Carnegie Mellon

Carnegie Mellon SCHOOL OF COMPUTER SCIENCE

Statistical Model Checking for Rare Events

Paolo Zuliani
Computer Science Department
Carnegie Mellon University

CMACS
NSF Expeditions in Computing

1. Problem

Verification of Stochastic Systems

- Verification of stochastic system models via statistical model checking

- Temporal logic specification:
"in the next 20 min. the system is unavailable for 1sec"

- If Φ = "in the next 20 min. the system is unavailable for 1 sec."

Probability (Φ) = ?

- Equivalently: A biased coin (Bernoulli random variable)
- Prob (Heads) = *p*   Prob (Tails) = *1-p*
  - *p* is unknown
- Question: What is *p*?
- A solution: flip the coin a number of times, collect the outcomes, and use statistical estimation

2. Statistical Model Checking

Key idea

(Haakan Younes, 2001)

- System behavior w.r.t. property Φ can be modeled by a Bernoulli random variable of parameter *p*:
  - System satisfies Φ with (unknown) probability *p*
- Question: What is *p?*
- Draw a sample of system simulations and use:
  - Statistical estimation: returns "*p* in interval (a,b)" with high probability

3. Temporal Logic

- A formal notation for expressing properties about the temporal evolution of a system
- Example: "*within 10 time units the system will shut down and the shutdown signal will be ON until then*"

`shutdown_ON` $\mathbf{U}^{10}$ `sysdown`

- Example: "*it is not the case that in the future 25 time units the system is globally down for one time unit*"

$\neg(\mathbf{F}^{25}\,\mathbf{G}^{1}$ `sysdown`$)$

4. Bounded Linear Temporal Logic

- Extension of LTL with time bounds on temporal operators.
  - No neXt operator
- Let $\sigma = (s_0, t_0), (s_1, t_1), \ldots$ be a trace of the model
  - the system stays in state s_i for time t_i
- The semantics of BLTL for trace σ starting at state k (σ^k):
  - $\sigma^k \models ap$ iff atomic proposition ap true in state s_k
  - $\sigma^k \models \Phi_1 \vee \Phi_2$ iff $\sigma^k \models \Phi_1$ or $\sigma^k \models \Phi_2$
  - $\sigma^k \models \neg\Phi$ iff $\sigma^k \models \Phi$ does not hold
  - $\sigma^k \models \Phi_1\, \mathbf{U}^t\, \Phi_2$ iff there exists natural i such that
    1) $\sigma^{k+i} \models \Phi_2$
    2) $\Sigma_{j<i}\, t_{k+j} \leq t$
    3) for each $0 \leq j < i$, $\sigma^{k+j} \models \Phi_1$

"within time t, Φ_2 will be true and Φ_1 will hold until then"

- In particular, $\mathbf{F}^t\,\Phi = true\ \mathbf{U}^t\,\Phi$, $\mathbf{G}^t\,\Phi = \neg\mathbf{F}^t\,\neg\Phi$

- *Definition:* The time bound of Φ:
  - $\#(ap) = 0$
  - $\#(\neg\Phi) = \#(\Phi)$
  - $\#(\Phi_1 \vee \Phi_2) = \max(\#(\Phi_1), \#(\Phi_2))$
  - $\#(\Phi_1\, \mathbf{U}^t\, \Phi_2) = t + \max(\#(\Phi_1), \#(\Phi_2))$
- *Lemma:* "Bounded simulations suffice"

Let Φ be a BLTL *property, and k≥0. For any two infinite traces ρ, σ such that* ρ^k *and* σ^k *"equal up to time* $\#(\Phi)$*" we have*

$$\rho^k \models \Phi \quad iff \quad \sigma^k \models \Phi$$

5. Rare Events

- Estimate Prob(X≥*t*) = *p*, when *p* is *small* (say 10^{-9})
- Standard (Crude) Monte Carlo: generate *K* i.i.d. samples of X; return the estimator e_K

$$e_K = \frac{1}{K}\sum_{i=1}^{K} I(X_i \geqslant t) = \frac{k_t}{K}$$

- Prob ($e_K \to p$) = 1 for $K \to \infty$ (strong law LN)
- Relative Error (RE) = $\dfrac{\sqrt{\mathrm{var}[e_K]}}{\mathrm{E}[e_K]} = \dfrac{\sqrt{p(1-p)}}{p\sqrt{K}}$
- More accuracy → more samples
- Want confidence interval of relative accuracy δ and coverage probability *c,* i.e., estimate e_K must satisfy:

$$\mathrm{Prob}(|\, e_K - p\,| < \delta \cdot p) \geq c$$

- From the CLT, a 99% (approximate) confidence interval of relative accuracy δ needs about

$$K \approx \frac{1-p}{p\delta^2} \text{ samples } \quad (\to \mathrm{Prob}(|\, e_K - p\,| < \delta p) \approx 0.99)$$

- Example: $p = 10^{-9}$ and $\delta = 10^{-2}$ (*ie*, 1% relative accuracy) we need about $\mathbf{10^{13}}$ **samples**!!

6. Importance Sampling

$$\begin{aligned} p &= E[I(X \geqslant t)] \\ &= \int I(x \geqslant t) f(x)\, dx \\ &= \int I(x \geqslant t) \boxed{\frac{f(x)}{f_*(x)}} f_*(x)\, dx \\ &= \int I(x \geqslant t) W(x) f_*(x)\, dx \\ &= E_*[I(X \geqslant t) W(X)] \end{aligned}$$

where *f* is the density of *X*.

- The Importance Sampling estimator is:

$$p_K = \frac{1}{K}\sum_{i=1}^{K} I(X_i \geqslant t) W(X_i), \qquad \boxed{X_i \sim f_*}$$

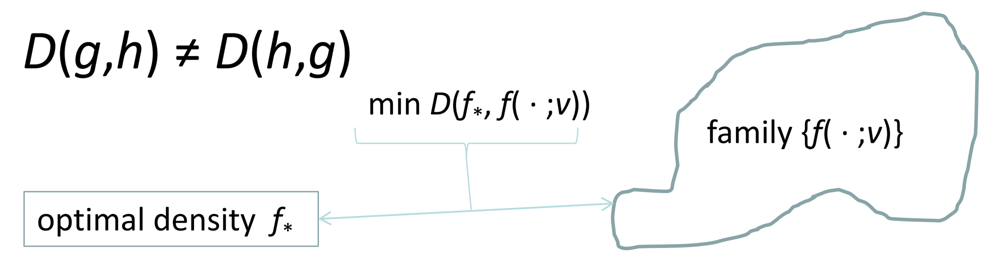
- Need to choose a "good" biasing density (low variance)
- Optimal density: $f_*(x) = \dfrac{I(x \geq t)\, f(x)}{p}$
- Idea: search for a "good density" in a parameterized family

7. Cross-Entropy

- The cross-entropy of densities *g*, *h* is

$$D(g,h) = E_g\left[\ln \frac{g(X)}{h(X)}\right] = \int g(x) \ln g(x) dx - \int g(x) \ln h(x) dx$$

  - $D(g,h) \geq 0$ (= 0 IFF $g = h$)
  - $D(g,h) \neq D(h,g)$



- The Cross-Entropy Method has two steps

1. find $v_* = \underset{v}{\arg\min}\, D(f_*(\cdot),\, f(\cdot\,; v))$
2. run importance sampling with biasing density $f(\cdot\,; v_*)$

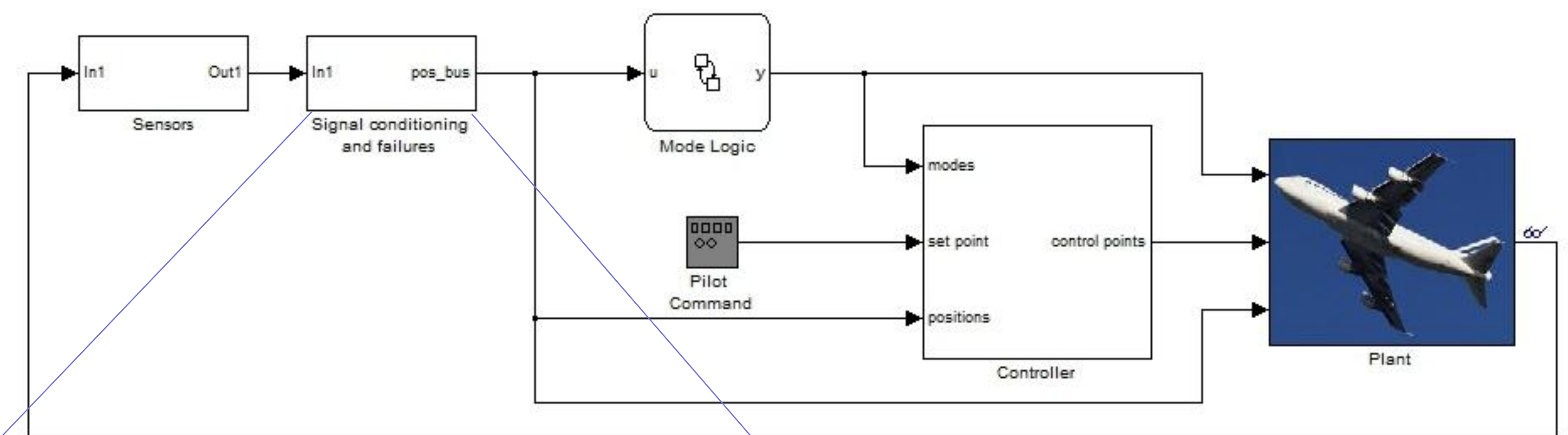
- We can estimate v_* by Monte Carlo simulation

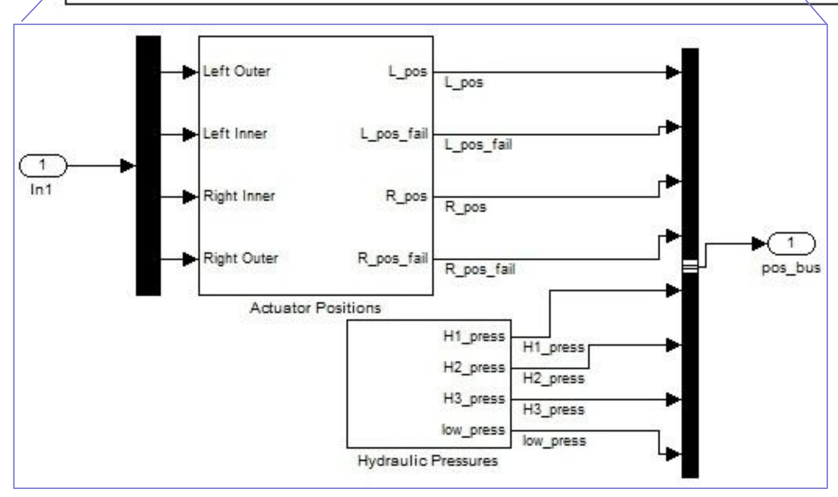
$$\bar{v}_* = \frac{\sum_{i=1}^{K} [I(X_i \geq t) W(X_i; u, w) X_i]}{\sum_{i=1}^{K} [I(X_i \geq t) W(X_i; u, w)]}$$

where $X_1, \ldots, X_K$ samples iid as $f(\cdot\,; w)$

8. Applications

- Fault-tolerant controller for an aircraft elevator system





- The three hydraulic circuits can independently fail
- What is the probability that in the next 25s for 1s no control input is passed to the elevators?

Prob($\mathbf{F}^{25}\,\mathbf{G}^{1}$ (H1_*fail* or H3_*fail*) and H2_*fail*)=?

	Samples	Estimate	Relative error	Time (h)
Samples	Step 1: 100 Step 2: 1,000	1.58 x 10^{-14}	0.58	0.23
	Step 1: 1,000 Step 2: 10,000	8.54 x 10^{-14}	0.24	2.45
	Step 1: 10,000 Step 2: 100,000	8.11 x 10^{-14}	0.17	23.9

9. References

- P. Zuliani, A. Platzer, E. M. Clarke. *Bayesian Statistical Model Checking with Application to Stateflow/Simulink Verification*. In HSCC 2010, pages 243-252.
- E. M. Clarke and P. Zuliani. *Statistical Model Checking for Cyber-Physical Systems*. In ATVA 2011, LNCS 6996, pages 1-12.
- P. Zuliani, C. Baier, E.M. Clarke. *Rare-Event Verification for Stochastic Hybrid Systems*. Submitted