

# 7. Probabilities: Probabilistic LTS and Statistical Model Checking

---

José Proença

System Verification (CC4084) 2025/2026

CISTER – U.Porto, Porto, Portugal

<https://fm-dcc.github.io/sv2526>



**CISTER** - Research Centre in  
Real-Time & Embedded  
Computing Systems

**Where we are**

---

- Introduction to model-checking
- CCS: a simple language for concurrency
  - Syntax
  - Semantics
  - Equivalence
  - mCRL2: modelling
- Dynamic logic
  - Syntax
  - Semantics
  - Relation with equivalence
  - mCRL2: verification
- Timed Automata
  - Syntax
  - Semantics (composition, Zeno)
  - Equivalence
  - UPPAAL: modelling
- Temporal logics (LTL/CTL)
  - Syntax
  - Semantics
  - UPPAAL: verification
- Probabilistic and stochastic systems
  - Going probabilistic
  - UPPAAL: monte-carlo

## Going probabilistic

---

## Systems can get very complex

- E.g., 5 components, 3 possible traces each
- No communication (pure interleaving)
- Many permutations

## Systems can get very complex

- E.g., 5 components, 3 possible traces each
- No communication (pure interleaving)
- Many permutations
- More components, more traces – untreatable

## Systems can get very complex

- E.g., 5 components, 3 possible traces each
- No communication (pure interleaving)
- Many permutations
- More components, more traces – untreatable
- Verifying deadlock freedom (and others) requires traversing all states
- **Approximation:**
  - traverse only part of the states
  - give more **priority** to some actions
  - return (statistically) likelihood of a given property

- $\alpha : S \rightarrow N \times S$  Moore machine
- $\alpha : S \rightarrow \text{Bool} \times S^N$  deterministic automata
- $\alpha : S \rightarrow \text{Bool} \times P(S)^N$  non-deterministic automata (reactive)
- $\alpha : S \rightarrow P(N \times S)$  non deterministic LTS (generative)
- $\alpha : S \rightarrow (S + 1)^N$  partial deterministic LTS
- $\alpha : S \rightarrow P(S)$  unlabelled TS
- $\alpha : S \rightarrow D(S)$  Markov chain



## Markov chains

$$\alpha : S \rightarrow D(S)$$

where  $D(S)$  is the set of all **discrete probability distributions** on set  $S$

A Markov chain goes from a state  $s$  to a state  $s'$  with probability  $p$  if

$$\alpha(s) = \mu \quad \text{with} \quad \mu(s') = p > 0$$

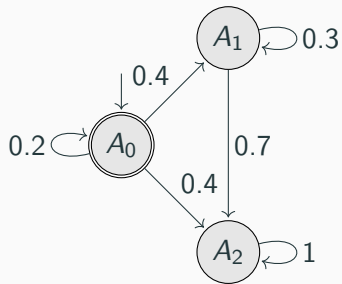
## Recall

$\mu : S \rightarrow [0, 1]$  is a **discrete probability distribution** if

- $\{s \in S \mid \mu(s) > 0\}$ , is finite (called the **support** of  $\mu$ ), and
- $\sum_{s \in S} \mu(s) = 1$

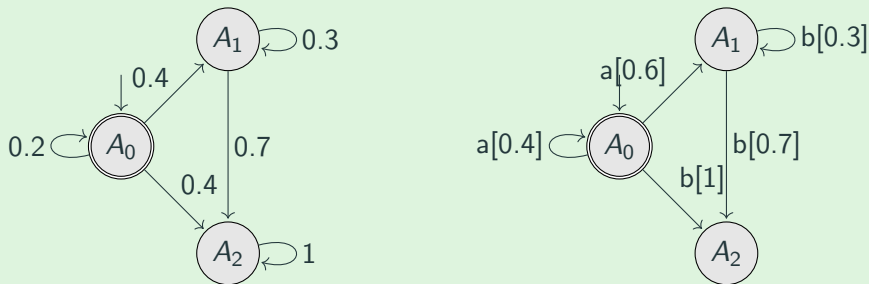
## Examples

- **Dirac distribution:**  $\mu_s^1 = \{s \rightarrow 1\}$
- **Product distribution:**  $(\mu_1 \times \mu_2)\langle s, t \rangle = \mu_1(s) \times \mu_2(t)$



$$\alpha : S \rightarrow (D(S) + 1)^N$$

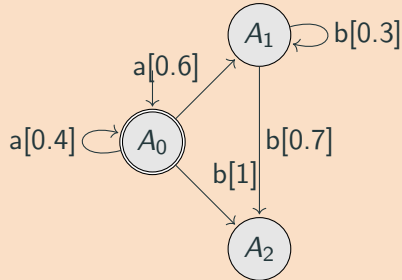
**Ex. 7.1: Formalise the system below on the right as a function**



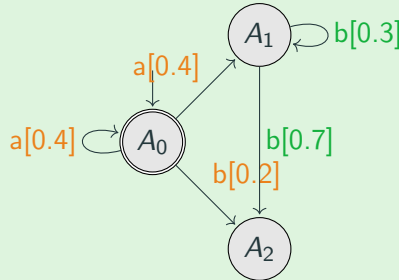
Notions of bisimulation arise naturally.

$$\alpha : S \rightarrow D(S \times N) + 1$$

Before (reactive)



Ex. 7.2: Now (generative) – formalise it



$$\alpha : S \rightarrow D(S \times N) + 1$$

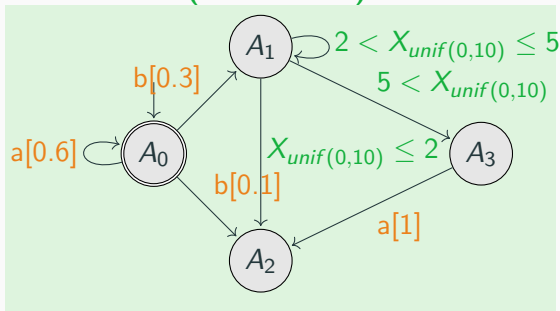
$$\alpha : S \rightarrow D(S \times N) + 1$$

$$\alpha : S \rightarrow D(S \times N) + D_{cont}(\mathcal{R}_0^+ \times S)$$

## Notes

- Continuous time: continuous distribution
- Probabilities both at
  - discrete transitions and
  - continuous delays

## Ex. 7.3: Now (Timed PTS)

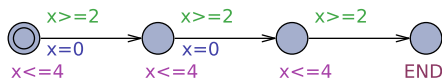


## Probabilities in Uppaal

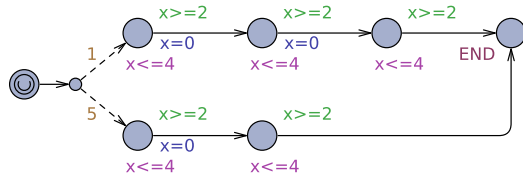
---



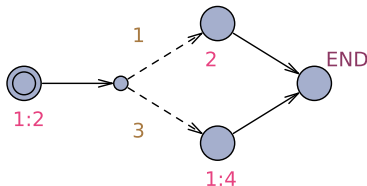
A1



A2



A3



$$\langle L, L_0, \text{Act}, C, \text{Tr}, \text{Inv} \rangle$$

where

- $L$  is a set of **locations**, and  $L_0 \subseteq L$  the set of **initial** locations
- $\text{Act}$  is a set of **actions** and  $C$  a set of **clocks**
- $\text{Tr} \subseteq L \times (\mathcal{C}(C) \cup \mathbb{N}) \times \text{Act} \times \mathcal{P}(C) \times L$  is the **transition relation**

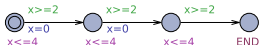
$$\ell_1 \xrightarrow{g, a, U} \ell_2 \qquad \text{or} \qquad \ell_1 \xrightarrow{w, a, U} \ell_2$$

denotes a transition from location  $\ell_1$  to  $\ell_2$ , **labelled** by  $a$ , enabled if **guard**  $g$  is valid, which, when performed, **resets** the set  $U$  of **clocks**, **with a probability given by the weight**  $w$

- $\text{Inv} : L \longrightarrow \mathcal{C}(C) + \mathbb{Q}$  is the assignment of **invariants or rates** (of an **exponential distribution**) to locations

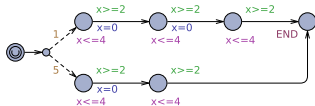
where  $\mathcal{C}(C)$  denotes the set of clock constraints over a set  $C$  of clock variables

## A1

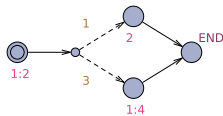


- Probability of  $\langle A1_0, \bar{0} \rangle \xrightarrow{0.5} \langle A1_0, \bar{0.5} \rangle$ ?

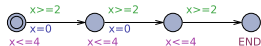
## A2



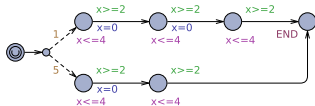
## A3



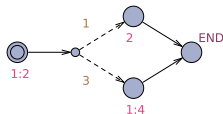
## A1



## A2

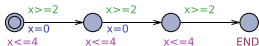


## A3

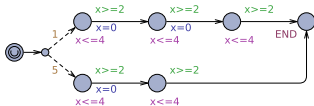


- Probability of  $\langle A1_0, \bar{0} \rangle \xrightarrow{0.5} \langle A1_0, \bar{0.5} \rangle$ ?
- Probability of reaching  $A1_1$  within 1?

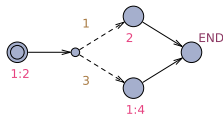
## A1



## A2

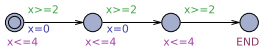


## A3

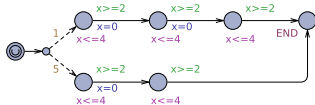


- Probability of  $\langle A1_0, \bar{0} \rangle \xrightarrow{0.5} \langle A1_0, \bar{0.5} \rangle$ ?
- Probability of reaching  $A1_1$  within 1?
- Probability of reaching  $A1_1$  within 5?

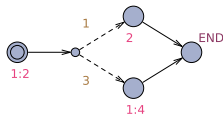
## A1



## A2

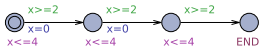


## A3

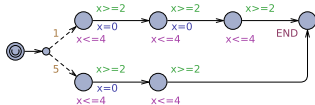


- Probability of  $\langle A1_0, \bar{0} \rangle \xrightarrow{0.5} \langle A1_0, \overline{0.5} \rangle$ ?
- Probability of reaching  $A1_1$  within 1?
- Probability of reaching  $A1_1$  within 5?
- Probability of reaching  $A2_1$  (above) within 5?

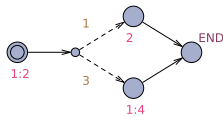
## A1



## A2

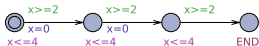


## A3

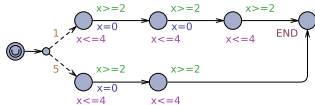


- Probability of  $\langle A1_0, \bar{0} \rangle \xrightarrow{0.5} \langle A1_0, \overline{0.5} \rangle$ ?
- Probability of reaching  $A1_1$  within 1?
- Probability of reaching  $A1_1$  within 5?
- Probability of reaching  $A2_1$  (above) within 5?
- Expected time to reach  $A1_1$ ?

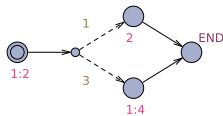
## A1



## A2



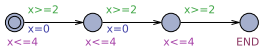
## A3



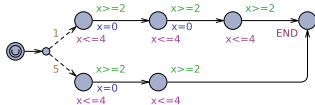
- Probability of  $\langle A1_0, \bar{0} \rangle \xrightarrow{0.5} \langle A1_0, \overline{0.5} \rangle$ ?
- Probability of reaching  $A1_1$  within 1?
- Probability of reaching  $A1_1$  within 5?
- Probability of reaching  $A2_1$  (above) within 5?
- Expected time to reach  $A1_1$ ?
- Expected time to reach  $A3_1$  or  $A3_2$ ?



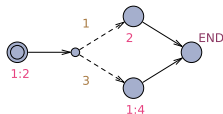
## A1



## A2



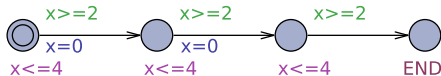
## A3



- Probability of  $\langle A1_0, \bar{0} \rangle \xrightarrow{0.5} \langle A1_0, \bar{0.5} \rangle$ ?
- Probability of reaching  $A1_1$  within 1?
- Probability of reaching  $A1_1$  within 5?
- Probability of reaching  $A2_1$  (above) within 5?
- Expected time to reach  $A1_1$ ?
- Expected time to reach  $A3_1$  or  $A3_2$ ?
- Expected time to reach  $A1_{END}$ ?
- Expected time to reach  $A2_{END}$ ?
- Expected time to reach  $A3_{END}$ ?

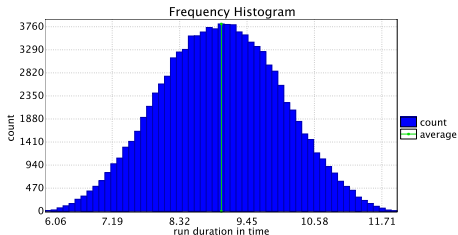
# A1: When does it end?

## A1



- Run 102000 times
- Histogram: how many times it took [9..9.1] seconds?
- ...

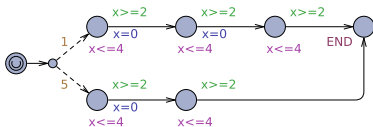
## A1's histogram



Parameters:  $\alpha=0.05$ ,  $\epsilon=0.05$ , bucket width=0.10002, bucket count=59  
Runs: 102000 in total, 102000 (100%) displayed, 0 (0%) remaining  
Span of displayed sample: [6.06618, 11.9675]  
Mean estimate of displayed sample:  $9.00732 \pm 0.00614869$  (95% CI)

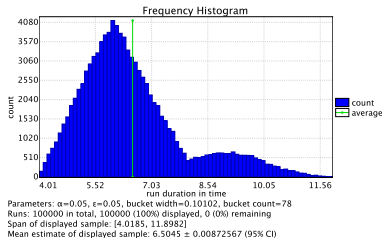
## A2: When does it end?

### A2

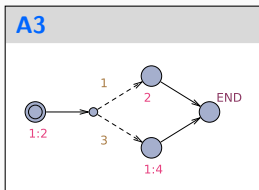


- Run 100000 times
- Histogram: how many times it took [9..9.1] seconds?
- ...

### A2's histogram

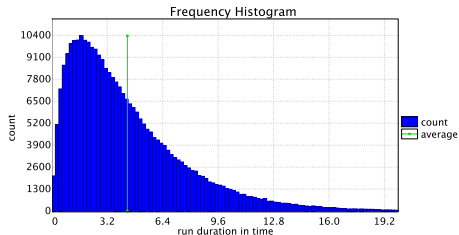


## A3: When does it end?



- Run 300000 times
- Histogram: how many times it took [9..9.1] seconds?
- ...

### A3's histogram



Parameters:  $\alpha=0.05$ ,  $\epsilon=0.05$ , bucket width=0.19991, bucket count=100  
Runs: 300000 in total, 299181 (99.727%) displayed, 819 (0.273%) remaining  
Span of displayed sample: [0.0045298, 19.9958]  
Mean estimate of displayed sample:  $4.31514 \pm 0.0118734$  (95% CI)

## Probabilistic queries in Uppaal

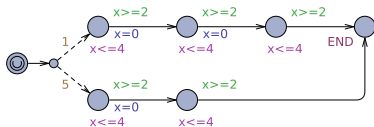
---

- `Pr[c<=10; 100] ([] safe)` – runs 100 stochastic simulations and estimates the probability of safe remaining true within 10 cost units, based on 100 runs.
- `Pr[<=10] (<> good)` – runs a number of stochastic simulations and estimates the probability of good eventually becoming true within 10 time units. The number of runs is decided based on the probability interval precision ( $\pm\epsilon$ ) and confidence level (level of significance  $\alpha$ ).
- `Pr[<=10] (<> good) >= 0.5` – checks if the probability of reaching good within 10 time units is greater than 50% (less runs than calculating the probability, using “Walds’s algorithm”)
- `E[<=10; 100] (max: cost)` runs 100 stochastic simulations and estimates the maximal value of cost expression over 10 time units of stochastic simulation.

More at [https://docs.uppaal.org/language-reference/query-syntax/statistical\\_queries/](https://docs.uppaal.org/language-reference/query-syntax/statistical_queries/)

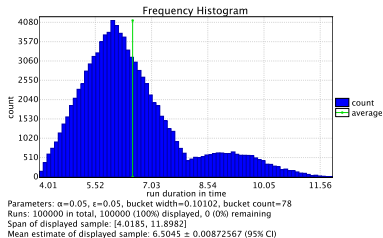
- `simulate[<=10] { x, y }` creates one stochastic simulation run of up to 10 time units in length and plot the values of `x` and `y` expressions over time (after checking, right-click the query and choose a plot).
- Variations: `[c<=10]` / `[#<=10]` – based on clock `c` or based on the number of transitions.

## A2



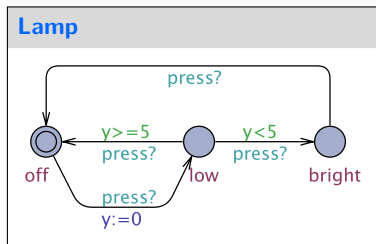
**Ex. 7.4:** Replicate the visualisation

## A2's histogram



**Ex. 7.5:** Replicate the visualisation also for A1 and A3





**Ex. 7.6:** Adapt the model to make it stochastic

**Ex. 7.7:** Adapt requirements to make them probabilistic

1. The lamp can become bright;
2. The lamp will eventually become bright;
3. The lamp can never be on for more than 3600s;
4. It is possible to never turn on the lamp;
5. Whenever the light is bright, the clock  $y$  is non-zero;
6. Whenever the light is bright, it will eventually become off.