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 Φ = “system shuts down within 0.1ms”

$$\text{Prob}(\Phi) = ?$$

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

Statistical Model Checking

Key idea

- System behavior w.r.t. a (fixed) 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

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)

- σ^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 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
- $\sigma^k \models \Phi_1 \, \mathcal{U}^t \, \Phi_2$ 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, Φ_2 will be true and Φ_1 will hold until then"

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

Semantics of BLTL (cont'd)

- Simulation traces are finite: is $\sigma \models \Phi$ well defined?

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

- *Lemma:* "Bounded simulations suffice"

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

$$\rho^k \models \Phi \quad \text{iff} \quad \sigma^k \models \Phi$$

Bayesian Statistics

Three ingredients:

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

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(θ | *data*)

Sequential Bayesian Statistical MC

- Suppose $\mathcal{M}$ satisfies ϕ 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 ϕ
- Generate independent and identically distributed (iid) sample (simulation) traces.
- x_i: the i^{th} sample trace σ satisfies ϕ
  - $x_i = 1$ 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)

$$f(x_i|u) = u^{x_i}(1 - u)^{1-x_i}$$

Beta Prior

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

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

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

- $F_{(\cdot,\cdot)}(\cdot)$ is the Beta distribution function (i.e., Prob(X ≤ 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)

Bayesian Interval Estimation - II

- By integrating the posterior we get Bayesian intervals for *p*
- Fix a coverage ½ < *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 δ
  - Continue sampling until the posterior probability of an interval of width 2δ containing the posterior mean exceeds coverage c

Bayesian Interval Estimation - III

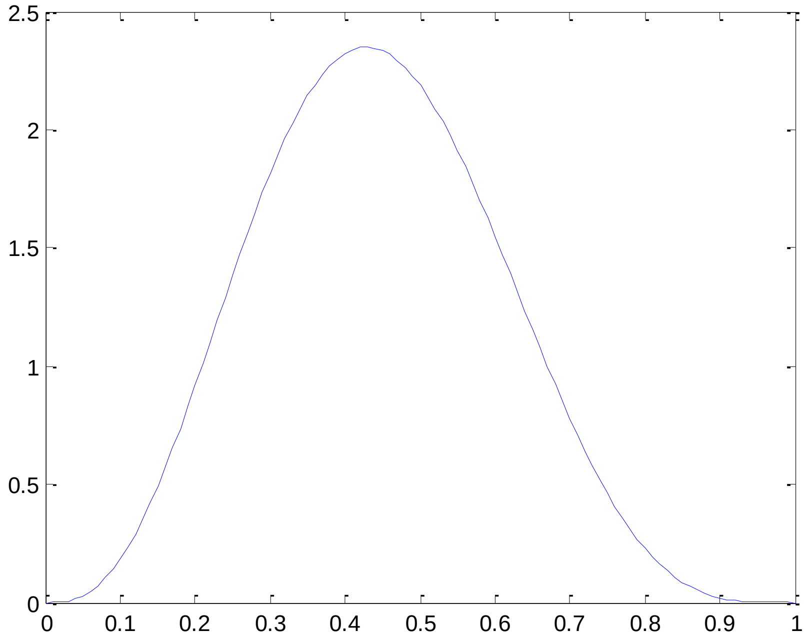
- Computing the posterior probability of an interval is easy

- Suppose *n* Bernoulli samples (with *x*≤*n* successes) and prior Beta(*α*,*β*)

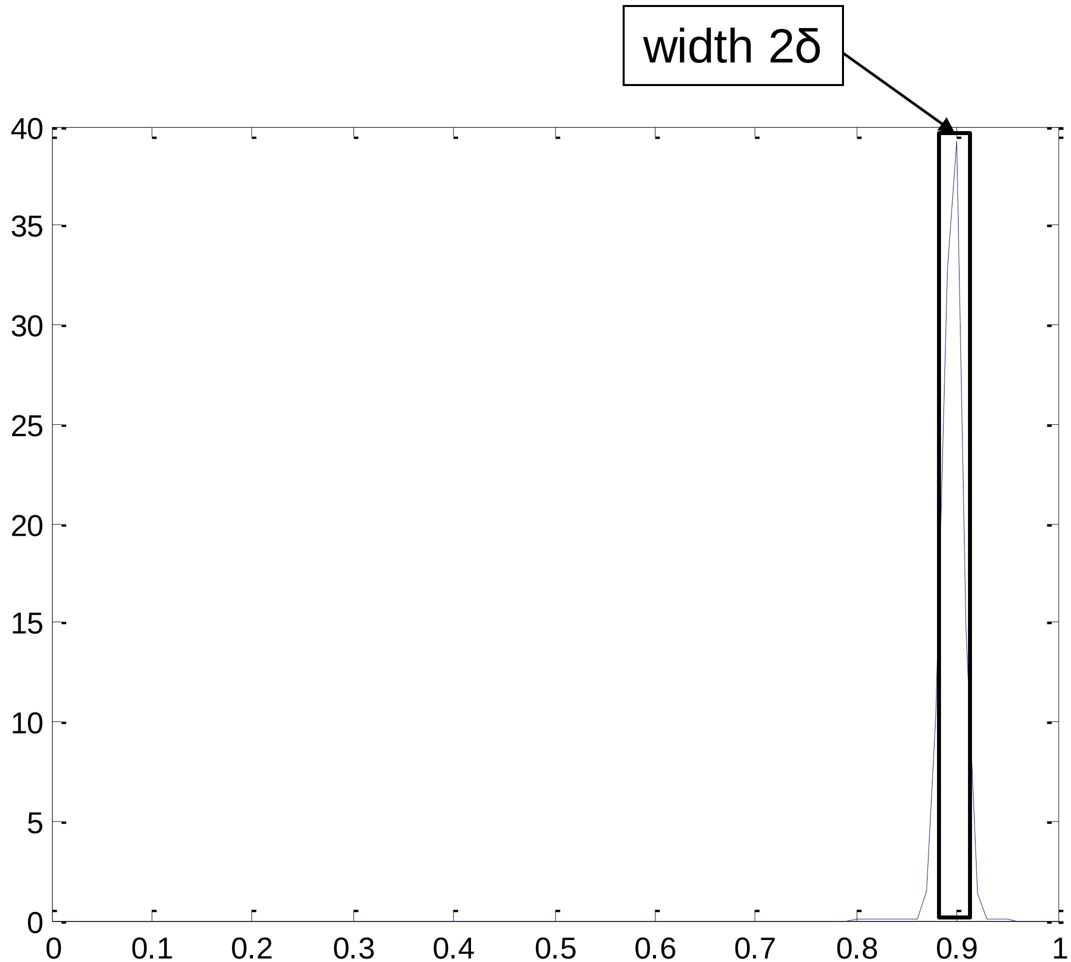
$$\begin{aligned} \mathrm{P}(t_0 < p < t_1 | x_1, \ldots, x_n) &= \int_{t_0}^{t_1} f(u \mid x_1, \ldots, x_n)\, du \\ &= \boxed{F_{(x+\alpha, n-x+\beta)}(t_1) - F_{(x+\alpha, n-x+\beta)}(t_0)} \end{aligned}$$

- Efficient numerical implementations (Matlab, GSL, *etc*)

Bayesian Interval Estimation - IV



prior is beta(α=4,β=5)



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

posterior mean = 0.8959

Bayesian Interval Estimation - V

Require: BLTL *property* Φ, *interval-width* δ, *coverage* c, *prior* beta parameters α,β

$n := 0$ {number of traces drawn so far}

$x := 0$ {number of traces satisfying so far}

repeat

  σ := 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) = (mean-δ, mean+δ)

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

until $(\mathcal{I} > c)$

return (t_0,t_1), mean

Bayesian Interval Estimation - VI

- 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

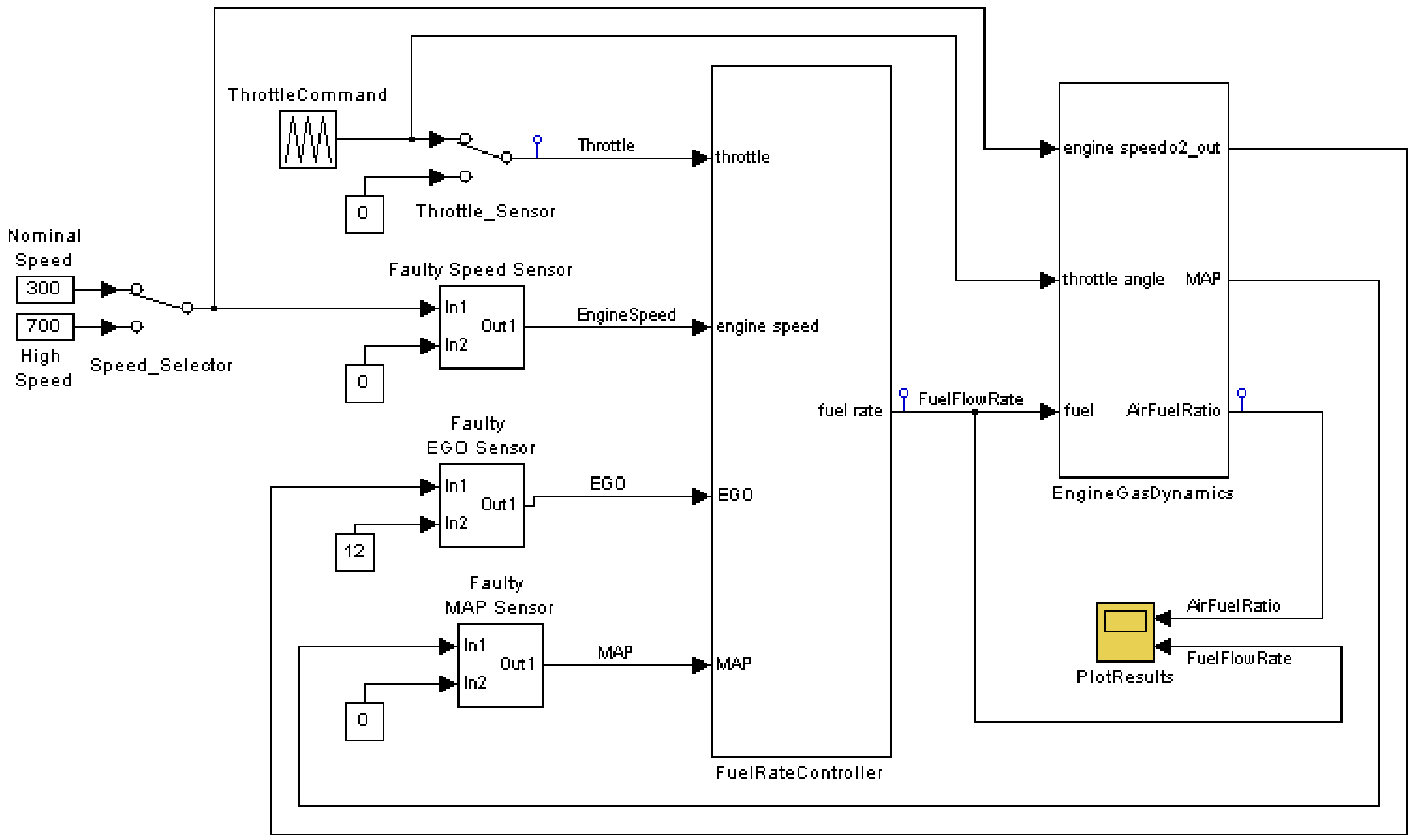
$$\text{Prob}(\text{"accept } H_0\text{"} \mid H_1) \leq (1/c - 1)\pi_0/(1-\pi_0)$$
$$\text{Prob}(\text{"reject } H_0\text{"} \mid H_0) \leq (1/c - 1)\pi_0/(1-\pi_0)$$

π_0 is the prior probability of H_0

Zuliani, Platzer, Clarke. HSCC 2010

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

$$\mathcal{M}, \mathit{FaultRate} \models (\neg \boldsymbol{F}^{100}\, \boldsymbol{G}^{1}(\mathit{FuelFlowRate} = 0))$$

- *"It is not the case that within 100 seconds, FuelFlowRate is zero for 1 second"*
- We use various values of *FaultRate for each of the* three sensors in the model
- Uniform prior

Verification

- Half-width δ=.01
- Several values of coverage probability c
- Posterior mean: add/subtract δ to get Bayesian interval

		Interval coverage c			
		.9	.95	.99	.999
Fault rates	[3 7 8]	.3603	.3559	.3558	.3563
	[10 8 9]	.8534	.8518	.8528	.8534
	[20 10 20]	.9764	.9784	.9840	.9779
	[30 30 30]	.9913	.9933	.9956	.9971

Verification

- Number of samples
- Comparison with Chernoff-Hoeffding bound

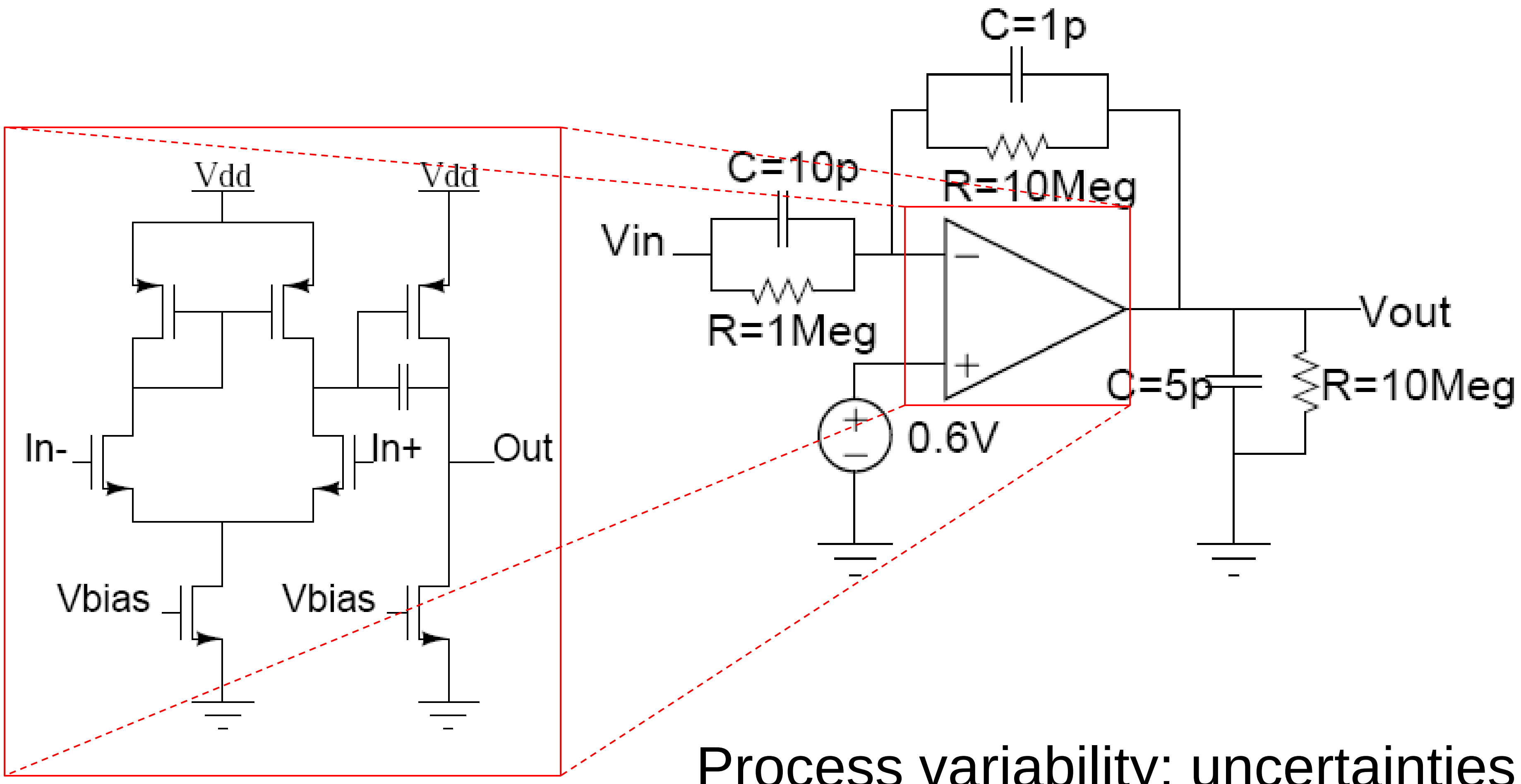
$$\Pr(|X - p| \geq \delta) \leq \mathit{exp}(-2n\delta^2)$$

where $X = 1/n \; \Sigma_i \; X_i$, $E[X_i]=p$

about 17hrs on 2.4GHz Pentium 4

		Interval coverage *c*			
		.9	.95	.99	.999
Fault rates	[3 7 8]	6,234	8,802	15,205	24,830
	[10 8 9]	3,381	4,844	8,331	13,569
	[20 10 20]	592	786	1,121	2,583
	[30 30 30]	113	148	227	341
Chernoff bound		11,513	14,979	23,026	34,539

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: Max(V_{out}) > 1.0V AND Min(V_{out}) < .2V
- Using BLTL specifications
  - In most cases, can be translated directly from definitions
  - e.g. Swing Range:
    - $\mathbf{F}^{[100\mu s]}(V_{out} < .2)$ AND $\mathbf{F}^{[100\mu s]}(V_{out} > 1.0)$
    - "within 100μs V_{out} will eventually be greater than 1V and smaller than .2V"
    - 100μs : end time of transient simulation
    - Note: unit in *bound* is only for readability

OP amp: BLTL Specifications

Specifications			BLTL Specifications
1	Input Offset Voltage	< 1 mV	$\mathbf{F}^{[100\mu s]}(V_{out} = .6)$ AND $\mathbf{G}^{[100\mu s]}((V_{out} = .6) \rightarrow (\lvert V_{in+} - V_{in-} \rvert < .001))$
2	Output Swing Range	.2 V to 1.0 V	$\mathbf{F}^{[100\mu s]}(V_{out} < .2)$ AND $\mathbf{F}^{[100\mu s]}(V_{out} > 1.0)$
3	Slew Rate	> 25 V/μSec	
	$\mathbf{G}^{[100\mu s]}(((V_{out} > 1.0 \text{ AND } V_{in} > .65) \rightarrow \mathbf{F}^{[0.032\mu s]}(V_{out} < .2))$ AND $(V_{out} < .2 \text{ AND } V_{in} < .55) \rightarrow \mathbf{F}^{[0.032\mu s]}(V_{out} < 1.0))$		

→ More properties and experiments in our ASP-DAC 2011 paper

Work in Progress: Rare events

- *p* is *small* (say 10^{-9})
- A 99% (approximate) confidence interval of relative accuracy δ needs about

  $$(1-p)/p\delta^2 \quad \text{samples}$$

- Examples:
  - $p = 10^{-9}$ and $\delta = 10^{-2}$ (ie, 1% accuracy) we need about 10^{13} samples!!
  - Bayesian estimation requires about 6×10^6 samples with $p=10^{-4}$ and $\delta = 10^{-1}$

Importance Sampling

- The fundamental Importance Sampling identity

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

Importance Sampling

- Estimate p_t=E[X>t]. A sample $X_1, \dots X_K$ iid as X

$$\hat{p}_t = \frac{1}{K}\sum_{i=1}^{K} I(X_i \geqslant t) = \frac{k_t}{K}, \qquad X_i \sim f$$

- Define a biasing density f_*

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

where $W(x) = f(x)/f_*(x)$ is the likelihood ratio

Importance Sampling: Toy Example

- Suppose X is Poisson with parameter λ
  - $\text{Prob}(X_t = k) = (1/k!)(\lambda t)^k \exp(-\lambda t)$
- Then $\text{Prob}(X_t >= 1) = 1 - \exp(-\lambda t)$
- Say t = 100 and $\lambda = 1/3 \times 10^{-11}$
  - $p_t = \text{Prob}(X_t >= 1) \approx 3.333 \times 10^{-10}$
  - Rare event!

Importance Sampling: Toy Example

- Define the biasing density a Poisson with parameter μ much larger than λ.
- 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 $k_1 \ldots k_N$ from the biasing density
- Importance sampling estimate is
  - $e_t = 1/N \, \Sigma_{\mathrm{i}} \, I(k_i >= 1) \, W(k_i)$

Importance Sampling: Toy Example

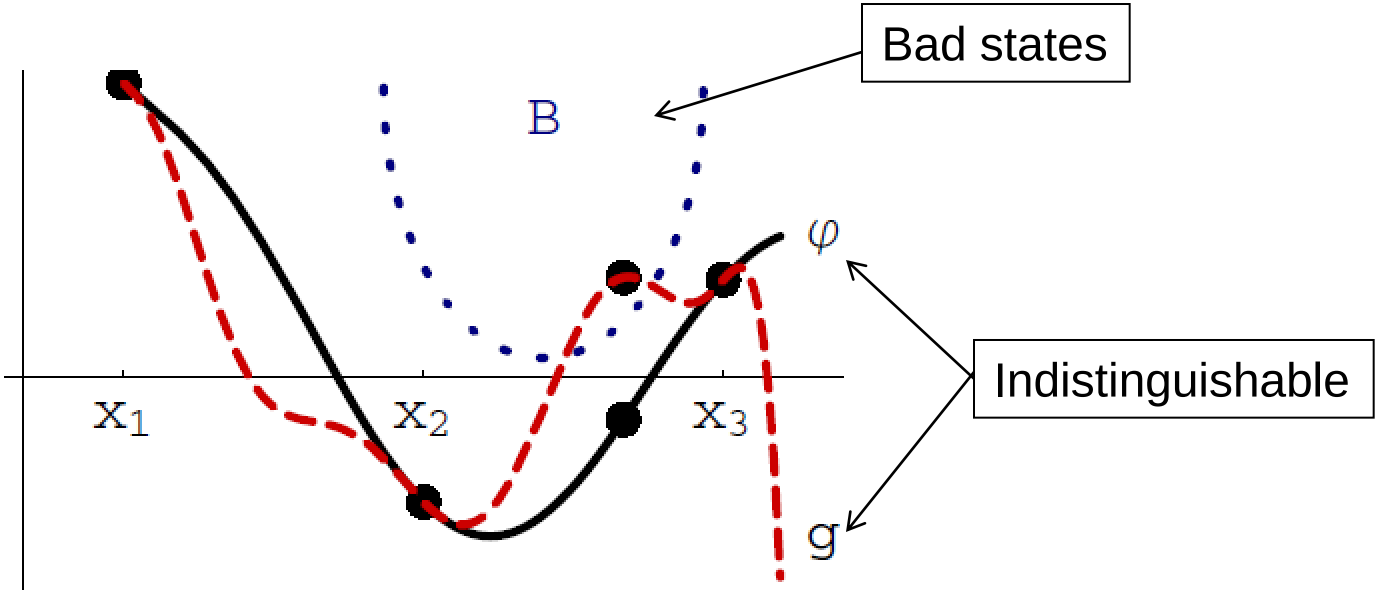
- With N = 100 samples and $\mu = 1/90$ we get an estimate

$$e_t = 3.2808 \times 10^{-10}$$

- Recall the “unbiased” system has $\lambda = 1/3 \times 10^{-11}$
- The (unknown) true probability is about 3.333×10^{-10}
- Try standard MC estimation …

Work In Progress

- Tackling the incompleteness of simulation
- *<u>Theorem</u> (Undecidability of image computation)*



Platzer and Clarke, HSCC 2007

Work In Progress

- 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 φ 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)

The End

Thank You!