HASL: an Expressive Language for Statistical Verification of Stochastic Models

Hilal Djafri (LSV)

Joint work with Paolo Ballarini (LACL)
Marie Duflot (LACL), Serge Haddad (LSV)
and Nihal Pekergin (LACL)

MeFoSyLoMa Seminar

Cachan, December 17th 2010

Outline

Outline

Stochastic Model Checking

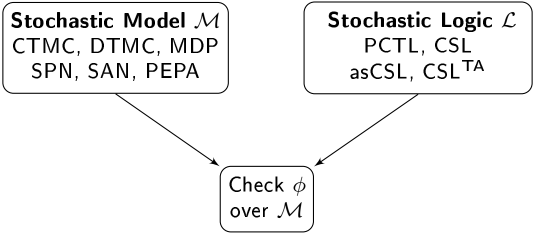
Stochastic Model $\mathcal{M}$
CTMC, DTMC, MDP
SPN, SAN, PEPA

Stochastic Model Checking

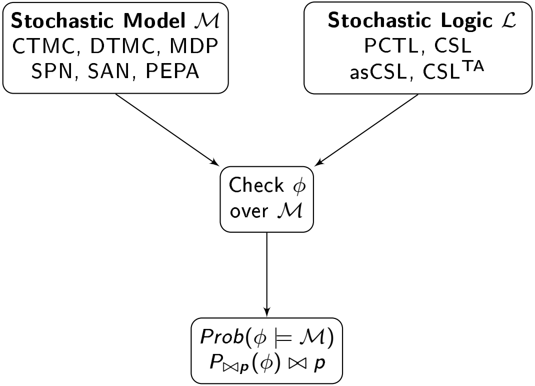
Stochastic Model $\mathcal{M}$
CTMC, DTMC, MDP
SPN, SAN, PEPA

Stochastic Logic $\mathcal{L}$
PCTL, CSL
asCSL, CSL^{TA}

Stochastic Model Checking



Stochastic Model Checking



Numerical Methods

- Principles
  - Generate a stochastic process from the high level description
  - Compute some measures from the process: numerical analysis, solving systems of equations.
- Advantages
  - accuracy of results
- Drawbacks
  - Require huge memory
  - The stochastic process must be markovian or semi-markovian

Statistical Methods

- Principles
  - Generate sufficient number of trajectories.
  - Discrete event simulation, statistic technics: estimation, hypothesis testing ...
- Advantages
  - No problem of memory
  - General class of stochastic processes
- Drawbacks
  - Execution time can be very important
  - Nested formulas are not considered
  - Steady state properties are difficult to compute.

Principle of a Statistical Estimation

- Let X a random variable such that $X \hookrightarrow \mathcal{N}(\mu, \sigma^2)$
- $x_1, ..., x_n$ independant sample normally distributed
- We want to estimate μ by $\overline{x}$ where
  $Prob(\overline{x} - \epsilon < \mu < \overline{x} - \epsilon) = 1 - \alpha$
- $\mu \in [\overline{x} - t^{n-1}_{\alpha/2} \times \frac{S}{\sqrt{n}}, \overline{x} + t^{n-1}_{\alpha/2} \times \frac{S}{\sqrt{n}}]$
- $\overline{x} = \frac{1}{n} \sum_{i=1}^{n} x_i$ sample mean,
  $S^2 = \frac{1}{n-1} \sum_{i=1}^{n} (x_i - \overline{x})^2$ sample variance,
  $t^{n-1}_{\alpha/2}$ Student percentile.
- Big value of n: $t_n \hookrightarrow \mathcal{N}(0, 1) \Rightarrow$ replace $t^{n-1}_{\alpha/2}$ by $Z_{\alpha/2}$
- Generate samples until $Z_{\alpha/2} \times \frac{S}{\sqrt{n}} < \epsilon$

Statistical Model Checkers

- Ymer: CSL with bounded until **[Younes 05]**
- VESTA: PCTL and CSL **[Sen et al. 05]**
- MRMC: CSL and CSRL and extensions **[Katoen et al. 05]**
- APMC: PLTL and PCTL **[Peyronnet et al. 03]**
- PRISM: PCTL and CSL **[Kwiatkowska et al. 00]**

Objectives

- Design of statistical model checking.
  - For a large class of stochastic models.
  - With an expressive logic
- Interest:
  - Combining model checking and performance evaluation.

Outline

Discrete Event Stochastic Process

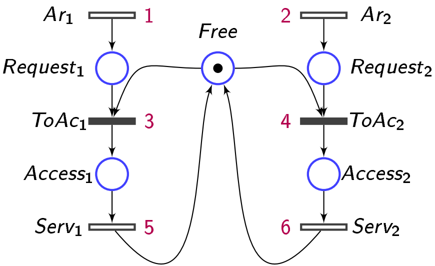
Definition

A Discrete Event Stochastic Process (DESP) is a tuple $\mathcal{D} = \langle S, \pi_0, E, Ind, enabled, target, delay, choice \rangle$.

- S : set of states
- π_0 : initial distribution
- E : set of events
- Ind : indicator function
- $enabled$: enabled events
- $target$: successor function
- $delay$: delay function
- $choice$: choice policy

A DESP Example

- S : GSPN markings
- π_0 : distribution of initial marking
- E : transitions of the GSPN.
- Ind : GSPN places.
- *enabled* : firing rule conditions
- *target* : firing rule execution
- *delay* : given by transitions distribution
- *choice* : time, priorities and weights



Shared Memory System

Discrete Event Stochastic Process (2)

- A *path* of a DESP is an infinite sequence $\sigma = s_0 \xrightarrow{e_0, \tau_0} s_1 \xrightarrow{e_1, \tau_1} \cdots$
- A *configuration* of a DESP is described as a triple $(s\,, \tau\,, sched)$
- Steps of an execution in a DESP
  1. Given a configuration $(s\,, \tau\,, sched)$, determine the set E' of enabled events with minimal delays
  2. With $choice(s, E')$ choose the event e to occur.
  3. Execute e, update the configuration of the DESP.

Synchronized Linear Hybrid Automaton

Definition

A *Synchronized Linear Hybrid Automaton* (LHA) is a tuple $\mathcal{A} = \langle E, L, \Lambda, init, final, X, flow, \rightarrow \rangle$.

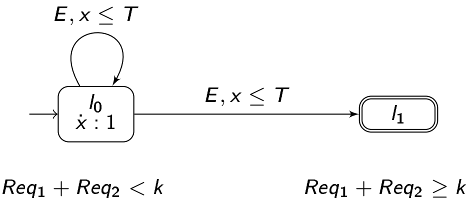
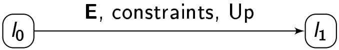


Figure: $TRUE \;\; \mathcal{U}^{[0,T]} \;\; (Req_1 + Req_2 \geq k)$

LHA Edges

- Synchronized edges



- Autonomous edges

Some properties in LHA

- Initial determinism
- Determinism on events
- Determinism on $\sharp$
- No $\sharp$-labelled loops

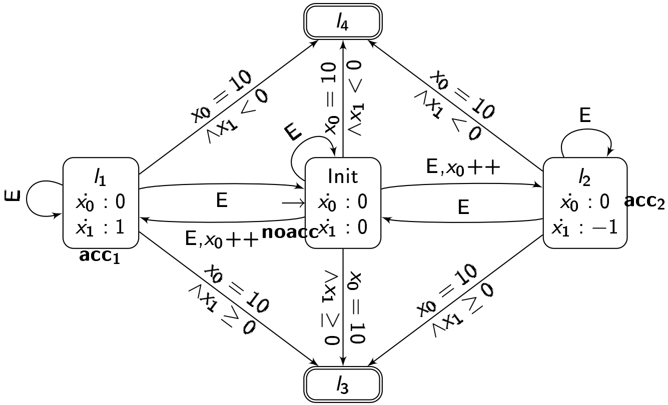
HASL expression

- Grammar:

$$Z ::= E(Y) \mid Z + Z \mid Z \times Z$$
$$Y ::= c \mid Y + Y \mid Y \times Y \mid Y/Y \mid last(y) \mid min(y) \mid max(y) \mid int(y) \mid avg(y)$$
$$y ::= c \mid x \mid y + y \mid y \times y \mid y/y$$

- Interest:
  - Model checking: $E[last(success)]$
  - Performance evaluation $E[max(x_1 - x_2)]$, $VAR[max(x_1 - x_2)]$
  - Conditional expectation $E[last(x_2 | x_2 > k)]$

An Example



$E[last(x_1)]$ difference of memory usage time

Outline

COSMOS: Concepts et Outils Statistiques pour les MOdels Stochastiques

- C++, Flex/Bison

- Inputs: A GSPN, a LHA, and an expression EXP.
- Output: Evaluation of EXP

- Events queue representation: Binary heap.
- Random numbers generation: BOOST librairie.

Outline

Tandem Queuing Network

		probability measure		exec-time		path avg exec-time		ratio
	T	prism	cosmos	prism	cosmos	prism	cosmos	$\frac{cosmos}{prism}$
$C=5$	20	0.337	0.335	20.2	30.9	0.00022	0.00052	2.38
	40	0.569	0.570	32.9	53.1	0.00036	0.00082	2.29
	60	0.718	0.719	40.3	53.5	0.00044	0.00101	2.29
	80	0.818	0.821	45.8	44.7	0.00050	0.00115	2.31
	100	0.883	0.885	49.4	32.3	0.00054	0.00120	2.24
	200	0.986	0.986	55.6	4.9	0.00060	0.00137	2.26
$C=7$	20	0.076	0.070	23.8	10.5	0.00026	0.00061	2.35
	40	0.152	0.145	44.8	36.2	0.00049	0.00110	2.26
	60	0.224	0.214	63.7	69.5	0.00069	0.00156	2.25
	80	0.289	0.277	81.8	105.3	0.00089	0.00198	2.23
	100	0.349	0.336	95.7	138.9	0.00104	0.00235	2.26
	200	0.578	0.561	157.7	250.4	0.00171	0.00385	2.25

$$\phi \equiv (\text{true } U^{[0,T]} \; Q_1\_\text{full})$$

Cyclic Polling System

	T	waiting-time measure prism	waiting-time measure cosmos	exec-time prism	exec-time cosmos	path avg exec-time prism	path avg exec-time cosmos	ratio $\frac{cosmos}{prism}$
$N=4$	5	0.403	0.402	138.3	691.3	0.00150	0.00471	3.13
	10	1.102	1.086	233.5	163.4	0.00254	0.00801	3.15
	20	2.557	2.510	427.10	191.90	0.00464	0.01454	3.13
	30	4.002	3.887	619.0	431.4	0.00673	0.02105	3.12
	40	5.466	5.313	824.2	780.4	0.00896	0.02758	3.07
	50	6.935	6.720	1040.1	1244.6	0.01130	0.03419	3.02
$N=8$	5	0.301	0.297	205.1	787.0	0.00223	0.00625	2.80
	10	0.929	0.905	350.6	220.3	0.00381	0.01006	2.64
	20	2.369	2.316	581.4	290.6	0.00632	0.01699	2.69
	30	3.861	3.760	827.0	717.6	0.00899	0.02376	2.64
	40	5.349	5.206	1073.4	1324.4	0.01166	0.03073	2.63
	50	6.837	6.656	1294.7	2082.8	0.01407	0.03733	2.65

Expected waiting time for Q_1 in $[0, T]$

Outline

Conclusion and Future Works

- An expressive logic.
- A large class of stochastic models.
- Model checking and performance evaluation.

Perpectives:

- Problematic of rare events.
- Application on real problems and complex systems
- Compiling approach for GSPN and LHA.