{0,2})$$

where the transition relation  $\xrightarrow{\cdot}$  is given by:

$$\frac{s_1 \xrightarrow{\alpha}_1 s'_1}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s'_1, s_2 \rangle}$$

only  $\mathcal{T}_1$  moves

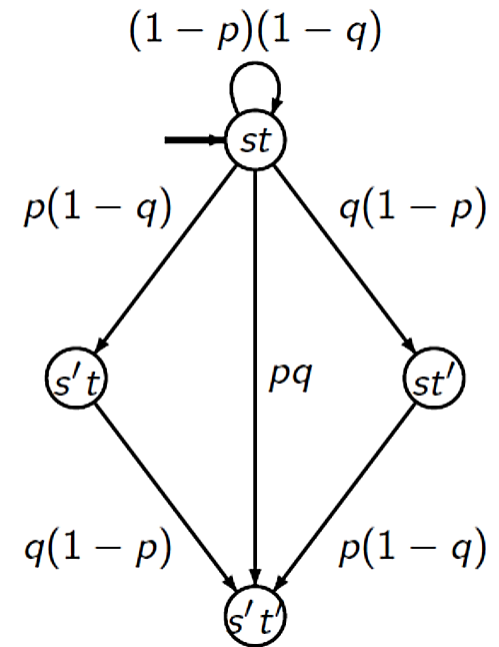
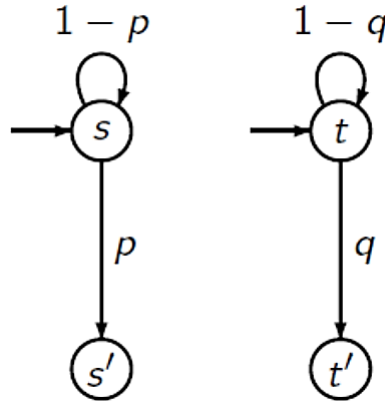
$$\frac{s_2 \xrightarrow{\alpha}_2 s'_2}{\langle s_1, s_2 \rangle \xrightarrow{\alpha} \langle s_1, s'_2 \rangle}$$

only  $\mathcal{T}_2$  moves

# Comparing CT-Interleaving with DT-synchrony

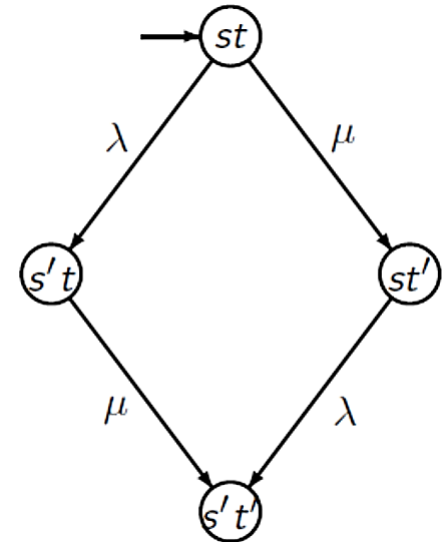
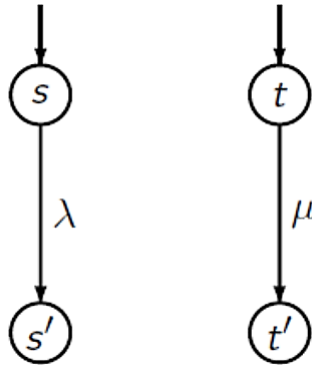
## Synchronous Composition of DTMCs

$\mathcal{D} \otimes \mathcal{D}'$



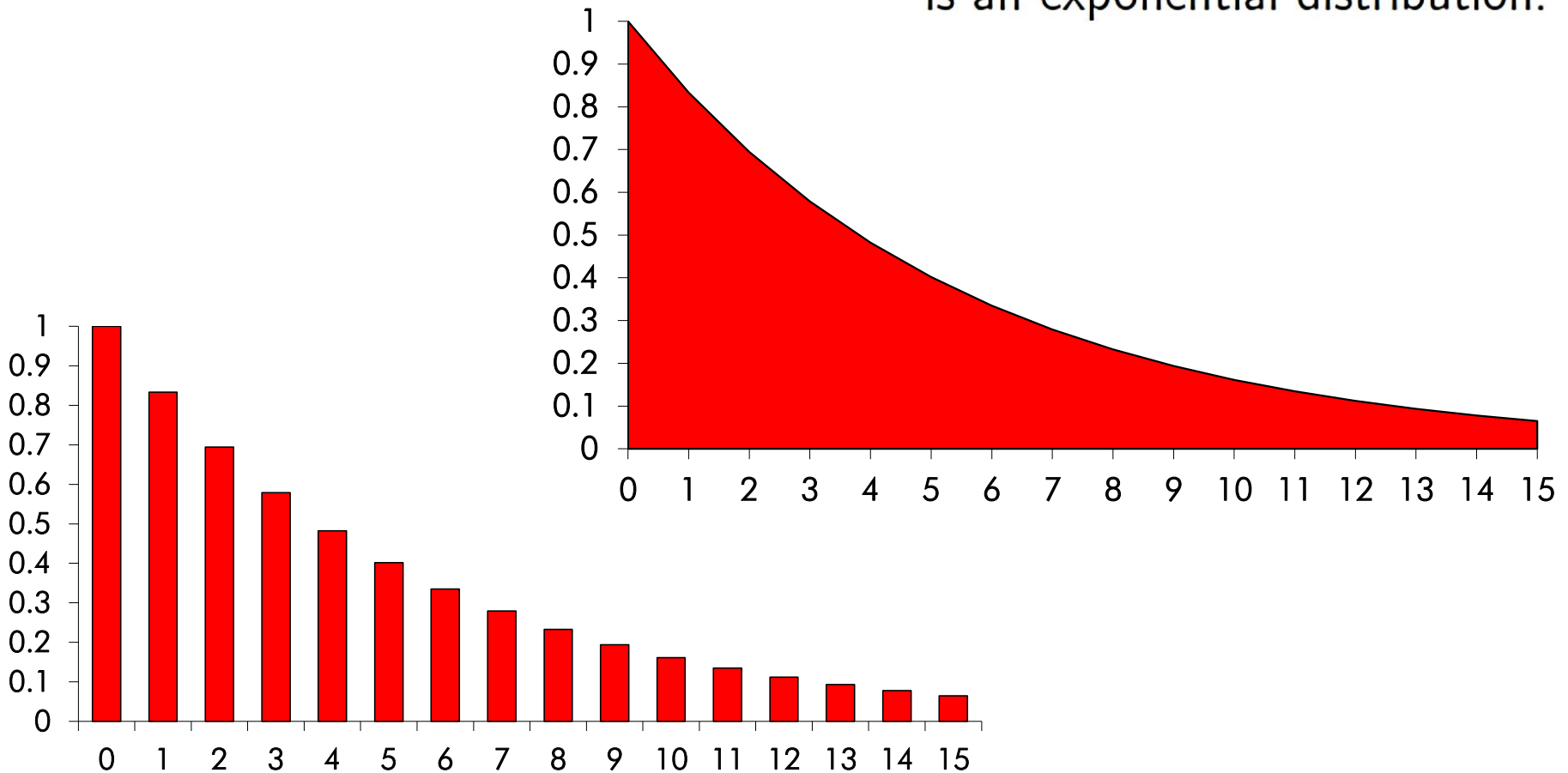
## Interleaving of CTMCs

$\mathcal{M} ||| \mathcal{M}'$



# Connecting CT-Interleaving with DT-synchrony

- For a given time step  $\Delta$  a discretised exponential distribution is a geometric distribution.
- In the limit  $\Delta \rightarrow 0$  a geometric distribution is an exponential distribution.



# Connecting CT-Interleaving with DT-synchrony

- For a given time step  $\Delta$  a discretised exponential distribution is a geometric distribution.
- In the limit  $\Delta \rightarrow 0$  a geometric distribution is an exponential distribution.
- This can be lifted to MCs:  
For each CTMC  $\mathcal{M}$  and time step  $\Delta$ , there is discretised DTMC  $\mathcal{D}_\Delta$ .

*Let*

- $\mathcal{M}$  and  $\mathcal{M}'$  be two CTMCs,
- $\mathcal{D}_\Delta, \mathcal{D}'_\Delta$  be the corresponding discretised DTMCs for time step  $\Delta$ ,

then:

$$\lim_{\Delta \rightarrow 0} (\mathcal{D}_\Delta \otimes \mathcal{D}'_\Delta) = \mathcal{M} ||| \mathcal{M}'$$

# Where We Stand

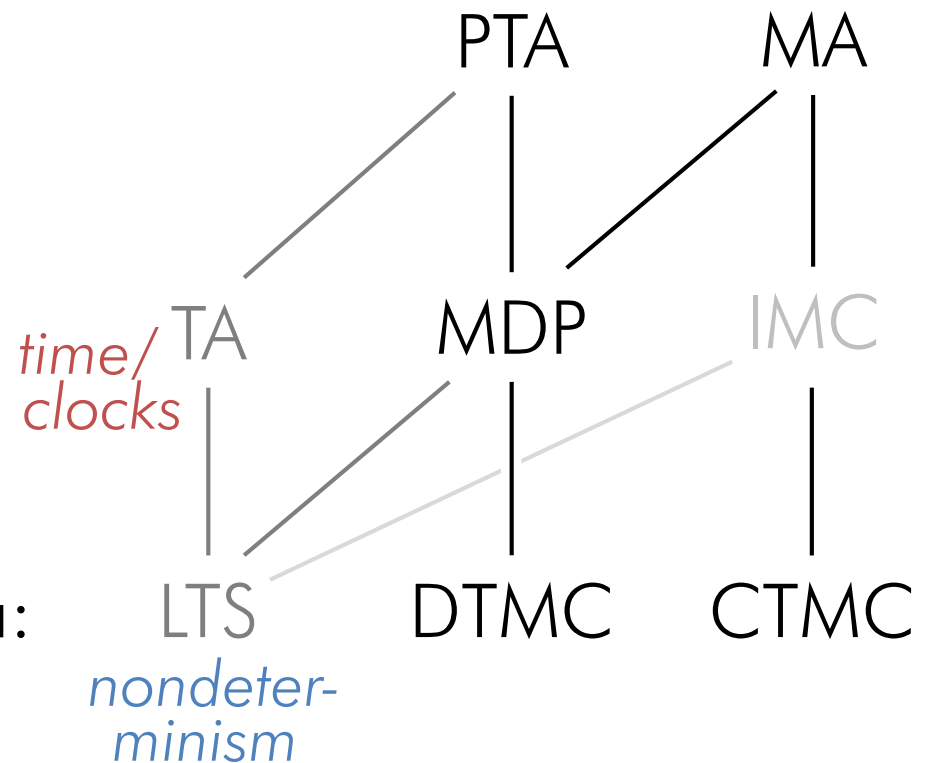
Discrete-time Markov chains:  
discrete probabilistic choices

Continuous-time Markov chains:  
continuous stochastic time

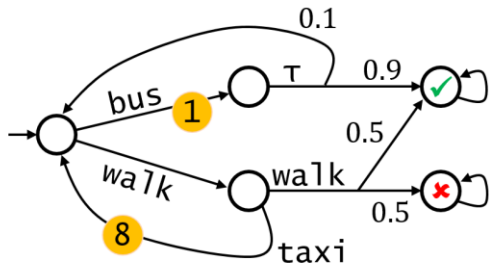
Markov decision processes:  
decisions and uncertainty

Markov automata:  
MDP plus CTMC,  
compositionally

Probabilistic timed automata:  
MDP plus hard real time



# Markov Decision Processes

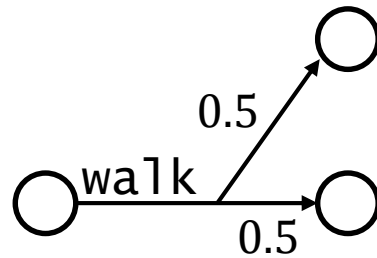


$$\max_{a \in A} \sum_{\mu \in T(s, a)} \mu(s') \cdot V_{\mathbb{P}}^{i-1}(s')$$

# Markov Decision Processes

The main difference:  $\longrightarrow \subseteq S \times \text{Act} \times \text{Distr}(S)$

Probability distributions over states.



## Concurrency Modelling Primer

Labelled transition systems:

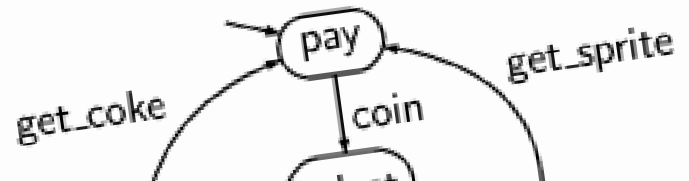
states  $S$

actions  $\text{Act}$

transitions  $\longrightarrow \subseteq S \times \text{Act} \times S$

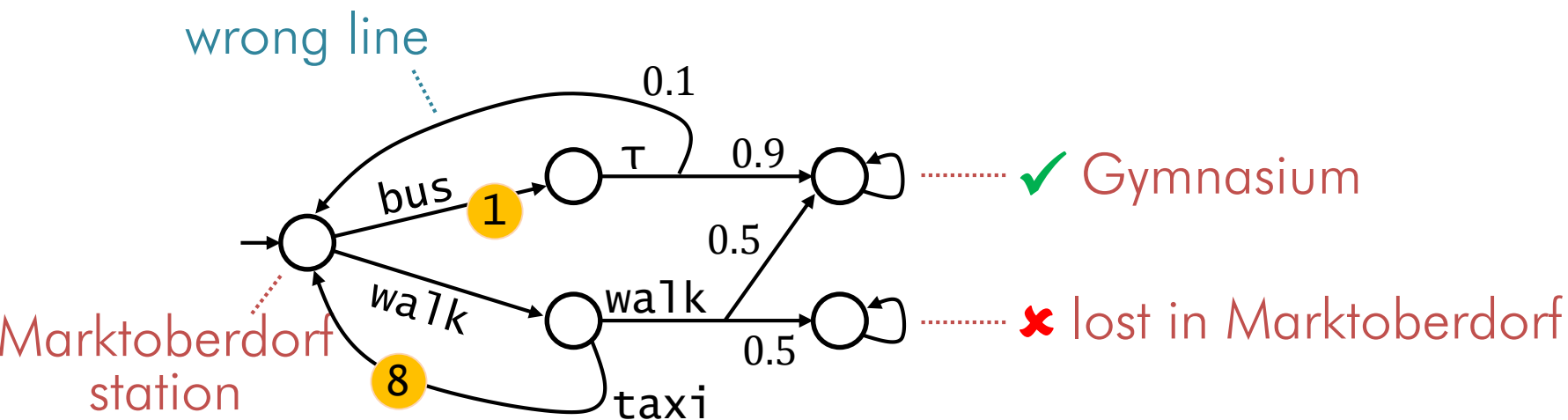
initial state (set)

actions:  
coin,  
 $\tau$   
get\_sprite,  
get\_coke



# Markov Decision Processes

## Decision making under uncertainty



Two decisions: **bus** or **walk**, **walk** or **taxi**

The *outcome* of (some) choices is probabilistic

$$\mathbb{P}(\diamond \checkmark) = ?$$

$$\mathbb{E}(\text{cost to } \checkmark \vee \times) = ?$$

results depend  
on decisions!

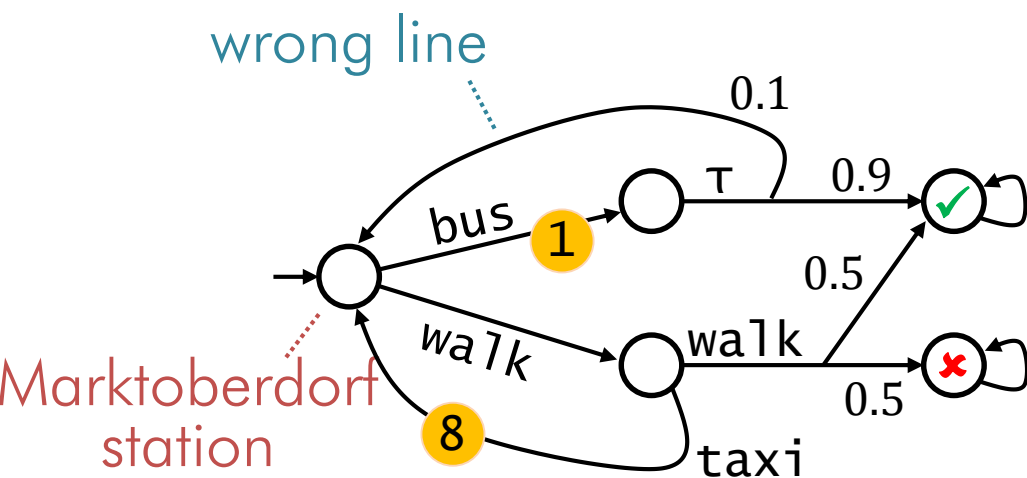


$$\begin{array}{l} \mathbb{P}_{\min}, \mathbb{P}_{\max}, \\ \mathbb{E}_{\min}, \mathbb{E}_{\max} \end{array}$$

*optimisation  
problem*

# Markov Decision Processes

## Computing values in MDP

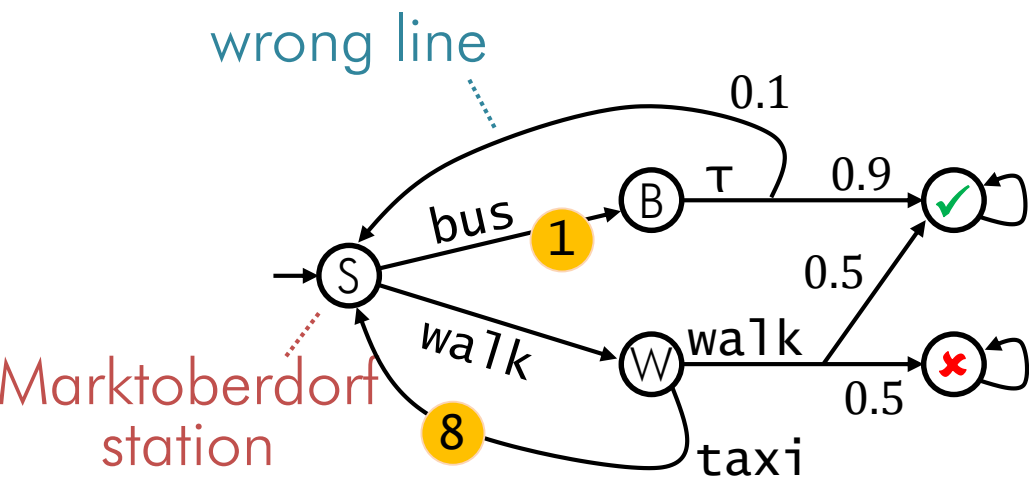


$$\mathbb{P}_{\max}(\diamond \checkmark) = ? \quad V_{\mathbb{P}}(s) = \max_{a \in A} \sum_{\mu \in T(s,a)} \underbrace{\mu(s')}_{\text{sum over } a\text{'s targets...}} \cdot \underbrace{V_{\mathbb{P}}(s')}_{\text{...of weighted target values}} \quad (1 \text{ if target})$$

maximum over all actions  $a$       sum over  $a$ 's targets...      ...of weighted target values

# Markov Decision Processes

## Value iteration: dynamic programming



	S	B	W	✓	✗
$V_{\mathbb{P}}^0$	0	0	0	1	0
$V_{\mathbb{P}}^1$	0	0.9	0.5	1	0
$V_{\mathbb{P}}^2$	0.9	0.9	0.5	1	0
$V_{\mathbb{P}}^3$	0.9	0.99	0.9	1	0
$V_{\mathbb{P}}^4$	0.99	0.99	0.9	1	0

...

$$\mathbb{P}_{\max}(\diamond \checkmark) = ?$$

Bellman equation for MDP ( $\mathbb{P}$ )

$$V_{\mathbb{P}}^i(s) = \max_{a \in A} \underbrace{\sum_{\mu \in T(s,a)} \mu(s')}_{\text{sum over } a\text{'s targets...}} \cdot \underbrace{V_{\mathbb{P}}^{i-1}(s')}_{\text{...of weighted target values}}$$

maximum over all actions  $a$       sum over  $a$ 's targets...      ...of weighted target values