Formalization of Normal Random Variables

M. Qasim, O. Hasan, M. Elleuch, S. Tahar
Hardware Verification Group
ECE Department, Concordia University, Montreal, Canada

CICM 16
July 28, 2016
Outline

- Introduction and Motivation
- Formalization
- Case Study: Clock Synchronization in WSNs
- Conclusions
Motivation

- Noise
- Aging Phenomena
- Environmental Conditions
- Unpredictable Inputs
Probabilistic Analysis

Random Components

Hardware
Software

System Model

Random Variables
(Discrete/Continuous)

Computer Based
Analysis Framework

Property Satisfied?

Probabilistic and Statistical Properties
Probabilistic Analysis Basics - Random Variables

- Discrete Random Variables
  - Attain a countable number of values
  - Example
    - Dice [1, 6]

- Continuous Random Variables
  - Attain an uncountable number of values
  - Examples
    - Uniform (all real numbers in an interval [a,b])
# Probabilistic Analysis Basics - Probabilistic Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Probability Mass Function (PMF)</strong></td>
<td>Probability that the random variable is equal to some number ( n )</td>
<td><img src="example.png" alt="Probability Mass Function" /></td>
</tr>
<tr>
<td><strong>Cumulative Distribution Function (CDF)</strong></td>
<td>Probability that the random variable is less than or equal to some number ( n )</td>
<td><img src="example.png" alt="Cumulative Distribution Function" /></td>
</tr>
<tr>
<td><strong>Probability Density Function (PDF)</strong></td>
<td><strong>Slope</strong> of CDF for continuous random variables</td>
<td><img src="example.png" alt="Probability Density Function" /></td>
</tr>
</tbody>
</table>
## Probabilistic Analysis Basics - Statistical Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Illustration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expectation</td>
<td>Long-run <em>average</em> value of a random variable</td>
<td><img src="image" alt="Illustration of Expectation" /></td>
</tr>
<tr>
<td>Variance</td>
<td>Measure of <em>dispersion</em> of a random variable</td>
<td><img src="image" alt="Illustration of Variance" /></td>
</tr>
</tbody>
</table>
# Probabilistic Analysis Approaches

<table>
<thead>
<tr>
<th></th>
<th>Simulation</th>
<th>Formal Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Model Checking</td>
</tr>
<tr>
<td>Random Components</td>
<td>Approximate random variable functions</td>
<td>Probabilistic State Machine</td>
</tr>
<tr>
<td>Analysis</td>
<td>Observing some test cases</td>
<td>Exhaustive Verification</td>
</tr>
<tr>
<td>Accuracy</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Expressiveness</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Automation</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Maturity</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>
Probabilistic Analysis using Theorem Proving

System Description

Higher-order logic Formalization of Probability Theory

Discrete Random Variables
- Probabilistic Properties: PMF, CDF
- Statistical Properties: Expectation, Variance

Continuous Random Variables
- Probabilistic Properties: CDF, PDF
- Statistical Properties: Expectation, Variance

Probabilistic Analysis Proof Goals

Theorem Prover

Formal Proofs of Properties

- [Hurd, 2002]: Probability Theory, Discrete Random Variables (RVs), PMF
- [Hasan, 2007]: Statistical Properties for Discrete RVs, CDF, Continuous RVs
- [Mhamdi, 2011] Probability (Arbitrary space) Lebesgue Integration, Multiple Continuous RVs Statistical Properties
- [Hölzl, 2012] Isabelle/HOL: Probability, Measure and Lebesgue Integration, Markov, Central Limit Theorem
Paper Contributions

- Formalization of Probability Density Function (PDF)
- Formalization of Normal Random Variable
  - Enormous Applications
  - Sample mean of most distributions can be treated as Normally Distributed
- Case Study: Clock Synchronization in WSNs
PDF $p(x)$ of a random variable $x$ is used to define its distribution

$$P(x_1 < x < x_2) = \int_{x_1}^{x_2} p(x) \, dx$$

The PDF of a random variable is formally defined as the Radon-Nikodym (RN) derivative of the probability measure with respect to the Lebesgue-Borel measure

- RN derivative and probability measure was available in HOL4
- Lebesgue-Borel measure
  - Ported from Isabelle/HOL [Hölzl, 2012]
  - Some theorems and tactics (e.g. SET_TAC) also ported from the Lebesgue measure theory of HOL-Light [Harrison, 2013]
The PDF of a random variable is formally defined as the Radon-Nikodym (RN) derivative of the probability measure with respect to the Lebesgue-Borel measure.

**Definition: Probability Density Function**

\[ \text{PDF} \ X \ p = \text{RN} \_\text{deriv} \ \text{l borel} \]

\[ (\text{space borel, subsets borel, measurable_distr p X}) \]
Normal Random Variable

- Normal PDF
  \[ N(\mu, \sigma) = \frac{1}{\sigma \sqrt{2\pi}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) \]
  where \( \mu \) represents its mean and \( \sigma \) is the standard deviation

- **Definition: Normal Random Variable**
  \[ \texttt{normal_rv} \texttt{ X p } \mu \texttt{ } \sigma = \texttt{random_variable} \texttt{ X p borel} \land (\texttt{measurable_distr} \texttt{ p X } = \texttt{normal_pmeasure} \mu \sigma) \]

- \( X \) is a real random variable, i.e., it is measurable from the probability space \( (p) \) to Borel space

- The distribution of \( X \) is that of the Normal random variable
Normal Random Variable - Properties

Theorem: PDF of a Normal random variable is non-negative
\[ \forall X \quad p \quad \mu \quad \sigma. \quad \text{normal}_r v \ X \quad p \quad \mu \quad \sigma \implies \forall x. \quad 0 \leq \text{PDF} \quad p \quad X \quad x \]

Theorem: PDF over the whole space is 1
\[ \forall X \quad p \quad \mu \quad \sigma. \quad \text{normal}_r v \ X \quad p \quad \mu \quad \sigma \implies (\text{integral lborel} (\text{PDF} \quad p \quad X) = 1) \]
Normal Random Variable - Properties

Theorem: PDF of a Normal random variable is symmetric around its mean

\[ \forall X \ p \mu \sigma \ a. \text{normal}_\text{rv} \ X \ p \mu \sigma \Rightarrow \]
\[ \text{pos}_\text{fn}_\text{integral} \ \text{lborel} \]
\[ (\lambda x. \text{PDF} \ p \ X \ x \ * \ \text{indicator}_\text{fn} \ \{x \mid \mu-a \leq x \land x \leq \mu\} \ x) = \]
\[ \text{pos}_\text{fn}_\text{integral} \ \text{lborel} \]
\[ (\lambda x. \text{PDF} \ p \ X \ x \ * \ \text{indicator}_\text{fn} \ \{x \mid \mu \leq x \land x \leq \mu+a\} \ x) \]

\[ \int_{-\infty}^{\mu} p(x) \, dx = \int_{\mu}^{\infty} p(x) \, dx = \frac{1}{2} \]

Theorem: PDF of a Normal random variable is symmetric around its mean

\[ \forall X \ p \mu \sigma. \text{normal}_\text{rv} \ X \ p \mu \sigma ^ \land A = \{x \mid x \leq \mu\} \land B = \{x \mid \mu \leq x\} \Rightarrow \]
\[ (\text{pos}_\text{fn}_\text{integral} \ \text{lborel} \ (\lambda x. \text{PDF} \ p \ X \ x \ * \ \text{indicator}_\text{fn} \ A \ x) = 1 / 2) \land \]
\[ (\text{pos}_\text{fn}_\text{integral} \ \text{lborel} \ (\lambda x. \text{PDF} \ p \ X \ x \ * \ \text{indicator}_\text{fn} \ B \ x) = 1 / 2) \]
Normal Random Variable - Properties

If $X_i \sim N(\mu_i, \sigma_i^2)$ is a finite set of independent Normal random variables, and $Z = \sum X_i$ then, $Z \sim N(\sum \mu_i, \sum \sigma_i^2)$.

Theorem: Summation of Normal Random Variables

- The proofs of these properties not only ensure the correctness of our definitions but also facilitate the formal reasoning process about the Normal Random Variable.
Application: Probabilistic Clock Synchronization in WSNs

- Synchronizing receivers with one another
- Randomness in Message delivery latency
- Probabilistic bounds on clock synchronization error
  - single hop
  - & multi-hop networks
Capturing the Randomness in the Latency

- Multiple pulses are sent from the sender to the set of receivers.
- The difference in reception time at the receivers is plotted.

Pairwise difference in packet reception time – Normally Distributed with mean = 0
Error Bounds - Single Hop

\[ P(|\epsilon| \leq \epsilon_{max}) = 2 \ \text{erf} \left( \frac{\sqrt{n} \epsilon_{max}}{\sigma} \right) \]

\( \epsilon \) is the synchronization error

\( \epsilon_{max} \) is the maximum allowable error

\( n \) is the minimum number of synchronization messages

\[ \text{erf}(z) = \frac{1}{\sqrt{2\pi}} \int_{0}^{z} \exp\left(-\frac{x^2}{2}\right) \, dx \]

**Theorem:** Probability of synchronization error for single hop network

\[ \forall p, X, \mu, \sigma, n, E_{\text{max}}. \ \text{prob\_space\_p} \land (I = (1 \ldots n)) \land \\
(0 < \sigma) \land (0 < n) \land (\forall i. \ i \in I \Rightarrow \text{sync\_error} \ (X, i) \ p, \mu, \sigma) \land \\
(Z = (\lambda x. \ \text{sum} \ I \ (\lambda i. \ X, i, x) / n)) \land (\mu = 0) \land 0 \leq E_{\text{max}} \Rightarrow \\
(\text{prob\_sync\_error} \ p, Z \ \{x \ | -E_{\text{max}} \leq x \land x \leq E_{\text{max}}\} = \\
2 \ast \text{err\_func} \ (E_{\text{max}} \ast \sqrt{\frac{n}{\sigma}})) \]
Conclusions

- Probabilistic Theorem Proving
  - Exact Answers
  - Useful for the analysis of Safety critical application

- Our Contributions
  - Formalization of Probability Density Functions and Normal random variables
  - Case Study
    - Clock Synchronization in WSNs

- Future Work
  - More Applications - Probabilistic Round off Error Bounds in Computer Arithmetic
Thank you!