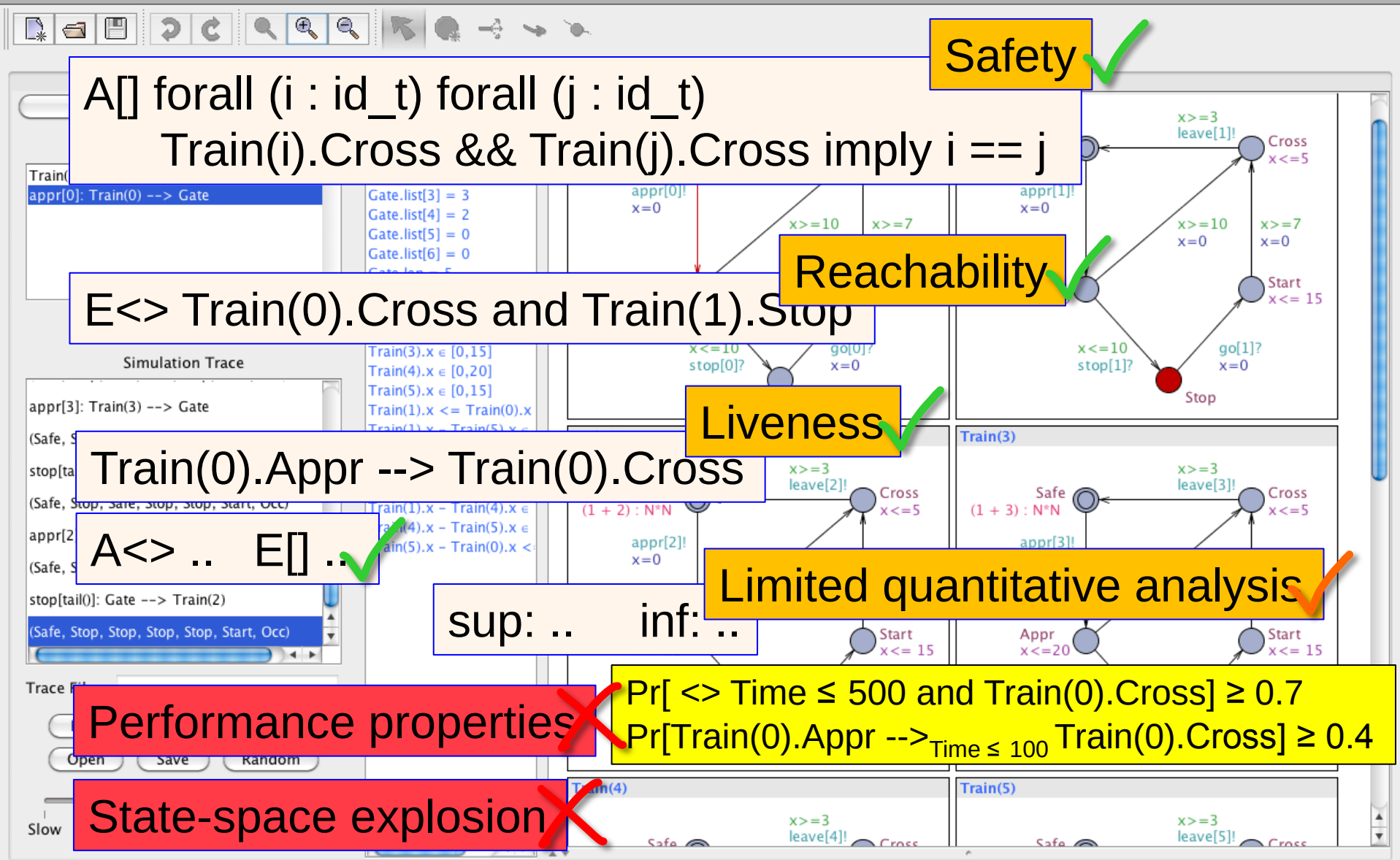
Statistical Model Checking in UPPAAL

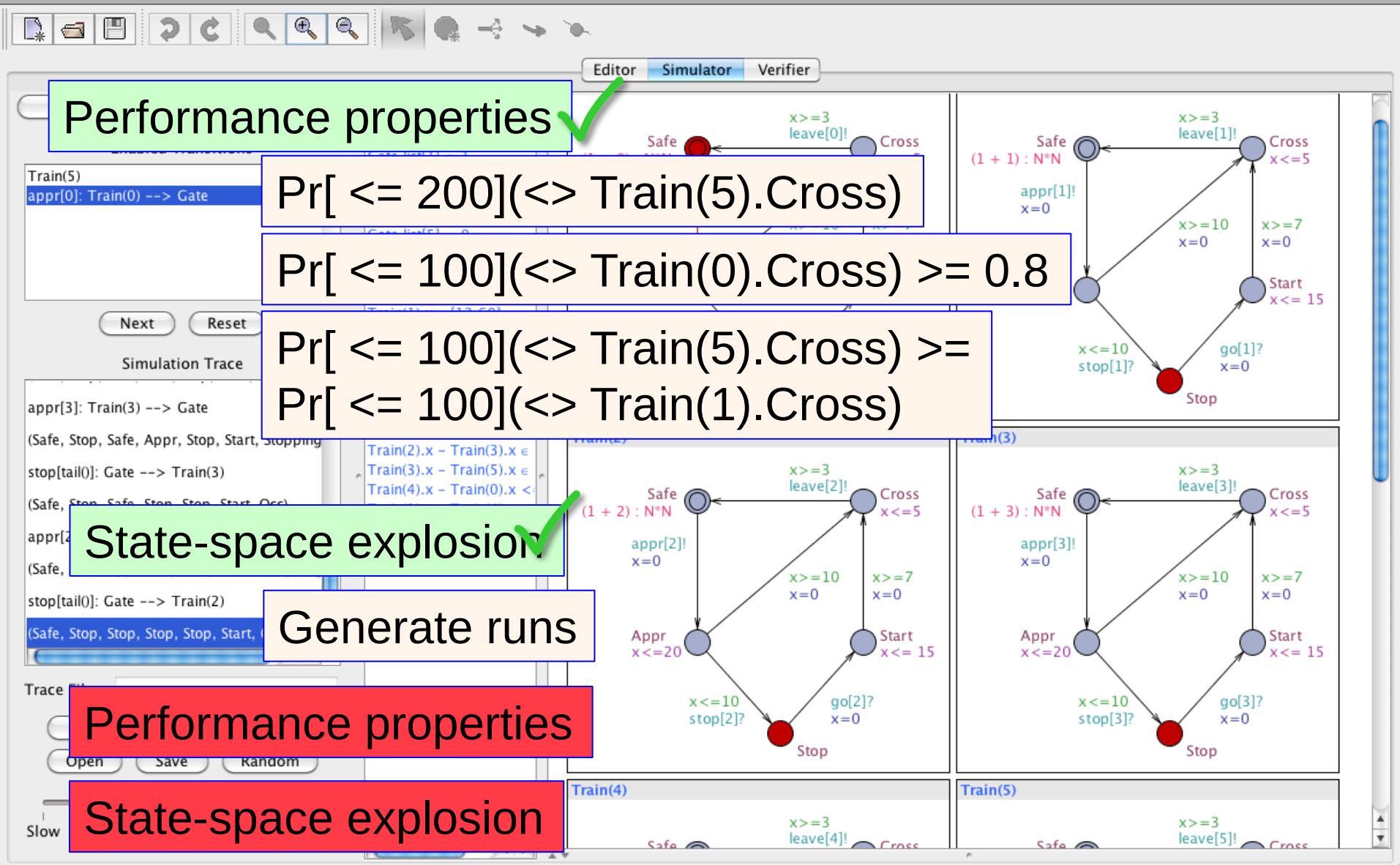
Alexandre David, Kim G. Larsen,
Axel Legay, Marius Mikucionis
Wang Zheng, Peter Bulychev,
Jonas van Vliet, Danny Poulsen,
Dehui Du, Guangyuan Li

CAV 11, PDMC 11,FORMATS 11,
QAPL12, LPAR12, iWIGPL12, RV12,
FORMATS12, HBS12,ISOLA12,
SCIENCE China,NFM13,RV13,AVOCS13

UPPAAL


A[] forall (i : id_t) forall (j : id_t)
Train(i).Cross && Train(j).Cross imply i == j
Safety
E<> Train(0).Cross and Train(1).Stop
Reachability
Train(0).Appr --> Train(0).Cross
Liveness
A<> .. E[] ..
sup: .. inf: ..
Limited quantitative analysis
Performance properties
Pr[<> Time ≤ 500 and Train(0).Cross] ≥ 0.7
Pr[Train(0).Appr -->Time ≤ 100 Train(0).Cross] ≥ 0.4
State-space explosion
Simulation Trace
Train(0)
Train(1)
Train(2)
Train(3)
Train(4)
Train(5)
Cross
Start
Stop
Safe
Appr

UPPAAL SMC


Editor
Simulator
Verifier
Performance properties
Pr[<= 200](<> Train(5).Cross)
Pr[<= 100](<> Train(0).Cross) >= 0.8
Pr[<= 100](<> Train(5).Cross) >=
Pr[<= 100](<> Train(1).Cross)
State-space explosion
Generate runs
Performance properties
State-space explosion
Train(5)
appr[0]: Train(0) --> Gate
Next
Reset
Simulation Trace
appr[3]: Train(3) --> Gate
stop[tail()]: Gate --> Train(3)
stop[tail()]: Gate --> Train(2)
Open
Save
Random
Slow
Safe
Cross
Appr
Start
Stop
x>=3
leave[0]!
leave[1]!
leave[2]!
leave[3]!
leave[4]!
leave[5]!
(1 + 1) : N*N
(1 + 2) : N*N
(1 + 3) : N*N
appr[1]!
appr[2]!
appr[3]!
x=0
x>=10
x>=7
x<=5
x<=15
x<=20
x<=10
stop[1]?
stop[2]?
stop[3]?
go[1]?
go[2]?
go[3]?
Train(3)
Train(4)
Train(5)

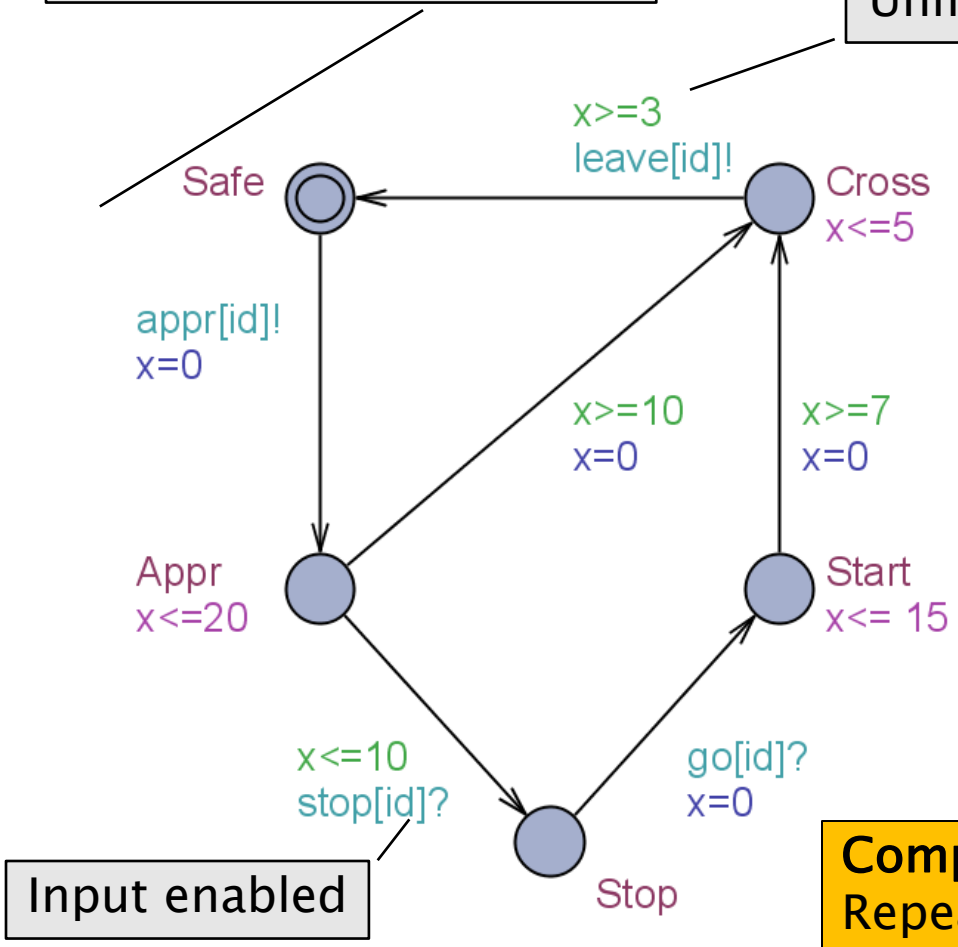
Overview

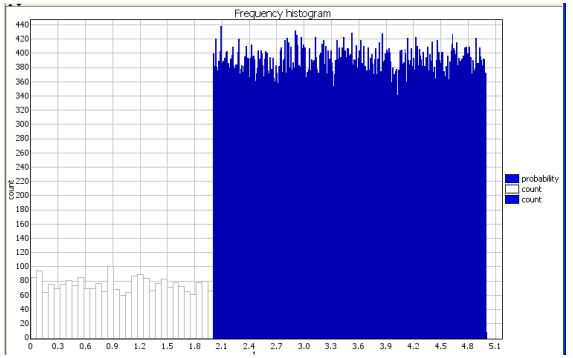
- Stochastic Semantics of Networks of Timed Automata
- Statistical Model Checking in UPPAAL
  - Estimation
  - Sequential Hypothesis Testing
  - Sequential Probability Comparison
  - Parameterized Probability Comparison
- SMC of Hybrid Automata
- Case Studies & Demo

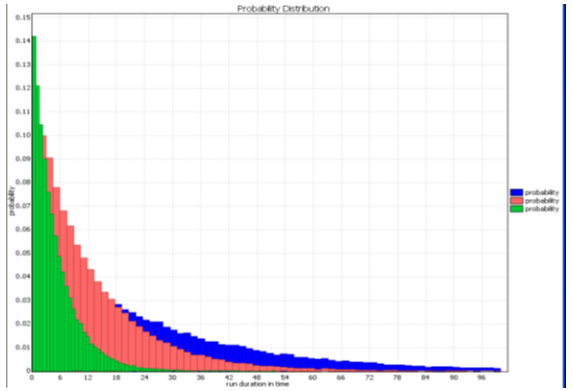
Stochastic Semantics of TA

Exponential Distribution

Uniform Distribution



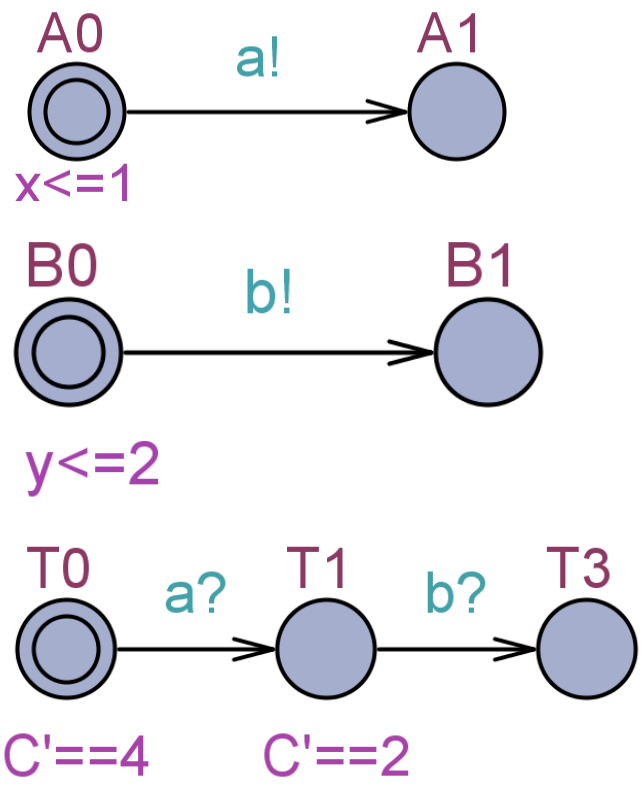




Input enabled

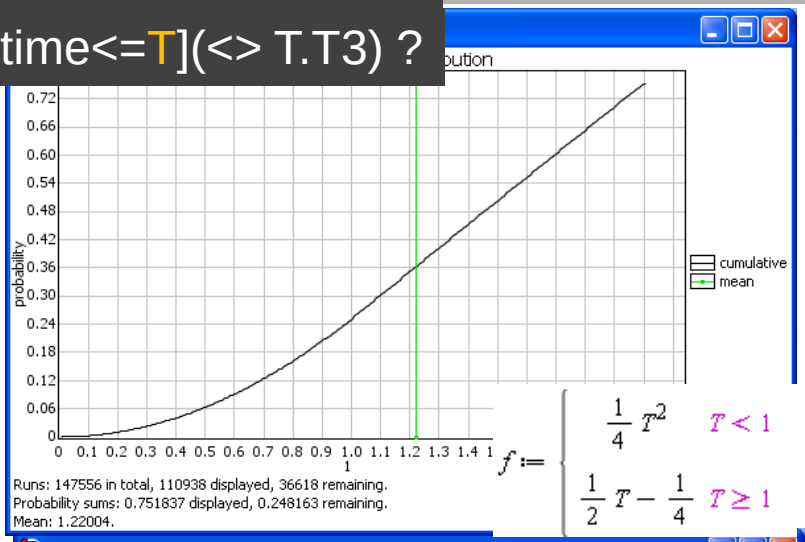
Composition =
Repeated races between components

Stochastic Semantics of Timed Automata

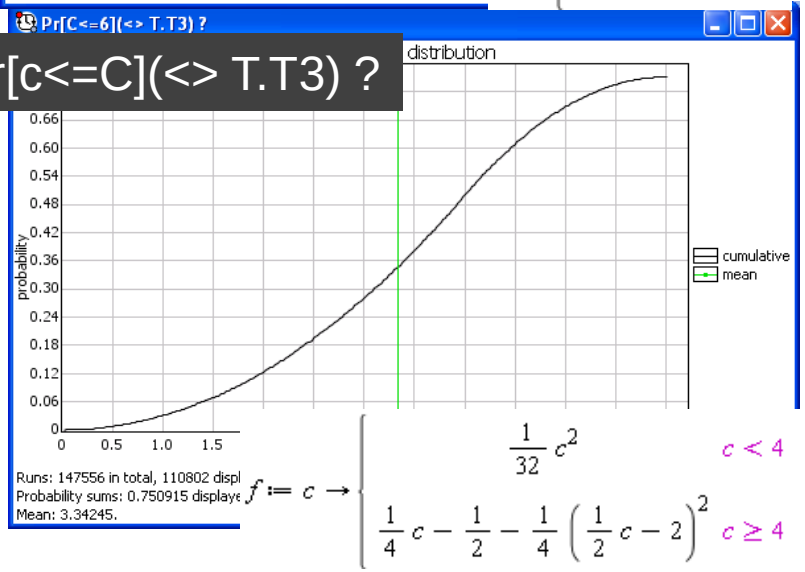


Composition = Race between components for outputting

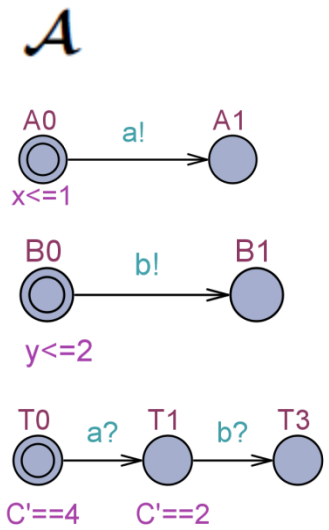
Pr[time<=T](<> T.T3) ?



Pr[c<=C](<> T.T3) ?



Stochastic Semantics of Timed Automata



Assumptions:
Component TAs are:
- Input enabled
- Deterministic
- Disjoint set of output actions

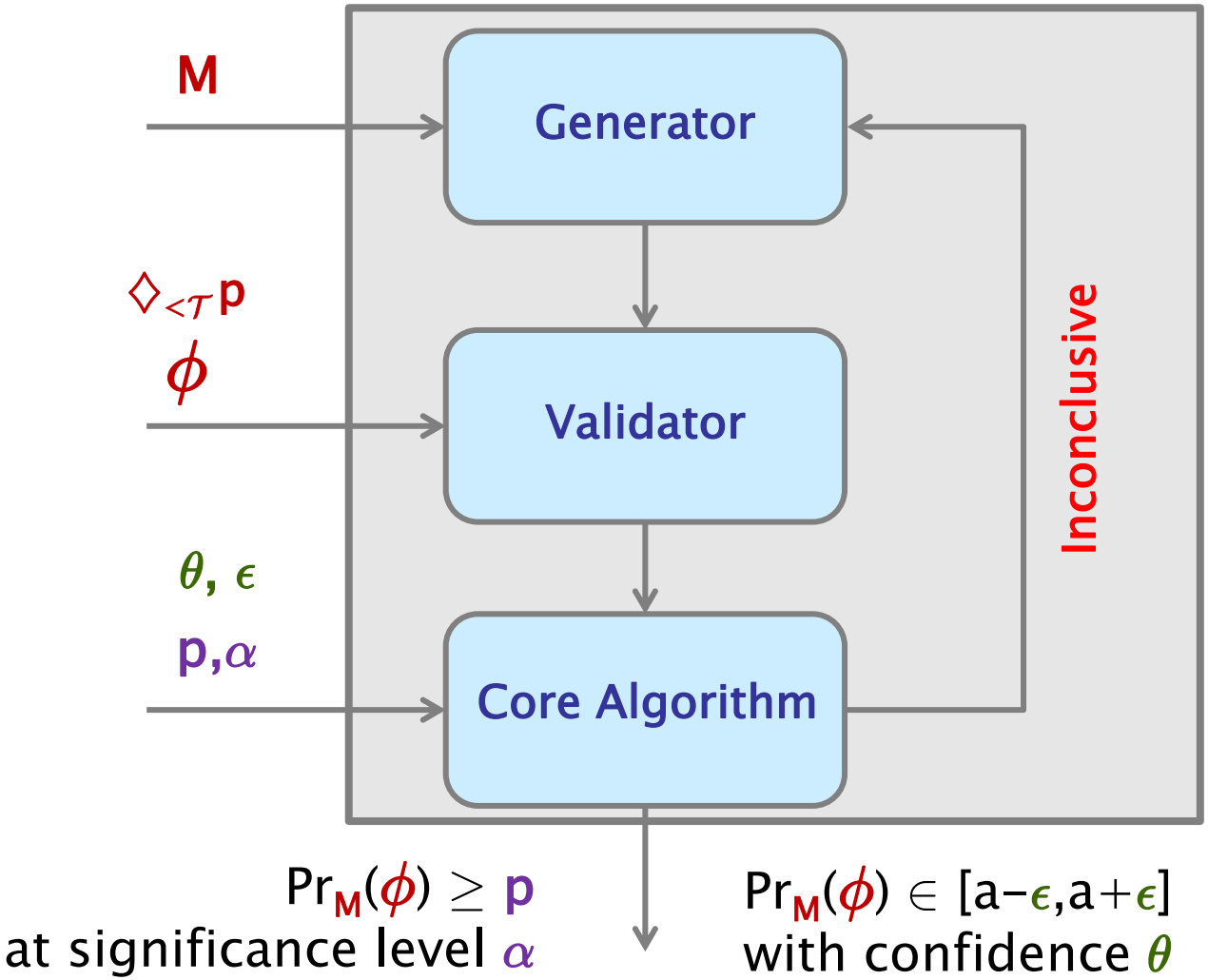
π (**s** , $a_1\ a_2\ \ldots.\ a_n$) :
the set of maximal runs from **s** with a prefix
$t_1\ a_1\ t_2\ a_2\ \ldots\ t_n\ a_k$
for some $t_1,\ldots,t_n \in \mathbf{R}$.

$$\mathbb{P}_{\mathcal{A}}\big(\pi(\mathbf{s},\, a_1 a_2 \ldots a_n)\big) =$$
$$\int_{t\geq 0} \mu_{s_c}(t) \cdot \Big(\prod_{j\neq c} \int_{\tau>t} \mu_{s_j}(\tau)\, d\tau\Big) \cdot \gamma_{s_c{}^t}(a_1) \cdot \mathbb{P}_{\mathcal{A}}\big(\pi(\mathbf{s}^t)^{a_1},\, a_2 \ldots a_n\big)\ dt$$

where $c = c(a_1)$, and as base case we take $P_{\mathcal{A}}(\pi(\mathbf{s}), \varepsilon) = 1$.

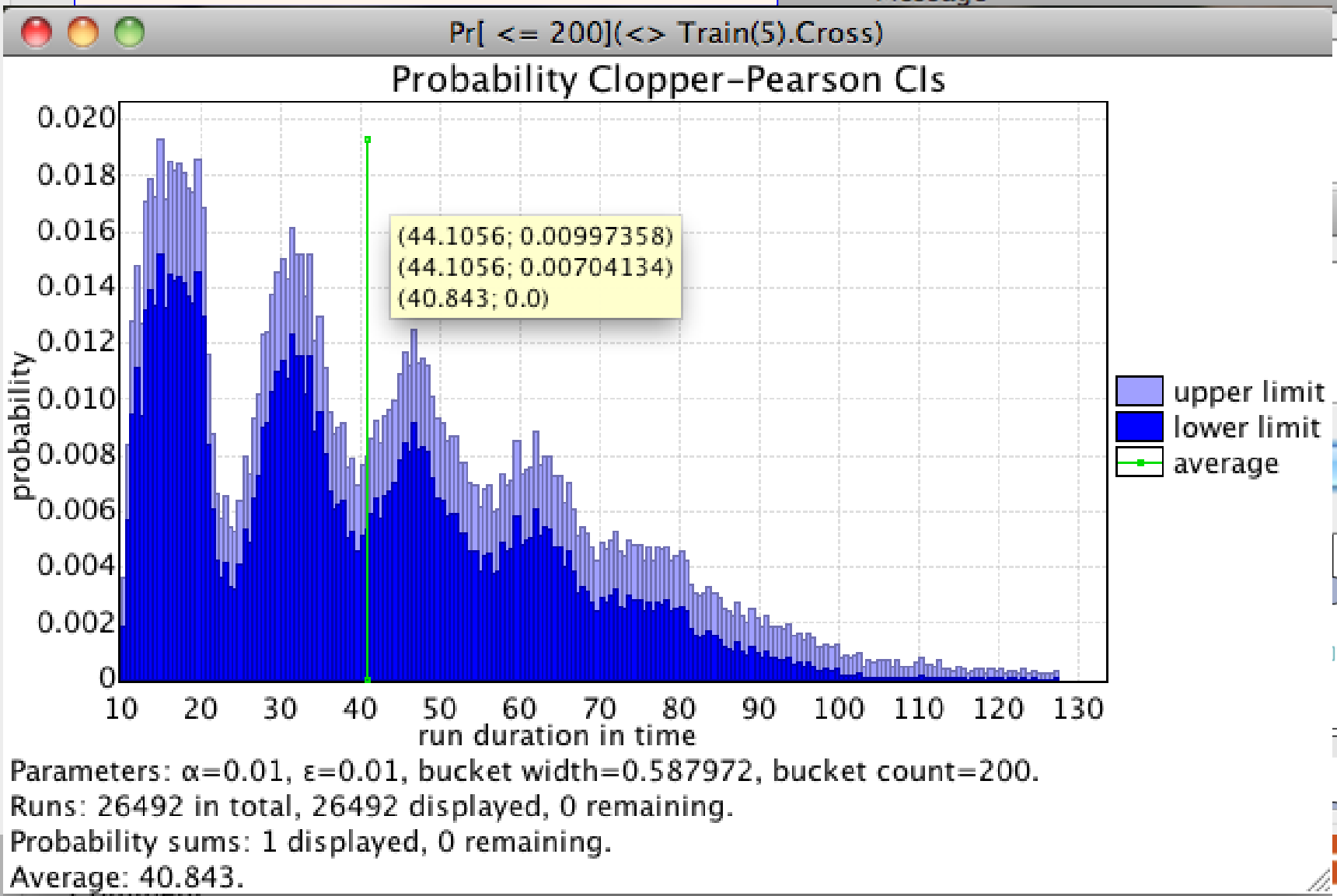
Statistical Model Checking

[FORMATS11, LPAR12, RV12]



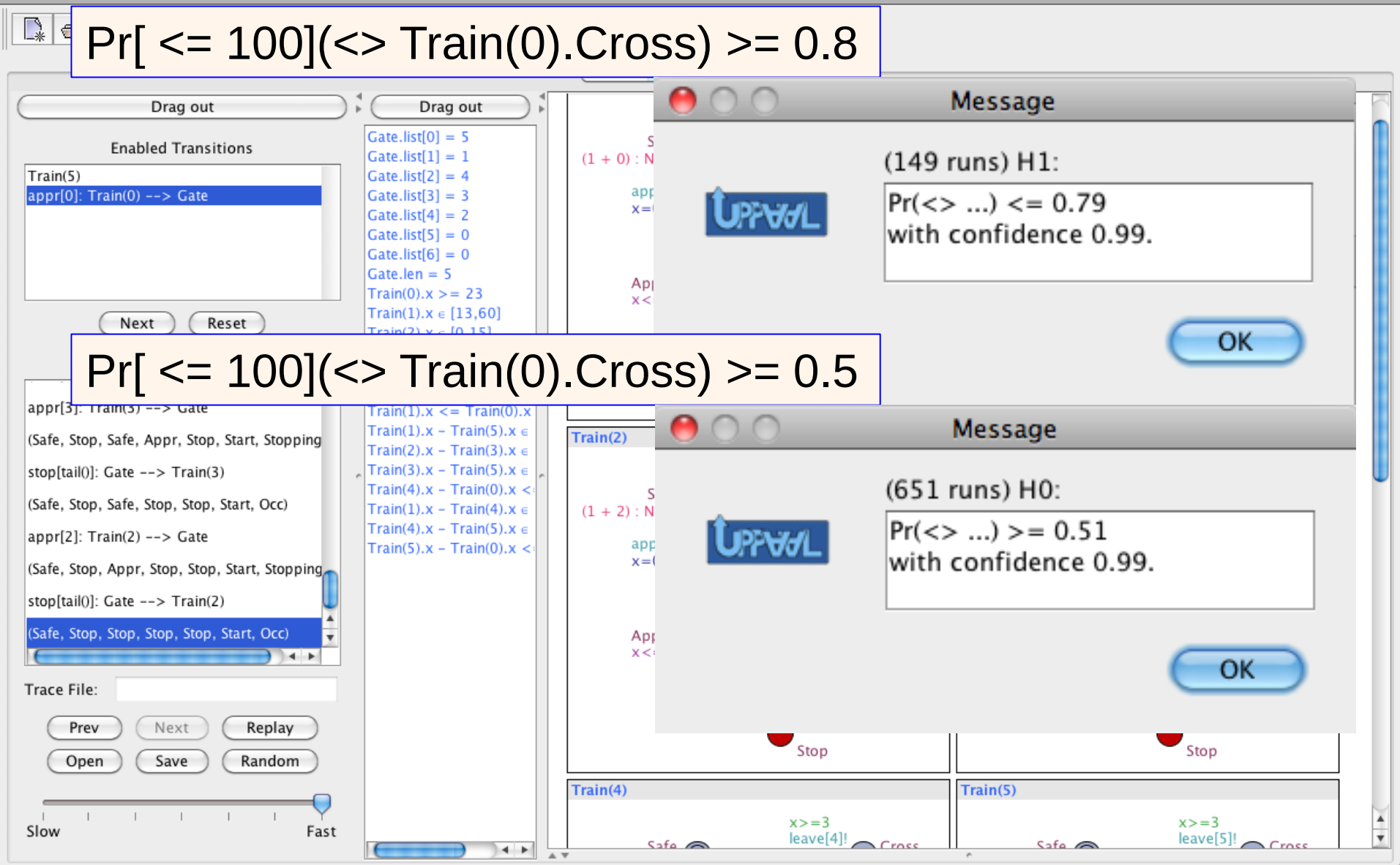
Queries in UPPAAL SMC

Pr[<= 200](<> Train(5).Cross)



Queries in UPPAAL SMC

Pr[<= 100](<> Train(0).Cross) >= 0.8



Pr[<= 100](<> Train(0).Cross) >= 0.5

Queries in UPPAAL SMC

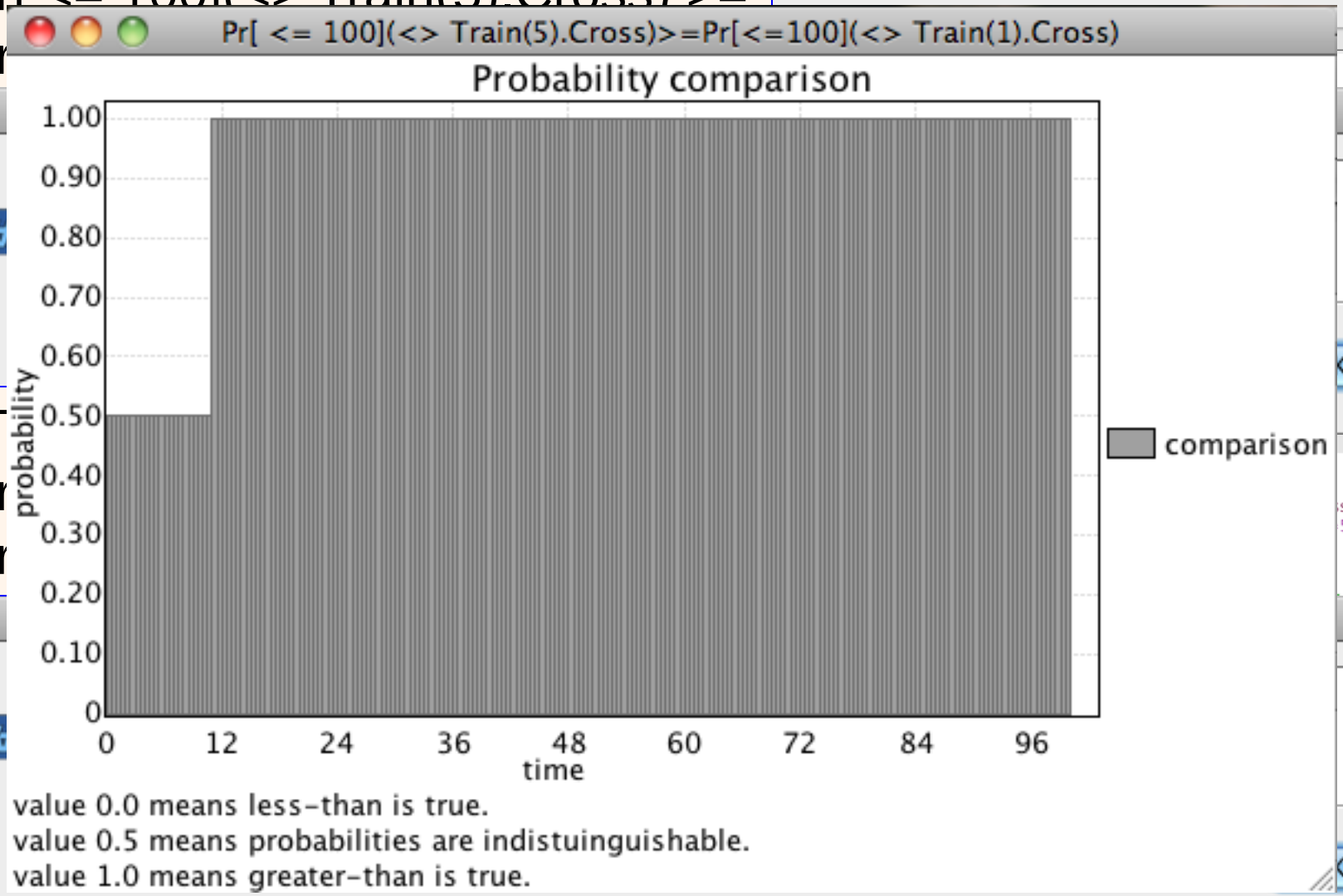
Pr[<= 100](<> Train(5).Cross) >=

Pr

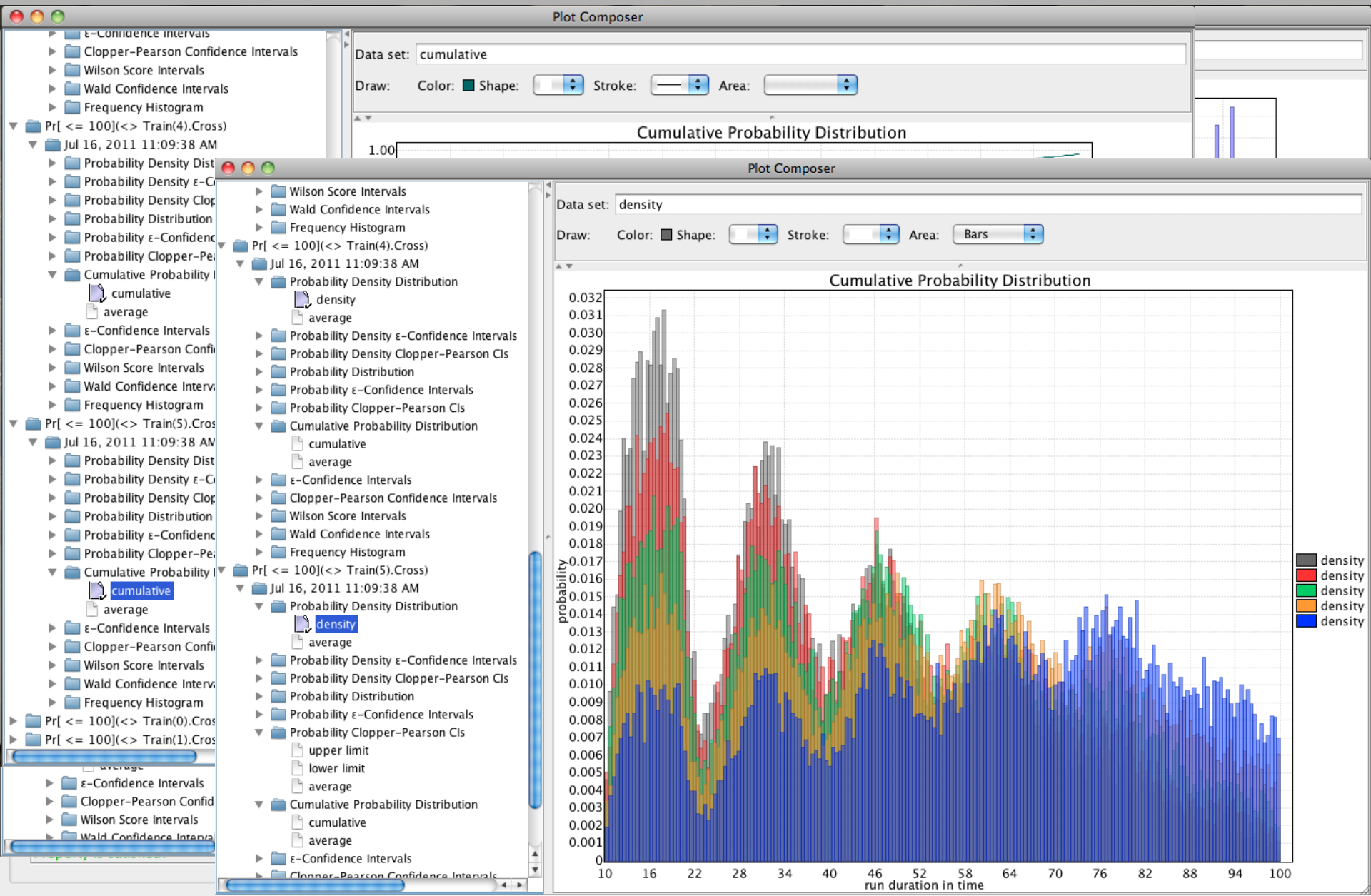
∀

Pr

Pr



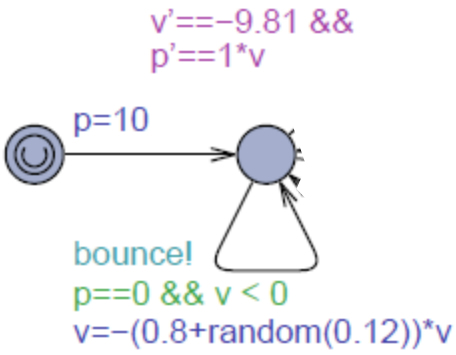
Analysis Tool: Plot Composer



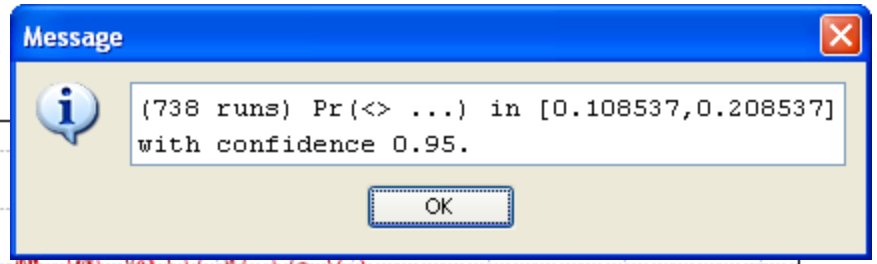
Demo

Stochastic Hybrid Systems

- A Bouncing Ball



Simulate 5 [<=20] {p}



Pr[<=20](<>(time >=12 && p >= 4))

Stochastic Hybrid Systems

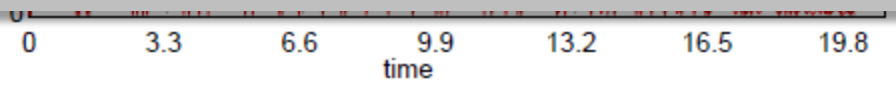
- A Bouncing Ball

UPPAAL SMC

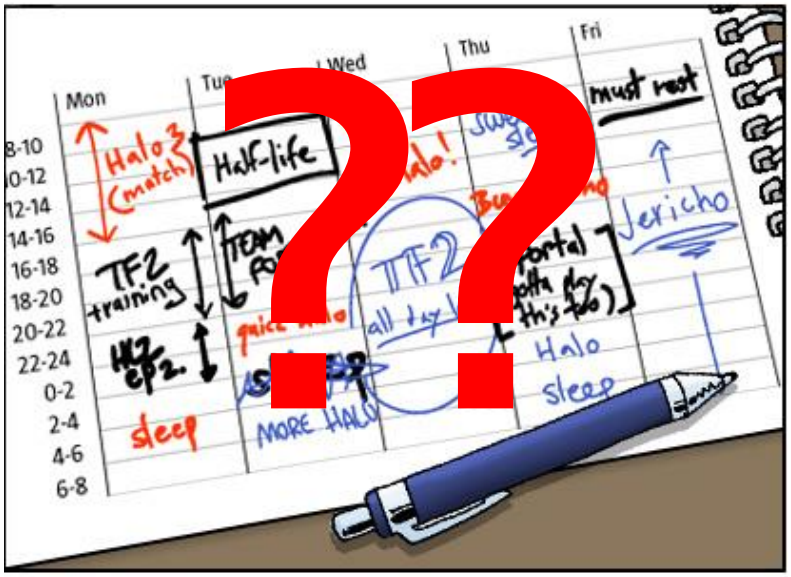
Uniform distributions (bounded delay)
Exponential distributions (unbounded delay)
Syntax for discrete probabilistic choice
Distribution on next state by use of `random`
Hybrid flow by use of ODEs
+ usual stuff (structured variables, user-defined types
  user-defined functions, ….)

Networks

Repeated races between components for outputting



Schedulability & Performance Analysis



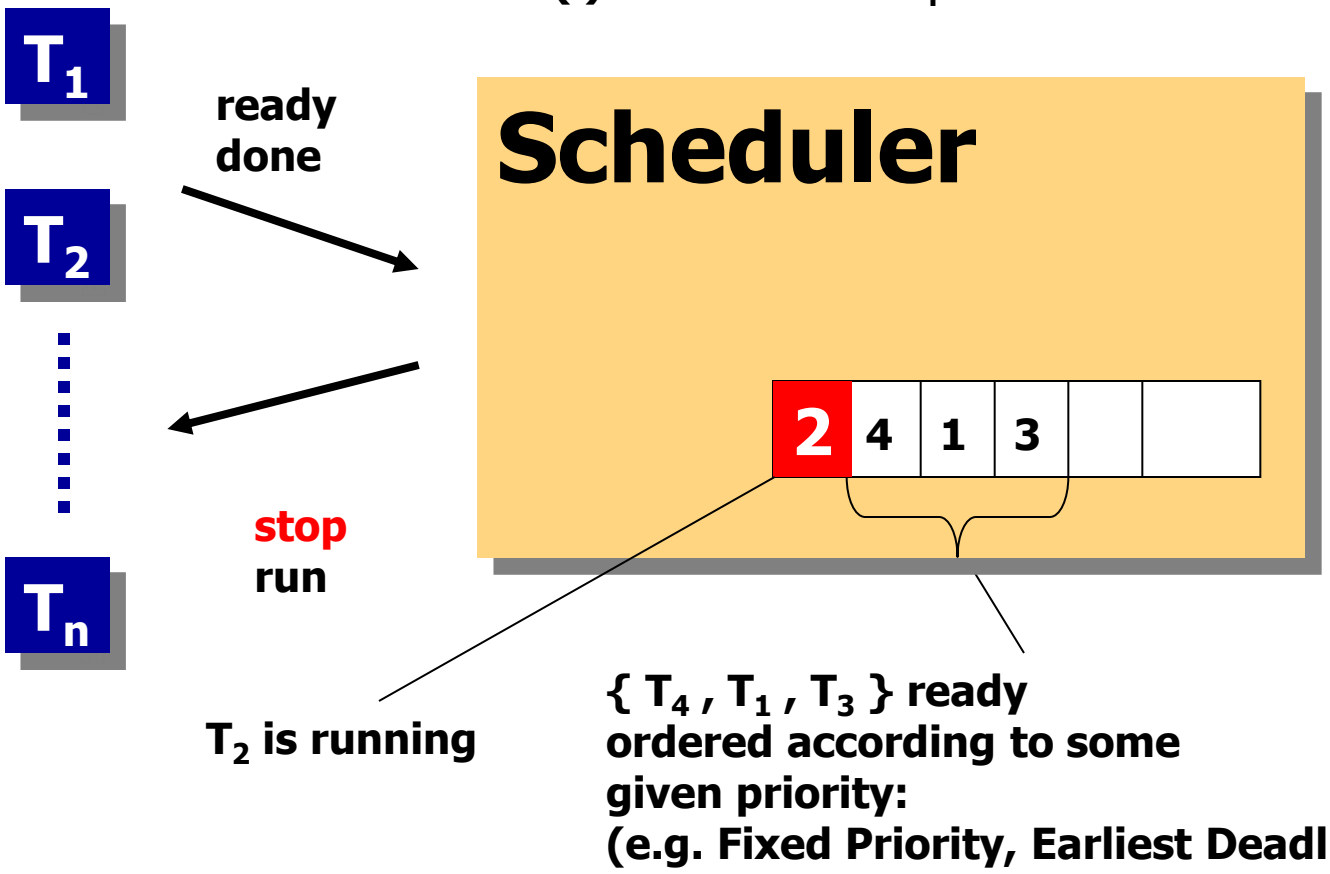
Task Scheduling

utilization of CPU

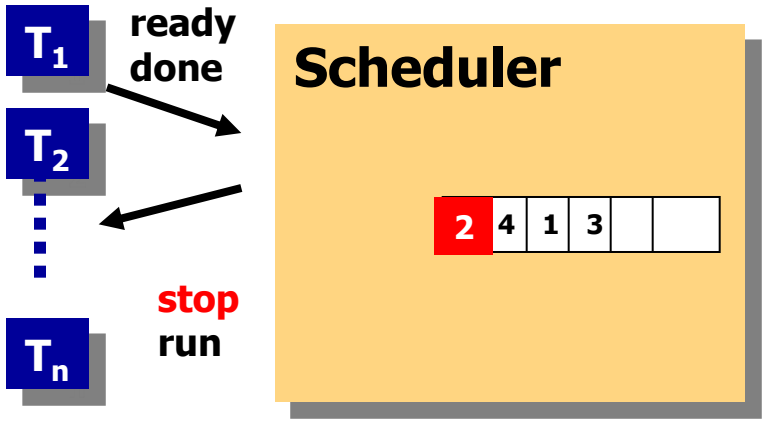
P(i), UNI[E(i), L(i)], .. : period or earliest/latest arrival or .. for T_i

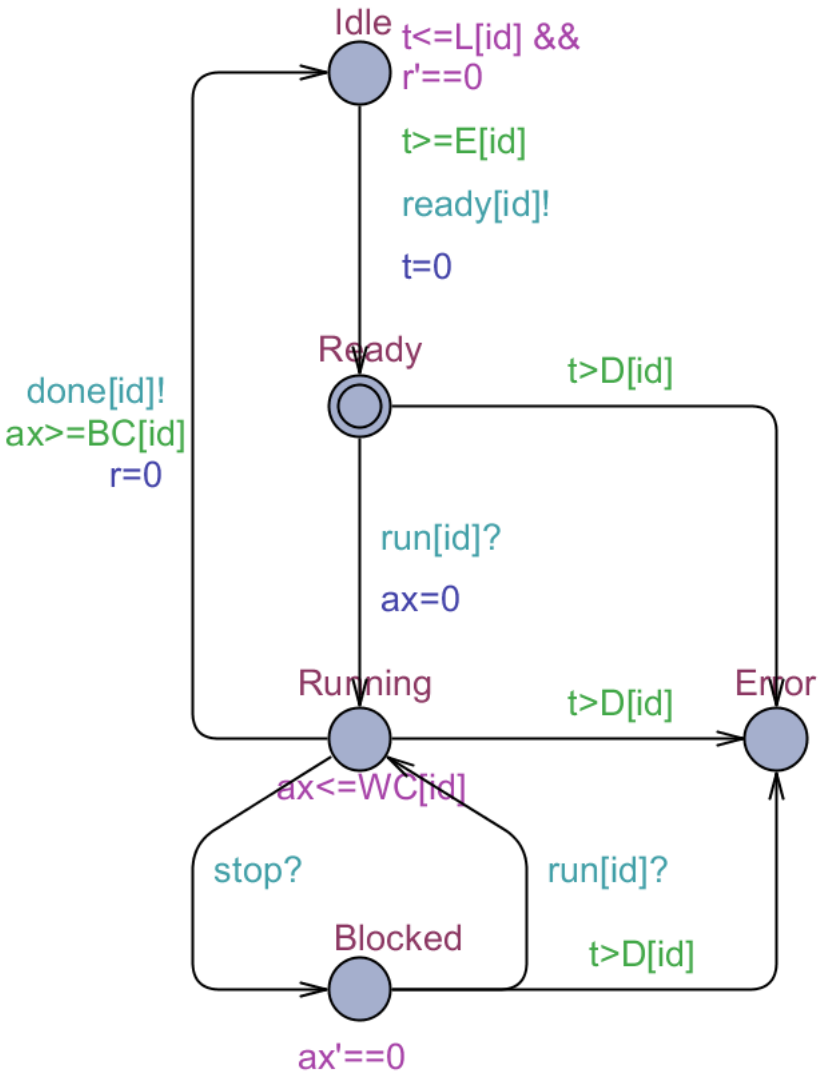
C(i), UNI[BC(i),WC(i)] : execution time for T_i

D(i): deadline for T_i

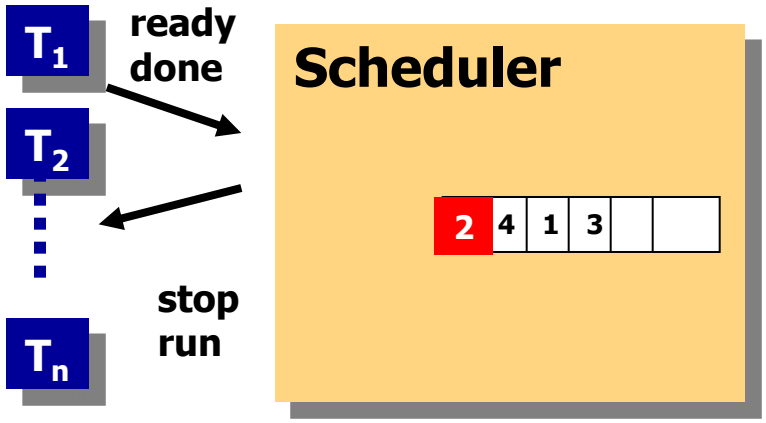


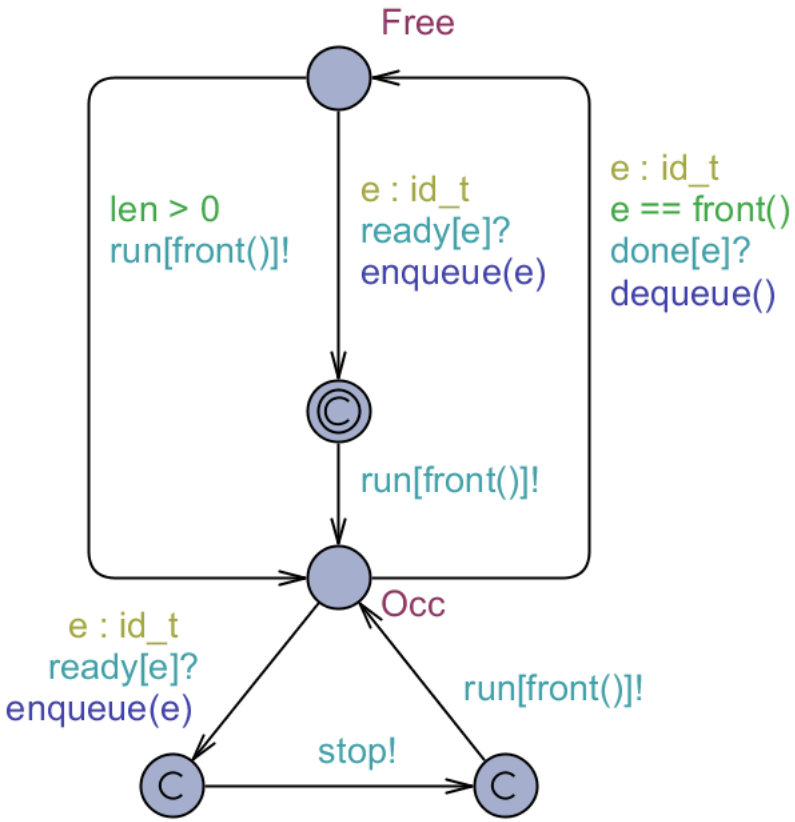
Modeling Task



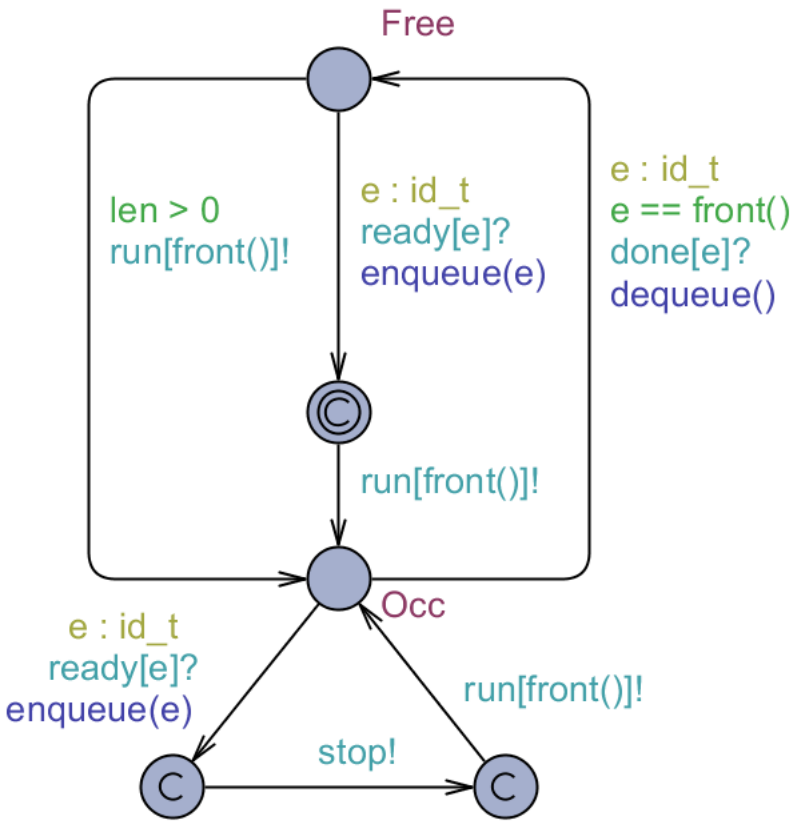


Modeling Scheduler





Modeling Queue



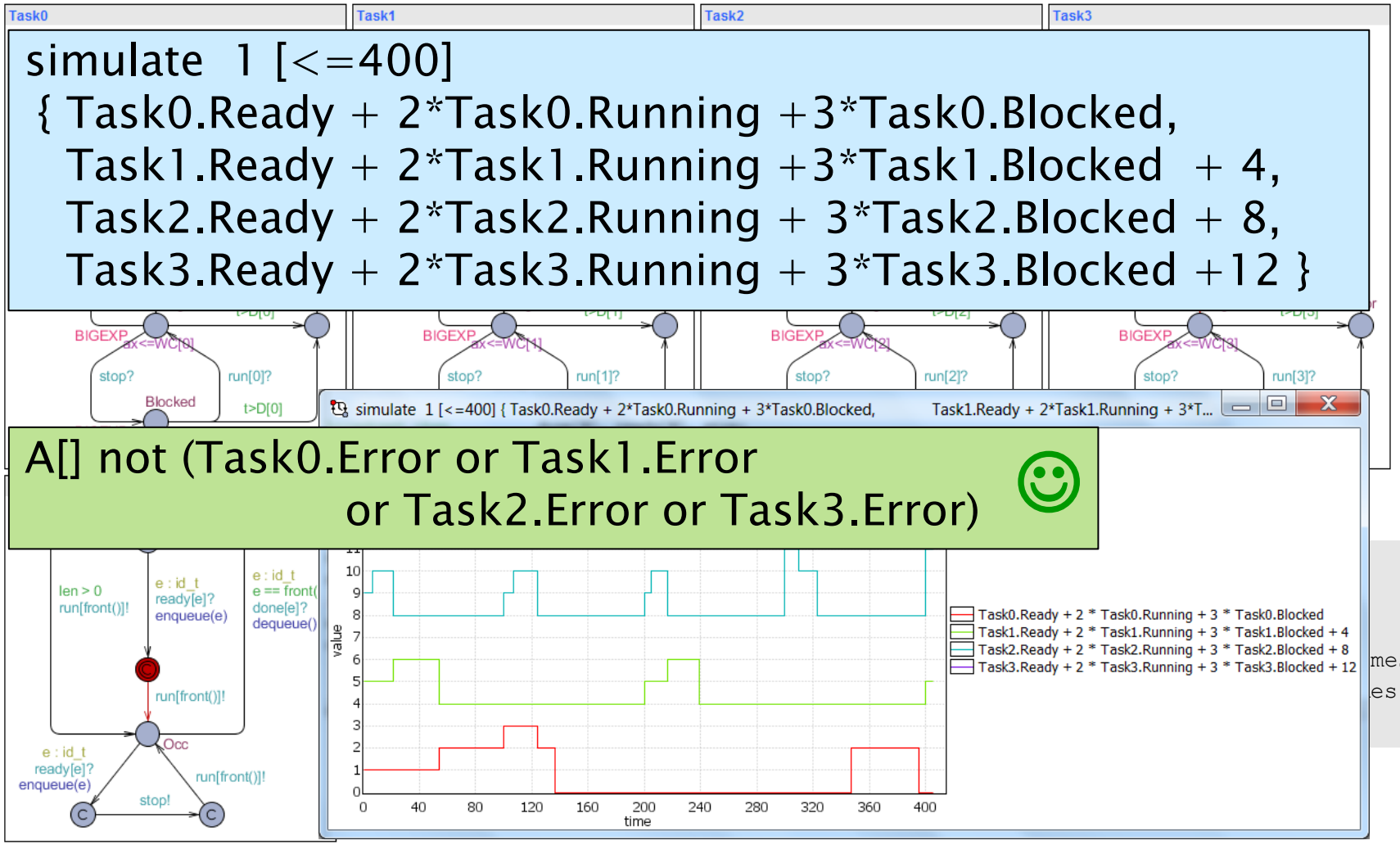

```
// Put an element at the end of the queue
void enqueue(id_t element)
{
int tmp=0;
list[len++] = element;
if (len>0)
{
        int i=len-1;
        while (i>1 && P[list[i]]>P[list[i-1]])
        {
                tmp = list[i-1];
                list[i-1] = list[i];
                list[i] = tmp;
                i--;
        }
}
}

// Remove the front element of the queue
void dequeue()
{
  ......
```

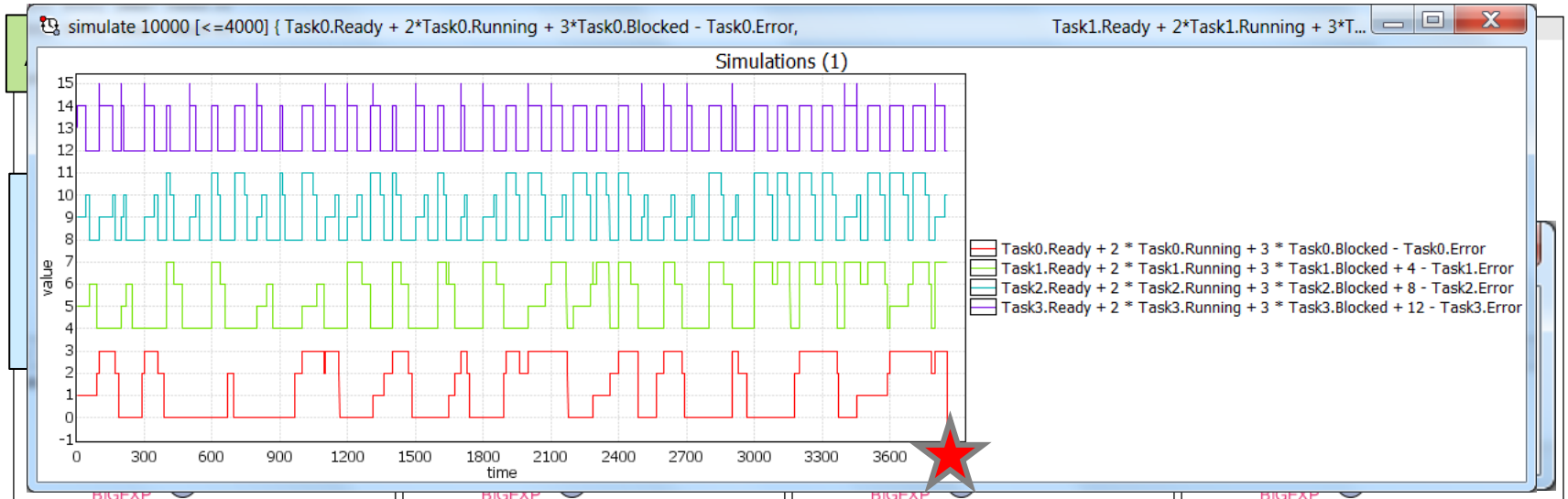
Schedulability Analysis

simulate 1 [<=400]
{ Task0.Ready + 2*Task0.Running +3*Task0.Blocked,
Task1.Ready + 2*Task1.Running +3*Task1.Blocked + 4,
Task2.Ready + 2*Task2.Running + 3*Task2.Blocked + 8,
Task3.Ready + 2*Task3.Running + 3*Task3.Blocked +12 }

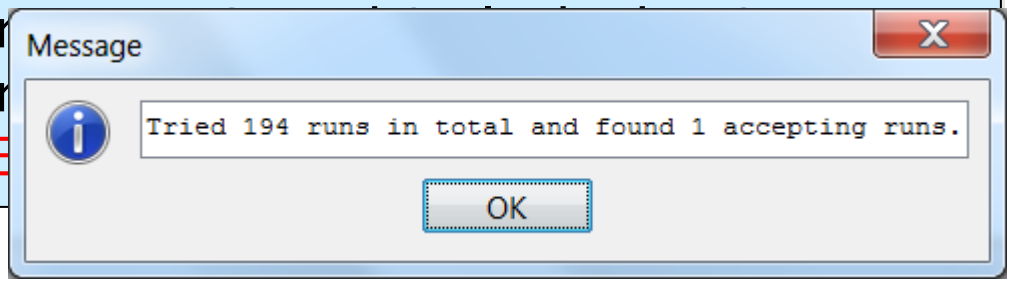
A[] not (Task0.Error or Task1.Error
or Task2.Error or Task3.Error)



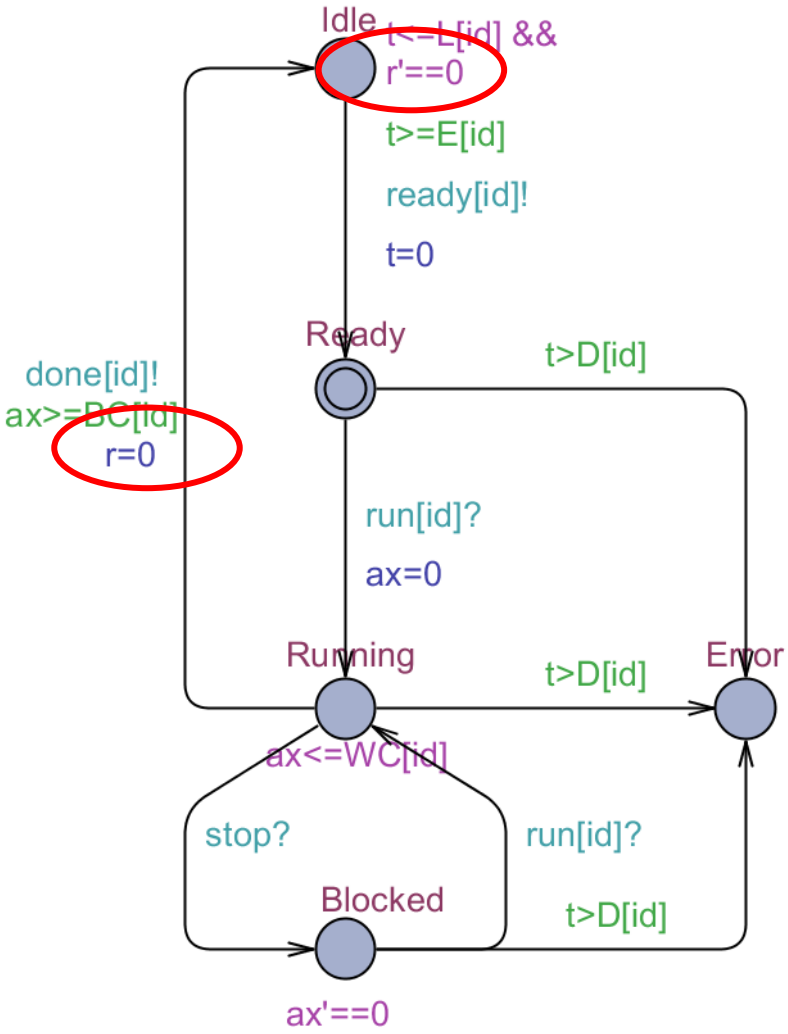
Schedulability Analysis



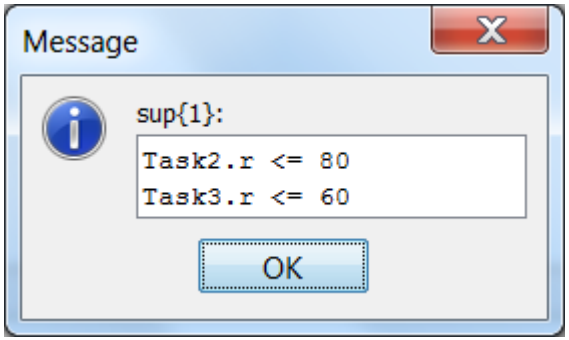
simulate 10000 [<=400]
{ Task0.Ready + 2*Task0.Running +3*Task0.Blocked,
Task1.Ready + 2*Task1.Running +3*Task1.Blocked + 4,
Task2.Ready + 2*Task2.Run
Task3.Ready + 2*Task3.Run
: 1 : (Task0.Error or Task1.E



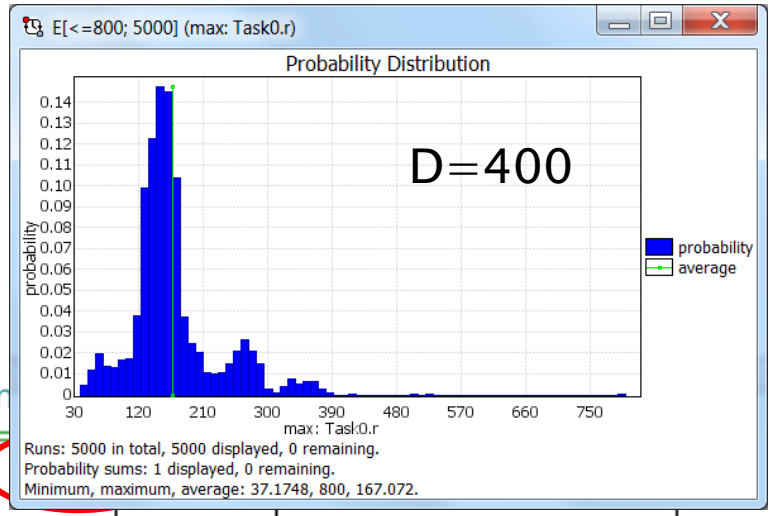
Performance Analysis

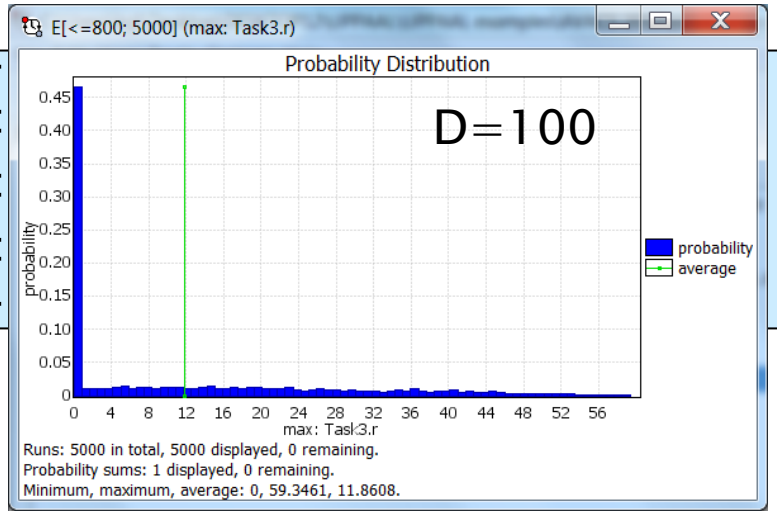


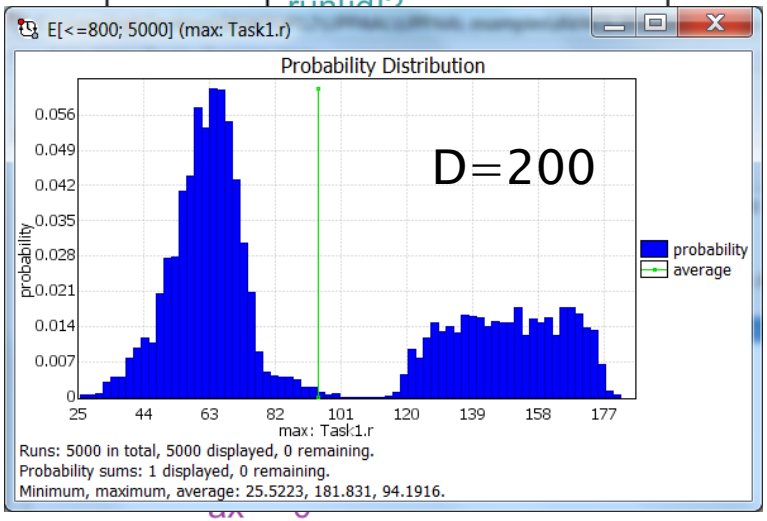
sup : Task2.r, Task3.r

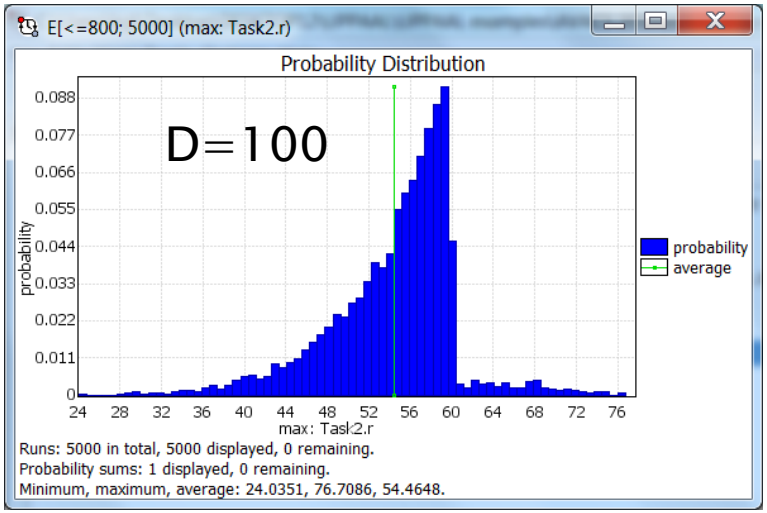


Performance Analysis







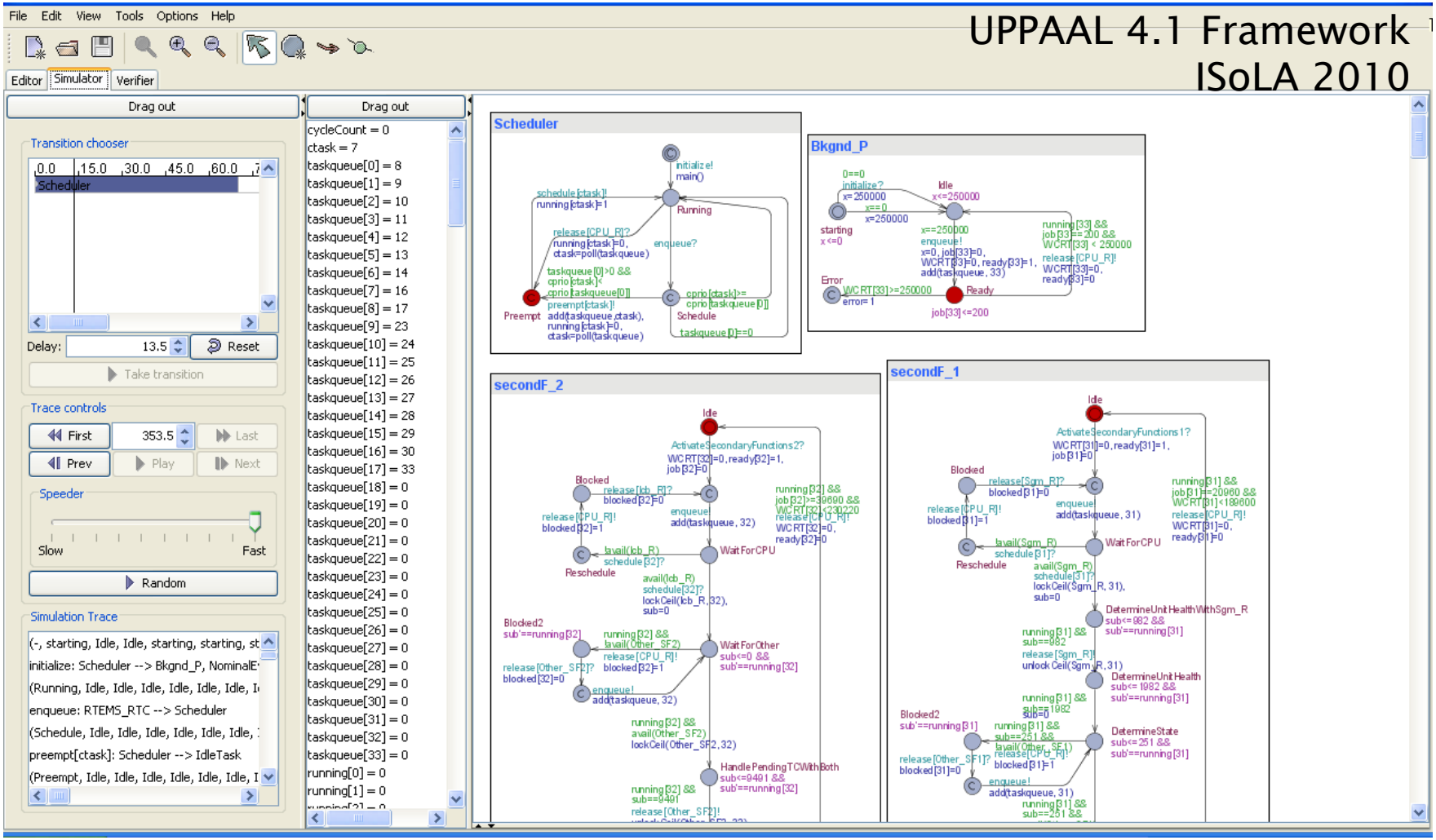


Herschel-Planck Scientific Mission at ESA

Attitude and Orbit Control Software
TERMA A/S Steen Ulrik Palm, Jan Storbank Pedersen, Poul Hougaard

Modeling in UPPAAL

TERMA



UPPAAL 4.1 Framework
ISoLA 2010

Symbolic MC vs. Statistical MC

Symbolic analysis:

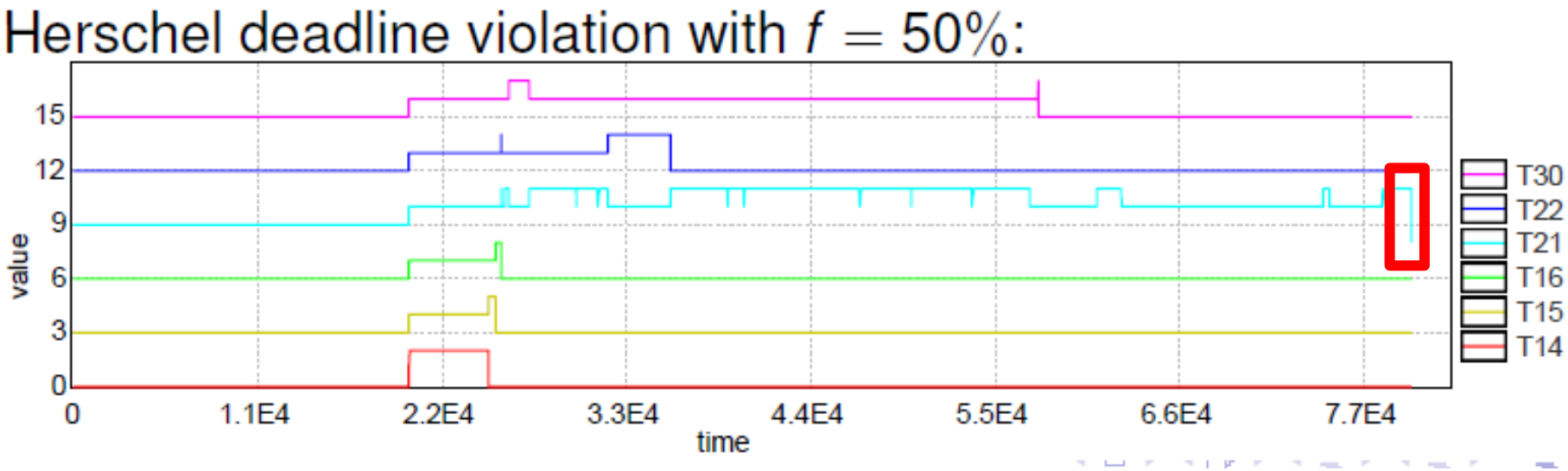
- Preemptive scheduler requires *stop-watches*.
- Exact reachability of stop-watch automata is *undecidable*.
- UPPAAL provides *over-approximation* for stop-watches.
- $\Rightarrow$ symbolic analysis may give spurious errors, but still suitable for *proving safety/schedulability*.

Statistical analysis:

- can show *presence of errors* but not absence.
- $\Rightarrow$ suitable for *disproving schedulability*.

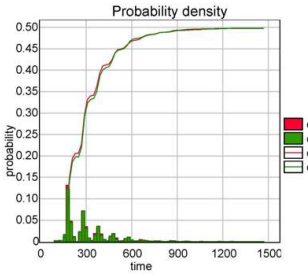
$f = \text{BCET}/\text{WCET}$:	0-71%	72-86%	87-89%	90-100%
Symbolic MC:	maybe	maybe	n/a	**Safe**
Statistical MC:	**Unsafe**	maybe	maybe	maybe

SMC Simulation to Find Error

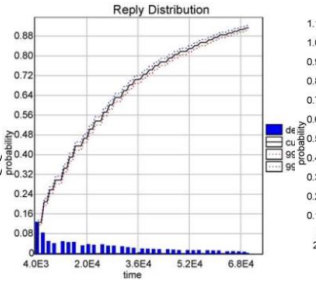


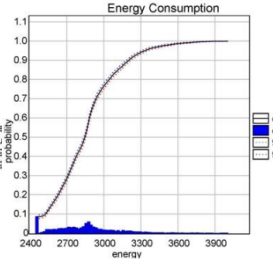

```
simulate 10000 [<=300] {
   (T(1).Ready+T(1).Computing+T(1).Release+runs[1]-2*T(1)
   (T(2).Ready+T(2).Computing+T(2).Release+runs[2]-2*T(1)
   (T(3).Ready+T(3).Computing+T(3).Release+runs[3]-2*T(1)
} : 1 : error
```

Other Case Studies

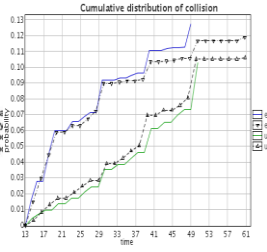


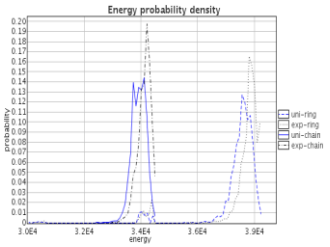
FIREWIRE



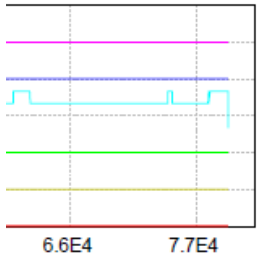


BLUETOOTH

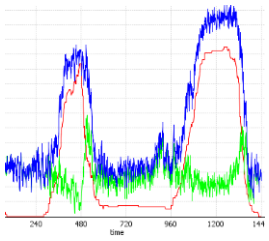




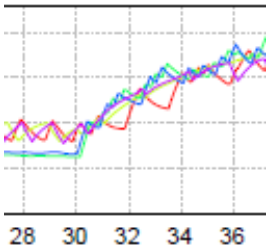
10 node LMAC



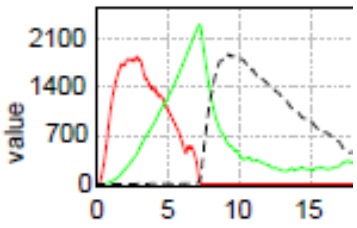
Schedulability Analysis for Mix Cr Sys



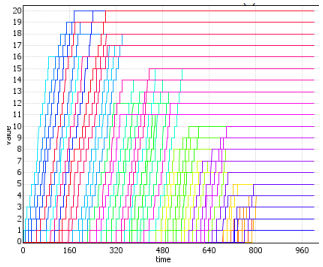
Smart Grid Demand / Response



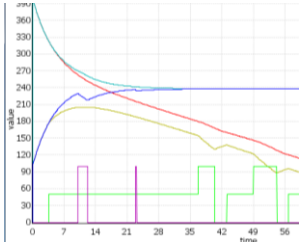
Energy Aware Buildings



Genetic Oscilator (HBS)



Passenger Seating in Aircraft



Battery Scheduling
(SENSATION)
Erik Wogensen

SMC Queries – Examples

- Pr[<=100](<> goal)
- Pr[#<=10]([] safe)
- Pr[x<=200](<> goal) >= 0.3
- E[<=100; 1000](min: expr)
- simulate 10 [<=100] { e1, e2, x1 }
- simulate 100 [<=10] { e } : 2 : goal

Exercise 28 (Jobshop scheduling part 2)