Statistical Model Checking

Paolo Zuliani

Joint work with
Edmund M. Clarke, James R. Faeder*,
Haijun Gong, Anvesh Komuravelli,
André Platzer, Ying-Chih Wang

Computer Science Department, CMU
*Department of Computational Biology, Pitt
Problem

Verification of Stochastic Systems

- Uncertainties in
  - the system environment,
  - modeling a fault,
  - biological signaling pathways,
  - circuit fabrication (process variability)

- Transient property specification:
  - “what is the probability that the system shuts down within 0.1 ms”?

- If $\Phi = \text{“system shuts down within 0.1 ms”}$
  $\text{Prob}(\Phi) = ?$
Equivalently

- A biased coin (Bernoulli random variable):
  - Prob (Head) = \( p \)   Prob (Tail) = \( 1-p \)
  - \( p \) is unknown

- Question: What is \( p \)?

- A solution: flip the coin a number of times, collect the outcomes, and use a statistical estimation technique.
Motivation

- **State Space Exploration** infeasible for large systems
  - Symbolic MC with OBDDs scales to $10^{300}$ states
  - Scalability depends on the structure of the system
- **Pros: Simulation** is feasible for **many more** systems
  - Often easier to simulate a complex system than to build the transition relation for it
- **Pros: Easier to parallelize**
- **Cons: Answers may be wrong**
  - But error probability can be bounded
- **Cons: Simulation is incomplete**
Key idea

- System behavior w.r.t. a (fixed) 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
Bounded Linear Temporal Logic

- Bounded Linear Temporal Logic (BLTL): Extension of LTL with time bounds on temporal operators.

- Let $\sigma = (s_0, t_0), (s_1, t_1), \ldots$ be an execution of the model
  - along states $s_0, s_1, \ldots$
  - the system stays in state $s_i$ for time $t_i$
  - divergence of time: $\Sigma_i t_i$ diverges (i.e., non-zeno)

- $\sigma^i$: Execution trace starting at state $i$.

- A model for simulation traces (e.g. Stateflow/Simulink)
Semantics of BLTL

The semantics of BLTL for a trace $\sigma^k$:

- $\sigma^k \models ap$ iff atomic proposition $ap$ true in state $s_k$
- $\sigma^k \models \Phi_1 \lor \Phi_2$ 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
- $\sigma^k \models \Phi_1 \mathcal{U}^t \Phi_2$ 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 $t$, $\Phi_2$ will be true and $\Phi_1$ will hold until then"

- In particular, $\mathcal{F}^t \Phi = true \mathcal{U}^t \Phi$, $\mathcal{G}^t \Phi = \neg \mathcal{F}^t \neg \Phi$
Simulation traces are finite: is $\sigma \models \Phi$ well defined?

**Definition:** The time bound of $\Phi$:

- $(ap) = 0$
- $\#(\neg \Phi) = \#(\Phi)$
- $\#(\Phi_1 \lor \Phi_2) = \max(\#(\Phi_1), \#(\Phi_2))$
- $\#(\Phi_1 \mathcal{U}^t \Phi_2) = t + \max(\#(\Phi_1), \#(\Phi_2))$

**Lemma:** “Bounded simulations suffice”

Let $\Phi$ be a BLTL property, and $k \geq 0$. For any two infinite traces $\rho, \sigma$ such that $\rho^k$ and $\sigma^k$ “equal up to time $\#(\Phi)$” we have

$$\rho^k \models \Phi \iff \sigma^k \models \Phi$$
Three ingredients:

1. **Prior distribution**
   - Models our initial (a priori) uncertainty/belief about parameters (what is $P(\theta)$?)

2. **Likelihood function**
   - Describes the distribution of data (e.g., a sequence of heads/tails), given a specific parameter value

3. **Bayes Theorem**
   - Revises uncertainty upon experimental data - compute $P(\theta \mid \text{data})$
Sequential Bayesian Statistical MC

- Suppose $\mathcal{M}$ satisfies $\phi$ with (unknown) probability $p$
  - $p$ is given by a random variable (defined on $[0,1]$) with density $g$
  - $g$ represents the prior belief that $\mathcal{M}$ satisfies $\phi$
- Generate independent and identically distributed (iid) sample (simulation) traces.
- $x_i$: the $i^{th}$ sample trace $\sigma$ satisfies $\phi$
  - $x_i = 1$ iff $\sigma_i \models \phi$
  - $x_i = 0$ iff $\sigma_i \not\models \phi$
- Then, $x_i$ will be a Bernoulli trial with conditional density (likelihood function)
  \[
  f(x_i/u) = u^x(1 - u)^{1-x_i}
  \]
Beta Prior

- Prior $g$ is Beta of parameters $\alpha>0, \beta>0$

\[ g(u, \alpha, \beta) = \frac{1}{B(\alpha, \beta)} u^{\alpha-1} (1 - u)^{\beta-1} \quad \forall u \in [0, 1] \]

\[ B(\alpha, \beta) = \int_0^1 t^{\alpha-1} (1 - t)^{\beta-1} \, dt \]

- $F(\cdot, \cdot)(\cdot)$ is the Beta distribution function (i.e., $\text{Prob}(X \leq u)$)

\[ F(\alpha, \beta)(u) = \int_0^u g(t, \alpha, \beta) \, dt \]
Bayesian Interval Estimation - I

- Estimating the (unknown) probability \( p \) that "system \( \models \Phi \)"
- Recall: system is modeled as a Bernoulli of parameter \( p \)
- **Bayes’ Theorem** (for conditional iid Bernoulli samples)

\[
f(u \mid x_1, \ldots, x_n) = \frac{f(x_1 \mid u) \cdots f(x_n \mid u)g(u)}{\int_0^1 f(x_1 \mid v) \cdots f(x_n \mid v)g(v) \, dv}
\]

- We thus have the **posterior distribution**
- So we can use the **mean of the posterior** to estimate \( p \)
  - mean is a posterior Bayes estimator for \( p \) (it minimizes the integrated risk over the parameter space, under a quadratic loss)
By integrating the posterior we get Bayesian intervals for $p$

Fix a coverage $\frac{1}{2} < c < 1$. Any interval $(t_0, t_1)$ such that

$$\int_{t_0}^{t_1} f(u \mid x_1, \ldots, x_n) \, du = c$$

is called a 100c percent Bayesian Interval Estimate of $p$

An optimal interval minimizes $t_1 - t_0$: difficult in general

Our approach:
- fix a half-interval width $\delta$
- Continue sampling until the posterior probability of an interval of width $2\delta$ containing the posterior mean exceeds coverage $c$
Computing the posterior probability of an interval is easy

Suppose \( n \) Bernoulli samples (with \( x \leq n \) successes) and prior Beta(\( \alpha, \beta \))

\[
P(t_0 < p < t_1 | x_1, \ldots, x_n) = \int_{t_0}^{t_1} f(u | x_1, \ldots, x_n) \, du
\]

\[
= F(x+\alpha, n-x+\beta)(t_1) - F(x+\alpha, n-x+\beta)(t_0)
\]

Efficient numerical implementations (Matlab, GSL, etc)
Bayesian Interval Estimation - IV

prior is beta(\(\alpha=4,\beta=5\))

posterior density after 1000 samples and 900 “successes” is beta(\(\alpha=904,\beta=105\))

posterior mean = 0.8959
Bayesian Interval Estimation - V

**Require**: BLTL property $\Phi$, interval-width $\delta$, coverage $c$, prior beta parameters $\alpha, \beta$

$n := 0$ \hspace{1cm} \{number of traces drawn so far\}

$x := 0$ \hspace{1cm} \{number of traces satisfying so far\}

repeat

$\sigma :=$ draw a sample trace of the system (iid)

$n := n + 1$

if $\sigma \models \Phi$ then

$x := x + 1$

endif

mean $= (x + \alpha)/(n + \alpha + \beta)$

$(t_0, t_1) = (\text{mean} - \delta, \text{mean} + \delta)$

$I := \text{PosteriorProbability} (t_0, t_1, n, x, \alpha, \beta)$

until $(I > c)$

return $(t_0, t_1)$, mean
Recall the algorithm outputs the interval \((t_0, t_1)\).

Define the null hypothesis

\[ H_0: t_0 < p < t_1 \]

**Theorem (Error bound).** When the Bayesian estimation algorithm (using coverage \(\frac{1}{2} < c < 1\)) stops – we have

\[
\text{Prob ("accept } H_0 \text{" | } H_1) \leq \frac{(1/c - 1)\pi_0}{1-\pi_0}
\]

\[
\text{Prob ("reject } H_0 \text{" | } H_0) \leq \frac{(1/c - 1)\pi_0}{1-\pi_0}
\]

\(\pi_0\) is the prior probability of \(H_0\).
Example: Fuel Control System

The Stateflow/Simulink model
Fuel Control System

- Ratio between **air mass flow** rate and **fuel mass flow** rate
  - Stoichiometric ratio is 14.6

- Senses amount of oxygen in exhaust gas, pressure, engine speed and throttle to **compute correct fuel rate**.
  - Single sensor faults are compensated by switching to a higher oxygen content mixture
  - Multiple sensor faults force engine shutdown

- Probabilistic behavior because of **random faults**
  - In the EGO (oxygen), pressure and speed sensors
  - Faults modeled by three independent Poisson processes
  - We did not change the speed or throttle inputs
Verification

- We want to estimate the probability that
  \[ M, \text{FaultRate} \models \neg F^{100} G^1(\text{FuelFlowRate} = 0) \]
- “It is not the case that within 100 seconds, \text{FuelFlowRate} is zero for 1 second”
- We use various values of \text{FaultRate} for each of the three sensors in the model
- Uniform prior
Verification

- Half-width $\delta = 0.01$
- Several values of coverage probability $c$
- Posterior mean: add/subtract $\delta$ to get Bayesian interval

<table>
<thead>
<tr>
<th>Fault rates</th>
<th>Interval coverage $c$</th>
</tr>
</thead>
<tbody>
<tr>
<td>[3 7 8]</td>
<td>.3603 .3559 .3558 .3563</td>
</tr>
<tr>
<td>[10 8 9]</td>
<td>.8534 .8518 .8528 .8534</td>
</tr>
<tr>
<td>[20 10 20]</td>
<td>.9764 .9784 .9840 .9779</td>
</tr>
<tr>
<td>[30 30 30]</td>
<td>.9913 .9933 .9956 .9971</td>
</tr>
</tbody>
</table>
## Verification

- **Number of samples**
- **Comparison with Chernoff-Hoeffding bound**

\[
Pr \left( |X - p| \geq \delta \right) \leq \exp(-2n\delta^2)
\]

where \( X = 1/n \sum X_i \), \( E[X_i] = p \)

### Fault rates

<table>
<thead>
<tr>
<th>Fault rates</th>
<th>[3 7 8]</th>
<th>[10 8 9]</th>
<th>[20 10 20]</th>
<th>[30 30 30]</th>
<th>Chernoff bound</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6,234</td>
<td>3,381</td>
<td>592</td>
<td>113</td>
<td>11,513</td>
</tr>
<tr>
<td></td>
<td>8,802</td>
<td>4,844</td>
<td>786</td>
<td>148</td>
<td>14,979</td>
</tr>
<tr>
<td></td>
<td>15,205</td>
<td>8,331</td>
<td>1,121</td>
<td>227</td>
<td>23,026</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2,583</td>
<td></td>
<td>34,539</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interval coverage</th>
<th>.9</th>
<th>.95</th>
<th>.99</th>
<th>.999</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6,234</td>
<td>8,802</td>
<td>15,205</td>
<td>24,830</td>
</tr>
<tr>
<td></td>
<td>3,381</td>
<td>4,844</td>
<td>8,331</td>
<td>13,569</td>
</tr>
<tr>
<td></td>
<td>592</td>
<td>786</td>
<td>1,121</td>
<td>2,583</td>
</tr>
<tr>
<td></td>
<td>113</td>
<td>148</td>
<td>227</td>
<td>341</td>
</tr>
</tbody>
</table>

about 17hrs on 2.4GHz Pentium 4
Example: OP Amplifier

Process variability: uncertainties in the fabrication process
OP amp: BLTL Specifications

- Properties are measured directly from simulation traces
- Predicates over simulation traces
  - e.g. Swing Range: \( \text{Max}(V_{\text{out}}) > 1.0\text{V AND Min}(V_{\text{out}}) < 0.2\text{V} \)
- Using BLTL specifications
  - In most cases, can be translated directly from definitions
  - e.g. Swing Range:
    - \( F^{[100\mu s]}(V_{\text{out}} < 0.2) \text{ AND } F^{[100\mu s]}(V_{\text{out}} > 1.0) \)
    - “within 100\(\mu\)s \(V_{\text{out}}\) will eventually be greater than 1V and smaller than 0.2V”
  - 100\(\mu\)s: end time of transient simulation
  - Note: unit in \textit{bound} is only for readability
### OP amp: BLTL Specifications

<table>
<thead>
<tr>
<th>Specifications</th>
<th>BLTL Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Input Offset Voltage</td>
<td>$&lt; 1 \text{ mV}$</td>
</tr>
<tr>
<td></td>
<td>$F^{[100\mu s]}(V_{out} = .6)$ AND $G^{[100\mu s]}((V_{out} = .6) \rightarrow (</td>
</tr>
<tr>
<td>2 Output Swing Range</td>
<td>$.2 \text{ V to } 1.0 \text{ V}$</td>
</tr>
<tr>
<td></td>
<td>$F^{[100\mu s]}(V_{out} &lt; .2)$ AND $F^{[100\mu s]}(V_{out} &gt; 1.0)$</td>
</tr>
<tr>
<td>3 Slew Rate</td>
<td>$&gt; 25 \text{ V/}\mu\text{Sec}$</td>
</tr>
<tr>
<td></td>
<td>$G^{[100\mu s]}((V_{out} &gt; 1.0 \text{ AND } V_{in} &gt; .65) \rightarrow F^{[0.032\mu s]}(V_{out} &lt; .2)) \text{ AND }$</td>
</tr>
<tr>
<td></td>
<td>$(V_{out} &lt; .2 \text{ AND } V_{in} &lt; .55) \rightarrow F^{[0.032\mu s]}(V_{out} &lt; 1.0))$</td>
</tr>
</tbody>
</table>

More properties and experiments in our ASP-DAC 2011 paper
- $p$ is small (say $10^{-9}$)
- A 99% (approximate) confidence interval of relative accuracy $\delta$ needs about
  \[
  \frac{(1-p)}{p\delta^2}
  \] samples
- Examples:
  - $p = 10^{-9}$ and $\delta = 10^{-2}$ (ie, 1% accuracy) we need about $10^{13}$ samples!!
  - Bayesian estimation requires about $6 \times 10^6$ samples with $p=10^{-4}$ and $\delta = 10^{-1}$
The fundamental **Importance Sampling** identity

\[
p_t = E[I(X \geq t)]
\]

\[
= \int I(x \geq t) f(x) \, dx
\]

\[
= \int I(x \geq t) \frac{f(x)}{f_*(x)} f_*(x) \, dx
\]

\[
= \int I(x \geq t) W(x) f_*(x) \, dx
\]

\[
= E_*[I(X \geq t)W(X)]
\]
Estimate \( p_t = E[X > t] \). A sample \( X_1, \ldots, X_K \) iid as \( X \)

\[
\hat{p}_t = \frac{1}{K} \sum_{i=1}^{K} I(X_i \geq t) = \frac{k_t}{K}, \quad X_i \sim f
\]

Define a biasing density \( f_* \)

\[
\hat{p}_t = \frac{1}{K} \sum_{i=1}^{K} I(X_i \geq t) W(X_i), \quad X_i \sim f_*
\]

where \( W(x) = f(x)/f_*(x) \) is the likelihood ratio
Importance Sampling: Toy Example

- Suppose $X$ is Poisson with parameter $\lambda$
  - $\text{Prob}(X_t = k) = (1/k!)(\lambda t)^k \exp(-\lambda t)$
- Then $\text{Prob}(X_t \geq 1) = 1 - \exp(-\lambda t)$
- Say $t = 100$ and $\lambda = 1/3 \times 10^{-11}$
  - $\rho_t = \text{Prob}(X_t \geq 1) \approx 3.333 \times 10^{-10}$
  - Rare event!
Importance Sampling: Toy Example

- Define the **biasing density** a Poisson with parameter $\mu$ much larger than $\lambda$.

- The likelihood ratio is

$$W(k) = (\lambda t)^k (\mu t)^{-k} \exp(-\mu t) \exp(\lambda t) = (\lambda/\mu)^k \exp(t(\mu-\lambda))$$

- Draw $N$ samples $k_1...k_N$ from the biasing density

- **Importance sampling estimate** is

$$e_t = 1/N \sum_i I(k_i \geq 1) W(k_i)$$
Importance Sampling: Toy Example

- With $N = 100$ samples and $\mu = 1/90$ we get an estimate
  
  $$e_t = 3.2808 \times 10^{-10}$$

- Recall the “unbiased” system has $\lambda = 1/3 \times 10^{-11}$

- The (unknown) true probability is about $3.333 \times 10^{-10}$

- Try standard MC estimation …
- Tackling the incompleteness of simulation
- **Theorem** (Undecidability of image computation)

Platzer and Clarke, HSCC 2007
Bad news, but …

**Theorem.** (Platzer and Clarke, 07)
If \( \text{Prob}(\|\varphi'\|_\infty > b) \to 0 \) when \( b \to \infty \), then image computation can be performed with arbitrarily high probability by evaluating \( \varphi \) on sufficiently dense grid.

**Idea:**
- given a simulation trace, “compute the probability that we have missed a (bad) state between two sample points”
- Bound the overall error probability *a priori* (combining bounds on \( \|\varphi'\|_\infty \) and the statistical test/estimation)
Thank You!