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 \( \Phi \) = “in the next 20 min. the system is unavailable for 1sec.”
  - Probability (\( \Phi \)) = ?
  - 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 Yoones, 2001)
- System behavior w.r.t. property \( \Phi \) can be modeled by a Bernoulli random variable of parameter \( p \)
- System satisfies \( \Phi \) 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 \( \text{ON} \) \( U \) 10 sybsdown
- Example: “it is not the case that in the future 25 time units the system is globally down for one time unit”
  - \( \neg (F^{25} G^1 \text{sybsdown}) \)

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 BTLT for trace \( \sigma \) starting at state \( s_k \) (\( k \geq 0 \)):
  - \( s_k \models \alpha \iff \) true in state \( s_k \)
  - \( s_k \models \neg \alpha \iff \) false in state \( s_k \)
  - \( s_k \models \alpha_1 \lor \alpha_2 \iff \) true or false in state \( s_k \)
  - \( s_k \models \alpha \rightarrow \beta \iff \) true \( \Rightarrow \) false in state \( s_k \)
  - \( s_k \models [\alpha ]_\beta \iff \) false until \( t \) in state \( s_k \)
  - \( s_k \models (\alpha . \beta) \alpha \iff \) true \( \Rightarrow \) false \( \Rightarrow \) false in state \( s_k \)

5. Rare Events

- Estimate \( \text{Pr}(X_{25}) = p \), when \( p \) is small (say \( 10^{-9} \))
- Standard (Crude) Monte Carlo: generate \( K \) i.i.d. samples of \( X \); return the estimator \( e_x \)
  - \( e_x = \frac{1}{K} \sum_{i=1}^{K} I(X_i \geq t) = \frac{h_k}{k} \)
- \( \text{Prob}(e_x \rightarrow p) = 1 \) for \( K \rightarrow \infty \) (strong law LN)
- Relative Error (RE) = \( \frac{\text{var}(e_x)}{E(e_x)} = \sqrt{\frac{p(1-p)}{p_k K}} \)
- More accuracy \( \rightarrow \) more samples
- Want confidence interval of relative accuracy \( \delta \) and coverage probability \( c \), i.e., estimate \( e_x \) must satisfy:
  - \( \text{Pr}(\{ e_x - p | < \delta \} ) \geq c \)
- From the CI, a 99% (approximate) confidence interval of relative accuracy \( \delta \) needs about
  - \( K \approx \frac{1-p}{p^2} \) samples \( \Rightarrow \) \text{Prob}(\{ e_x - p | < \delta \}) \approx 0.99 \)
- Example: \( p = 10^{-9} \) and \( \delta = 10^{-2} \) (ie, 1% relative accuracy) we need about \( 10^{14} \) samples!!

6. Importance Sampling

\[ p = E[I(X \geq t)] \]
\[ = \int I(x \geq t)f(x)\,dx \]
\[ = \int I(x \geq t)\frac{f(x)}{f_0(x)}f_0(x)\,dx \]
\[ = \int I(x \geq t)W(x)f_0(x)\,dx \]
\[ = E[I(X \geq t)|W(x)] \]

where \( f \) is the density of \( X \).
- The Importance Sampling estimator is:
  - \( p_k = \frac{1}{K} \sum_{i=1}^{K} I(X_i \geq t)W(X_i), \quad X_i \sim f_0 \)
- Need to choose a “good” biasing density (low variance)
- Optimal density: \( f_0(x) = \frac{I(x \geq t)f(x)}{p} \)
- Idea: search for a “good” density in a parameterized family

7. Cross-Entropy

- The cross-entropy of densities \( g, h \) is
  \[ D(g, h) = E_x \left[ \ln g(\frac{x}{h}(x)) \right] = \int g(x) \ln g(x)dx - \int g(x) \ln h(x)dx \]
- \( D(g, h) \geq 0 \)
- We can estimate \( v_x \) by Monte Carlo simulation
  \[ v_x = \frac{d}{d \theta} \frac{1}{K} \sum_{i=1}^{K} I(X_i \geq t)W(X_i; u, w) \]
  where \( X_i, \ldots, X_K \) 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?

\[ \text{Prob}(F^{25} G^1 (H_1 \_\text{fail} \lor H_2 \_\text{fail}) \lor H_2 \_\text{fail}) = ? \]

<table>
<thead>
<tr>
<th>Estimate</th>
<th>Relative error</th>
<th>Time (h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.58 x 10^{-14}</td>
<td>0.58</td>
<td>0.23</td>
</tr>
<tr>
<td>8.54 x 10^{-14}</td>
<td>0.24</td>
<td>2.45</td>
</tr>
<tr>
<td>8.11 x 10^{-14}</td>
<td>0.17</td>
<td>23.9</td>
</tr>
</tbody>
</table>

9. References

- P. Zuliani, C. Baier, E.M. Clarke. Rare-Event Verification for Stochastic Hybrid Systems. Submitted