Formal Reliability Analysis using Higher-Order Logic Theorem Proving

Naeem Ahmad Abbasi

A Thesis

in

The Department

of

Electrical and Computer Engineering

Presented in Partial Fulfillment of the Requirements

for the Degree of Doctor of Philosophy at

Concordia University

Montréal, Québec, Canada

March 2012

CONCORDIA UNIVERSITY

Division of Graduate Studies

This is to certify that the thesis prepared

By: **Naeem Ahmad Abbasi**

Entitled: **Formal Reliability Analysis using Higher-Order Logic Theorem Proving**

and submitted in partial fulfilment of the requirements for the degree of

Doctor of Philosophy

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

_____ Dr. Roger Villemaire

_____ Dr. Chun-Yi Su

_____ Dr. Amir G. Aghdam

_____ Dr. Ali Ghrayeb

_____ Dr. Sofiene Tahar

Approved by _____

Chair of the ECE Department

_____ 2012 _____

Dean of Engineering

ABSTRACT

Formal Reliability Analysis using Higher-Order Logic Theorem Proving

Naeem Ahmad Abbasi, Ph. D.

Concordia University, 2012

Traditional techniques used in the reliability analysis of engineering systems have limitations. Paper-and-pencil based analysis is prone to human error and simulation based techniques cannot be computationally one hundred percent accurate. An alternative to these two traditional approaches is modeling and analysis of reliability of systems using formal methods based techniques such as probabilistic theorem proving. Probabilistic theorem proving using higher-order logic can be used for modeling and analysis of reliability of engineering systems provided a certain reasoning infrastructure is developed. The developed infrastructure can include random variables, their probabilistic and statistical properties, and basic reliability theory concepts such as survival and hazard functions. This thesis describes state-of-the-art research in reliability analysis using theorem proving. It also describes the main contributions of this thesis which include: the formalization of statistical properties of continuous random variables, the formalization of multiple continuous random variables and the formalization of the basic notions of reliability that can be applied to single and multiple component systems. Engineering applications of the formalization are presented that illustrate the usefulness of our formalization infrastructure. These applications include reliability analysis of electronic system components such as a capacitor and an underground power transmission cable. We also present the reliability analysis of an automobile transmission using our higher-order logic formalization.

To the best of our knowledge, for the very first time, the use of theorem proving based infrastructure enables formal reliability analysis of engineering systems that is computationally one hundred percent accurate and sound. The analysis is performed using real and true random variables. We show that the results presented in this thesis are general and can be applied to many reliability engineering problems.

To My Mother and Father

ACKNOWLEDGEMENTS

Many thanks to Dr. Sofiene Tahar for his help, support, and guidance. I am very grateful for his patience, encouragement, and pragmatic and expert advice throughout my graduate studies. I could not have wished for a better thesis supervisor. Many thanks to Dr. Osman Hasan for his support in my research, sound advice, insightful criticisms, prompt feedbacks and encouragement. Many thanks to the members of the thesis committee, whose comments allowed me to focus my research on areas of practical interest. Many thanks to the School of Graduate studies for the two scholarships that allowed me to travel to conferences and assisted me in writing this thesis. Many thanks to my good friends at the hardware verification group for their help and support. Finally, I would like to thank my Mother, Anis Jehan Begum, for her unconditional love and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

ACL	A Computational Logic for Applicative Lisp
CAD	Computer Aided Design
CDF	Cumulative Distribution Function
CRV	Continuous Random Variable
FK	Fitting Key
FMEA	Failure Mode Effect Analysis
FTA	Fault Tree Analysis
G12P	Gear 1,2 Pitting
G1B	Gear 1 Breakage
G2B	Gear 2 Breakage
HDL	Hardware Description Language
HOL	Higher-Order Logic
IS	Input Shaft
ITM	Inverse Transform Method
LCF	Logic of Computable Function
LISP	LISt Processing
ML	Meta Language
MTTF	Mean Time To Failure
OS	Output Shaft
PDF	Probability Density Function
PRISM	PRobabilistIc Symbolic Model checker
PVS	Prototype Verification System
RB1	Roll Bearing 1

RB2	Roll Bearing 2
RB3	Roll Bearing 3
RB4	Roll Bearing 4
SS1	Shaft Seal 1
SS2	Shaft Seal 2
VLSI	Very Large Scale Integration

Chapter 1

Introduction

1.1 Motivation

If something can go wrong, it will - Murphy's Law

European Journal of Applied Physics, 1995

The above statement, popularly known as the Murphys Law, is attributed to captain A. Murphy of the United States Air Force who was involved in experiments designed to study the effects of sudden deceleration on humans in the late 1940s. Analogues of similar nature have been known to exist earlier than the 1940s in many disciplines of engineering and applied science. They all highlight the fact that if there are more than one ways to do something and one of which could be wrong, then some one will eventually intentionally or un intentionally use the wrong method. This has become a very serious problem in modern engineering designs and is motivating the development of systematic and accurate methods, algorithms and tools.

Engineering systems are usually complex, involve a lot of detail, and operate in unpredictable environments. In order to predict accurate behavior, often times

it is necessary to build mathematical models that take into account unpredictable behavior of the system and its environment. System function, system performance and system trustworthiness is evaluated through system analysis. System function analysis refers to the ability of a system to perform certain operations in a predefined sequence in response to given stimuli. System performance analysis usually refers to the completion of the function in a certain amount of time. For example, average time taken to complete a certain operation. An important component of system trustworthiness is its reliability. Reliability of a system is a measure of continuity of service under specified conditions.

Probabilistic and statistical analysis enables us to answer questions about system function, performance and reliability that cannot be answered using traditional deterministic analysis techniques. For example, what is the probability of a failure causing the system to shut down within N hours? or what is the expected size of a message queue after X minutes? Engineering systems whose failure can result in serious harm to humans, significant loss of revenue or both are called safety critical systems. Examples of such systems can be found in health care, transportation, electrical power transmission and distribution, communications, chemical, nuclear and aerospace industries.

Traditionally, paper-and-pencil based approaches and computer simulations have been used for the analysis of safety critical systems. Both of these techniques are unsuitable for safety critical applications. This is due to the possibility of human error in paper and pencil based analysis and the lack of accuracy in computer simulations. In computer simulations, a trade-off between the accuracy of computations and the simulation run time is often made. Moreover, modeling of true random behavior is a challenge in computer simulations as computer generated random numbers are in

fact only pseudo random.

A fairly new development in the area of functional, performance and reliability analysis is the formal analysis of systems using higher-order logic theorem proving. In such formal analysis, first the system is described using an expressive logic, and then its functional, performance and reliability properties are verified through rigorous mathematical reasoning. Theorem proving is a formal verification technique in which an equivalence or an implication relation between the implementation and the specification of a system is proved using mathematical reasoning. The theorem proving approach can handle infinite systems; it can help establish properties of potentially infinite systems, such as stacks, queues etc. This technique together with higher-order logic has been extended to deal with performance analysis problems. Formalized real numbers facilitate functional performance analysis of systems. Higher-order logic theorem proving can be used to reason about large sized systems that cannot be dealt with by model checking [21], but the process of verification is interactive as higher-order logic is undecidable. Model checking is a formal technique that considers finite systems or finite models of infinite systems and is only suitable for relatively small sized reliability analysis problems.

At this time theorem proving lacks formalized mathematical foundations for reliability analysis. For example, formalized multiple random variables, statistical properties of continuous random variables and basic notions of reliability. This thesis provides a framework for reliability analysis of engineering systems in a theorem proving environment. The work is important as it enables modeling of true random behavior, one hundred percent computationally accurate reliability analysis and provides an accurate alternative to the traditional reliability analysis techniques such as paper and pencil analysis and computer simulations.

1.2 System Reliability Analysis

Tragedies such as the industrial accident at the union carbide pesticide plant in Bhopal India [11] and the high-speed train accident near the village of Eschede in Lower Saxony in Germany [35] highlight the importance of design reliability in various disciplines of engineering. The reliability of a system is defined as the probability that it will adequately perform its specified purpose for a given period of time under certain specific environmental conditions [43].

A system usually consists of two or more components each performing a certain sub function of the system. Series, parallel, a combination of series-parallel and parallel-series, and sometimes more complicated interconnections exist in a system. Additional functional units are often added in safety critical systems to increase redundancy that helps improve its reliability.

System reliability analysis involves mathematically expressing the arrangement of components in a system and computing its overall reliability. The modeling process deals with the structural properties associated with a system of components and the analysis involves probabilistic and statistical properties and the bounds of these measures of reliability associated with the system of components.

Qualitative methods help in determining reliability relevant components of a system. They provide a systematic way of determining whether a system component affects the system reliability. These methods analyze the function and the environmental stresses a component experiences and try to determine if and how the component will affect the system reliability, and what would be the effects of failure of the component on the system. For example, Failure Model Effect Analysis (FMEA) and Fault Tree Analysis (FTA).

Reliability behavior and lifetime properties of engineering systems can be modeled with the help of continuous random variables. Most commonly used measures of reliability of a system are a function of the standard probabilistic and statistical properties of these random variables. System lifetime is modeled using positive real valued random variables. For example, Exponential and Weibull random variables. Four commonly used lifetime distribution representations are the survival function, the hazard function, the cumulative hazard function, and the fractile function. They are all measures of reliability of a system and can be derived from each other. Statistical properties such as expectation and variance are useful ways to summarize the reliability behavior. For example, the expectation property of the distribution is used to describe the mean time to failure of a system component. Once the component lifetime distributions and the arrangement of various components in a system are known, the reliability functions of the entire system and its distribution can be determined.

1.3 State-of-the-art in Reliability Analysis

One of the earliest examples of detailed reliability studies in engineering systems dates back to 1938 [18]. In this study, factors for the improvement of service reliability for electrical power systems were considered. In the field of electronics, the concepts related to reliability were initially introduced after the second world war to improve the performance of communication and navigational systems [55].

In order to predict reliability, one must model a system and its constituent components in a way that captures failure mechanisms. For example, in the case of electronic systems, a method called the part failure method has been shown to be very accurate [51]. This method has been extensively used by military engineers to predict useful lifetimes of systems and to develop highly reliable systems and equipments. This

method is based on calculating failure rates of individual components of the system and then using appropriate formulas to determine the reliability of the whole system. Standards such as MIL-HDBK-2173 [52], FIDES [22], and IEEE 1332 [53] are some of the examples which specify adequate performance requirements and environmental conditions for reliability modeling, analysis, and risk assessment.

Simulation techniques for analyzing reliability are sometimes attractive because the process can be completely automated. Moreover, for some reliability problems, either the analytical solutions are not available (for example non-determinism arising in problems involving concurrency) or prohibitively complex to find due to the amount of detail involved, as is the case in many modern engineering systems.

Simulation based analysis cannot be termed one hundred percent accurate because of the computational inaccuracies, the use of fixed and floating point arithmetic and the use of pseudo random numbers instead of true random numbers. This can lead to inaccurate result, resulting in serious consequences sometime. For example, the spectacular disaster with space shuttle Challenger in which the entire crew of seven lost their lives with in 75 seconds of the take off was due to a reliability issue in the design of one of the booster rockets [56]. Table 1.3 lists a few examples of simulation based tools for analyzing reliability and their applications [37].

Formal methods for performance analysis include run time verification [44], model checking [21] and theorem proving [38]. These techniques have been extended to analyze reliability of systems during the last two decades. Many expressive formalisms such as stochastic petri nets [41] and process algebras [13] along with various probabilistic [40] and stochastic temporal logics [5], and compositional and guarded command notations [36] have been used in modeling, specification and analysis of complex engineering [31] and applied science problems [7]. They were either not designed

Reliability Analysis Tool	**Description and Application**
CARE[60, 49], ARP[37], SHARE[37], SURF[15], AIRES[37]	Fault Tolerant Computer Architectures
RELIANT[23], SysRel[4], ERNI[12]	Integrated Circuit conductor reliability and failure analysis, predict reliability and hazards due electro-migration
MARK1[42]	Markov Modeling Package
METASAN[58]	Michigan Evaluation tool for the analysis of stochastic activity
SAVE[27]	System AVailability Estimation
BERT[61]	BErkely Reliability Tool

Table 1.1: Simulation based reliability analysis tools

to deal with reliability analysis problems or lack the capability to handle reliability problems due to lack of infrastructure.

Formal methods based techniques, such as probabilistic model checking, can be used to analyze reliability; however, they do not have support for the verification of statistical properties (moments and variance) of the commonly used lifetime distributions [5, 57]. The proposed approach on the other hand is capable of handling these and other probabilistic and statistical properties. Probabilistic model checkers, for example PRISM [39], have the ability to verify exact solutions for probabilistic properties in an automated manner. Moreover, they have been used to determine expected values in what amounts to a semi-formal method. In the PRISM model checker, probabilistic finite state models are constructed with real value probabilities associated with the transitions between various states of the model. Probabilistic model checking tools run out of memory very quickly when the probabilistic state space is large, and that puts a practical limit on the number of reliability analysis problems that can be reasonably handled with this technique and the tools associated with it. Both simulation and probabilistic model checking do, however, have their

place and can play an important role within a comprehensive verification methodology where appropriate and reasonably small parts of a problem can be automatically verified using these techniques.

Probabilistic theorem proving techniques, on the other hand, though interactive, are completely formal, sound, one hundred percent computationally accurate, and, in theory, have no limitations as far as the number of states is concerned. In order to analyze systems formally in a theorem proving environment, it is important to have an infrastructure for reasoning about the underlying mathematical concepts of probability and statistics. The accuracy of reliability analysis depends on both the field data gathering and the methods and tools used for analysis. In this thesis, we do not address the problem of field data gathering. Our focus is on the higher-order logic formalization of fundamental concepts of the reliability theory. Until recently it was only possible to reason about reliability problems that involved discrete random variables in a theorem proving environment [29]. Hurd [34] formalized a probability theory along with discrete random variables in the HOL theorem prover [26]. Building upon Hurd's work [34], Hasan [29] formalized statistical properties of single and multiple discrete random variables. Hasan [29] also formalized a class of continuous random variables for which the inverse CDF functions can be expressed in a closed form. Hasan *et al.* [32] presented higher-order-logic formalizations of some core reliability theory concepts and successfully formalized and verified the conditions for consistent repairability for reconfigurable memory arrays in the presence of stuck-at and coupling faults.

1.4 Proposed Methodology

Based on the above discussion and the stated limitations of the state-of-the-art in the area of formal reliability analysis, we propose a formal reliability analysis framework for reasoning about practical engineering problems. Our approach is based on higher-order logic theorem proving. We develop necessary infrastructure needed for formal reliability analysis by formalizing underlying mathematics and basic notions of reliability theory.

Reliability modeling and analysis process requires formalized continuous single and multiple random variables. In this process, an engineer first constructs a formal model of the system and its environment. He or she then specifies functional and reliability requirements of the system as formal logic statements to check the function and reliability of the system. The proposed reliability analysis framework facilitates verification, computation, reasoning, and documentation of the reliability proofs in the sound environment of the HOL theorem prover. Finally, the formal functional and reliability analysis results are unformalized and interpreted and stated in an appropriate language in the problem domain.

The formal reliability analysis framework is shown in Figure 1.1. The solid box below the top dotted line in Figure 1.1 highlights some of the main features of the proposed reliability analysis framework.

An important class of reliability properties are the statistical properties. These properties conveniently summarize the complete reliability behavior into one or more quantitative measures such as the expectation and the variance. Positive real valued continuous random variables such as the exponential random variable are commonly used random variables in reliability analysis of engineering systems. In such analysis, system lifetime is modeled as a random variable and the average time taken by the

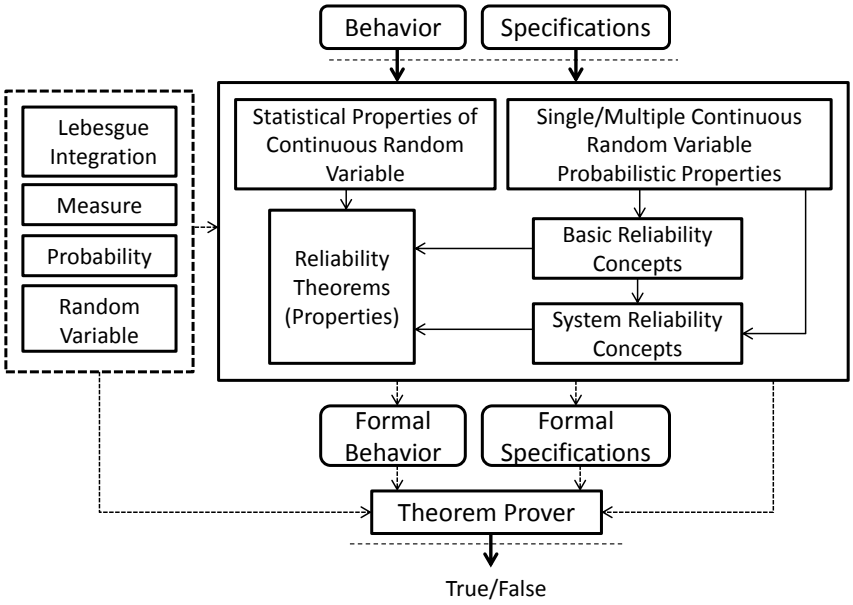

Figure 1.1: Formal reliability analysis framework.

system to fail is defined as the expected value of the random variable and is commonly known as the mean time to failure or MTTF in reliability analysis literature. We provide a large set of lemmas and theorems for facilitating verification of statistical reliability properties of a system.

Multiple continuous random variables play an important role in the reliability modeling and analysis of engineering systems. Our proposed reliability analysis framework includes formalized multiple continuous random variables and their probabilistic properties such as the joint and marginal cumulative distribution functions and results which verify that the cumulative distribution functions are bounded, monotonic non-decreasing and tend to 0 and 1 as the argument of these functions tend to $-\infty$ and ∞ respectively. These formalized properties help define basic notions of reliability such as the survival function and the hazard function. We verify a large set of helper lemmas, theorems and properties of the basic notions of reliability theory.

All of these reduce the interactive effort required for reliability analysis of engineering systems using theorem proving.

Complex systems usually consist of multiple functional units. Each of these units behave independently as far as their reliability behavior is concerned. In order to determine the overall system reliability, formal modeling of system structure is absolutely important. Therefore, we have formalized and verified results for modeling and verification of reliability of various system configurations such as series, parallel, series-parallel and parallel-series structures.

These formalizations together provide capabilities of complete formal reliability analysis of engineering systems and provide an alternative to traditional simulation based reliability analysis approach.

1.5 Thesis Contributions

This thesis focuses on developing an infrastructure for carrying out formal reliability analysis using higher-order logic theorem proving. The theorem proving based approach, described in this thesis, for formal reliability analysis is very useful in constructing formal proofs of correctness of reliability related properties of safety critical hardware and software. The thesis makes the following main contributions.

1. It presents the formalization of statistical properties of continuous random variables. Expectation, variance and moment relations are formally verified in higher-order logic using Lebesgue integration theory. Basic properties of the linearity of expectation and variance are also verified using Lebesgue integration theory. These higher-order logic proofs document detailed proof steps and are generalized expressions with quantifications over random and real variables and probability distribution parameters; they explicitly state all the assumptions

and are valid and sound, something that is not possible with existing formal and simulation based techniques.

2. It presents formalization of multiple continuous random variables. The framework allows us to specify and verify higher-order logic theorems related to probabilistic properties of multiple continuous random variables.

3. It presents the formalization of basic notions of reliability in higher-order logic. We believe this is the first such formalization of reliability theory in any higher-order logic theorem proving environment

4. It provides a framework to model reliability structure of engineering systems. The theorems related to various system configurations, such as series, parallel, series parallel and parallel series, facilitate the reliability analysis process and reduce the interactive effort.

5. The usefulness of the proposed reliability analysis framework is demonstrated with the help of practical engineering applications: 1) Reliability analysis of electronic and electrical power system components, 2) Reliability analysis of an automobile transmission.

1.6 Organization of the Thesis

The rest of the thesis is organized as follows: In Chapter 2, we introduce some preliminary concepts which will facilitate reading of the rest of the thesis. In Chapter 3, we describe the methodology for the formalization and verification of statistical properties of continuous random variables. In Chapter 4, we provide formal definitions of multiple continuous random variables and the formalization and verification of

probabilistic properties of a list of random variables. We also formalize the notion of independence of random variables. We present the formalization of the basic notions of reliability in Chapter 5 and verify their important properties. We also verify standard results related to various multi-component system configurations. In Chapter 6, we present practical applications utilizing our formalization of multiple continuous random variables and reliability theory concepts. Finally, with a summary of the main contributions and suggestions for future work, we conclude the thesis.

Chapter 2

Preliminaries

In this chapter, we provide a brief introduction to probabilistic and statistical properties of continuous random variables, Lebesgue integration and the HOL theorem prover. An introduction to basic notation used in the rest of this thesis is also introduced. The chapter concludes with a brief description of theories of probability, random variables and Lebesgue integration in HOL.

2.1 Random Variables and Distributions

A random variable is a deterministic function that maps the outcomes of a random experiment to a real value. Figure 2.1 graphically shows how a random variable RV assigns a real value to an event A in the sample space S of the random variable. An event A can be any valid subset of the sample space S. The domain of the random variable is the sample space S of the random experiment, and the range of the random variable is the whole real line. There are two main types of random variables; discrete and continuous. The range of discrete random variables is a finite or a countably infinite set. They mostly appear in problems involving counting. The

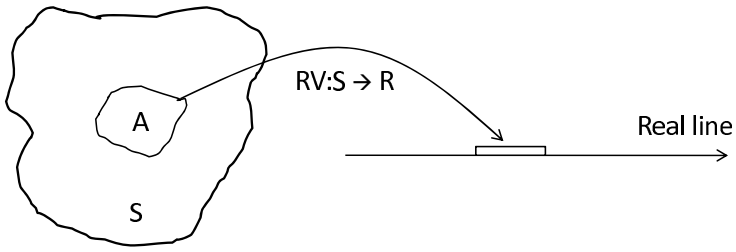

Figure 2.1: Random variable.

range of a continuous random variable is an infinite set. They are easier to handle analytically, represent a limiting form of many discrete random variables, and can be used to model a larger class of problems with just a few parameters. The cumulative distribution function or *CDF* of a random variable X, denoted as $F_X(x)$, is defined as the probability of an event $\{X \leq x\}$ and is mathematically stated as:

$$F_X(x) = P\{X \leq x\}, \qquad -\infty < x < +\infty \tag{2.1}$$

The Cumulative Distribution Function (*CDF*) of a discrete random variable is a right-continuous, staircase function, with jumps at a countable set of points whereas the *CDF* of a continuous random variable is continuous everywhere. The probability density function (*PDF*) of a continuous random variable X, if it exists is denoted as $f_X(x)$, and is defined as the derivative of its *CDF*.

$$f_X(x) = \frac{dF_X(x)}{dx} \tag{2.2}$$

A valid PDF of a random variable is a non-negative, continuous or piecewise continuous function that has a finite integral.

2.2 Statistical Properties of Random Variables

The definitions of expectation, variance, and moment of a discrete and continuous random variable are summarized in Table 2.1. Other important and interesting statistical properties include the moment generating function, the characteristic function, the Laplace transform, and the tail distribution bounds. A good description can be found in [19].

Property	Discrete	Continuous
Expectation, $E[X] = \mu_X$	$\sum_i x_i p_X(x_i)$	$\int_{-\infty}^{+\infty} x f_X(x) dx$
Variance, $VAR[X]$	$\sum_i (x_i - \mu_X)^2 p_X(x_i)$	$\int_{-\infty}^{+\infty} (x - \mu_X)^2 f_X(x) dx$
k-th Moment, $E[X^k]$	$\sum_i x_i^k p_X(x_i)$	$\int_{-\infty}^{+\infty} x^k f_X(x) dx$

Table 2.1: Expectation, variance, and moment of a random variable.

2.3 Multiple Random Variables

Many real-world applications require finding the probabilities of events that involve the joint behavior of two or more random variables. The joint *CDF* and the joint *PDF* functions of multiple random variables completely define the probabilities of product-form events. For example, consider two random variables X and Y. The joint cumulative distribution function of X and Y is defined as the probability of an event described by a semi-infinite rectangle ($\{(x_1, y_1) | x \leq x_1 \text{ and } y \leq y_1\}$) in the real x-y plane. It is mathematically expressed as:

$$F_{X,Y}(x_1, y_1) = P\{X \leq x_1, Y \leq y_1\} \tag{2.3}$$

If both X and Y are jointly continuous random variables, then their joint PDF $f_{X,Y}(x, y)$, if it exists, can be obtained by partial differentiation of their joint *CDF*

function $F_{X,Y}(x, y)$

$$f_{X,Y}(x, y) = \frac{\partial^2 F_{X,Y}(x, y)}{\partial x \partial y} \tag{2.4}$$

The joint *CDF* and *PDF* functions of n random variables are similarly defined. Table 2.2 shows the definitions of the jk-th moment and the jk-th central moments of two jointly discrete and continuous random variables. Where $p_{X,Y}(x, y)$ is the joint probability mass function of the two random variables.

Property	Discrete	Continuous
jk-th Moment	$\sum_{i=0}^{i=I} \sum_{n=0}^{n=N} x_i^j y_n^k p_{X,Y}(x_i, y_n)$	$\int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} x^j y^k f_{X,Y}(x, y) dxdy$
jk-th Central Moment	$\sum_{i=0}^{i=I} \sum_{n=0}^{n=N} (x_i - \mu_X)^j (y_n - \mu_Y)^k$ $p_{X,Y}(x_i, y_n)$	$\int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} (x - \mu_X)^j (y - \mu_Y)^k$ $f_{X,Y}(x, y) dxdy$

Table 2.2: The jk-th moment and the jk-th central moment of two jointly discrete and continuous random variables.

2.4 Lebesgue Integration

Lebesgue integral formalization partitions the range of the function rather than its domain and thus is able to integrate some functions for which Riemann integral does not exist. Also it does not put any restriction on the type of domain of a function and is not limited to functions which have real type as their domain, as is the case with Riemann integral. To understand the Lebesgue formalization of the integral, lets consider a bounded function $y = f(x)$ with an upper and lower limit as shown in Figure 2.2. Here the y interval, or the range of the function, is divided into n parts. Let E_k be a set of points or values for which $y_k \leq f(x) \leq y_{k+1}$. For example E_3 is a set for which all points are marked in black, where $y_3 \leq f(x) \leq y_4$. In general $l(E_k)$ stands for the total length of the set E_k (i.e., that sum of lengths of x-intervals for which $y_k \leq f(x) \leq y_{k+1}$). As n increases the summation in Equation 2.5 approaches

the true area under the curve $f(x)$

$$\int_E f(x)dx = \lim_{n\to\infty} \sum_{k=1}^{N} h_{nk} l(E_{nk}) \tag{2.5}$$

where $y_k \leq h_{nk} \leq y_{k+1}$, and $N = 2^n$. The points of E_k are chosen because the value of the function on these points is close. This allows us to pick sets of points E_k without saying anything about the continuity property of $f(x)$. This way the

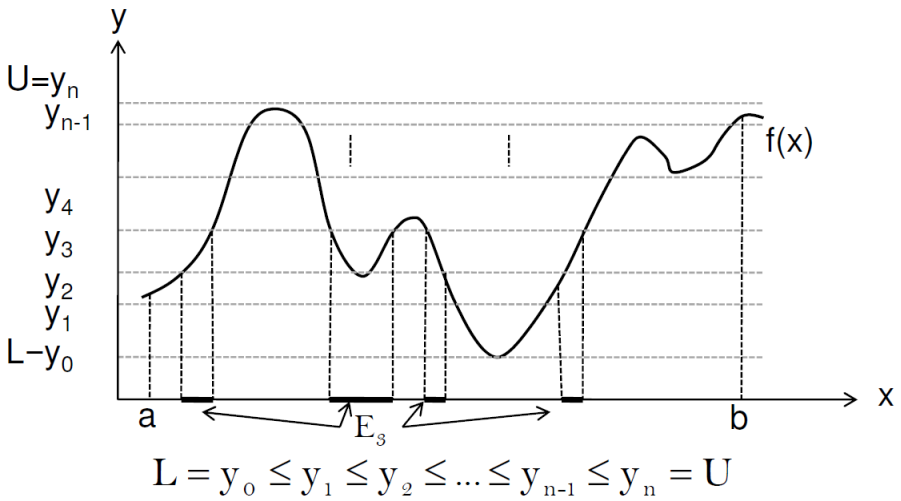

Figure 2.2: Lebesgue integral formalization.

Lebesgue integral is able to handle a class of functions far larger than the Riemann definition. It is important to point out here that even though in this example we used the real line as the domain of the function f, the Lesbegue integral puts no such restriction on the domain of the functions. The Lebesgue integral is based on the concept of measure (which in this example was the length of the real interval E_k). In general the Lebesgue integral is defined for a class of functions called *measurable functions*, which are well-behaved functions between measurable spaces. Several texts contain very good descriptions of Lebesgue integral formalization [8][63]. In this thesis research, we formally define the statistical properties of the random variables such as their expectation based on Lebesgue's integration theory.

2.5 The HOL Theorem Prover

The HOL [26] system is a general purpose theorem prover whose underlying logic is called HOL. It is based on meta language (ML), which is a functional programming language. HOL is a descendant of LCF system [25] and supports both forward and backward proofs. It does not use decision procedures, and all theorems are proven using basic axioms and inference rules. The proof process consists of applying tactics to proof goals. Tactics are functions used to rewrite and simplify the goals. Each tactic automatically generates a set of elementary inferences required to justify the proof step. Users are allowed to write their own tactics, and such tactics cannot compromise the soundness of the proof because the basic inferences operate on proof states implemented as an abstract data type in ML. Once a theorem is proven, it can be used in other proofs.

Table 2.3 lists HOL versions of mathematical symbols and their explanation. Some of these symbols appear in various definitions and theorems described in this thesis.

HOL	Mathematical	English
\	λ	Lambda abstraction
!	$\forall$	Universal quantification
?	$\exists$	Existential quantification
/\	$\wedge$	Conjunction
\/	$\vee$	Disjunction
==>	$\Rightarrow$	Implication
~	$\neg$ and $-$	Logical and numerical negation
=	= and $\Leftrightarrow$	Equality and "if and only if"
{}	ϕ	Empty Set

Table 2.3: HOL mathematical symbols.

2.6 Probability Theory and Random Variables in HOL

A *measure space* is defined as a triple (Ω, Σ, μ), where Ω is a set, called the *sample space*, Σ represents a σ-algebra of subsets of Ω and the subsets are usually referred to as *measurable sets*, and μ is a *measure* with domain Σ [24]. A *probability space* is a measure space (Ω, Σ, P) such that the measure, referred to as the probability and denoted by P, of the sample space is 1.

Hurd in [34] formalized some measure theory concepts in HOL to define a measure space as a pair (Σ, μ). Building upon this formalization, the probability space was also defined in HOL as a pair $(\mathcal{E}, \mathbb{P})$, where the domain of $\mathbb{P}$ is the set $\mathcal{E}$, which is a set of subsets of infinite Boolean sequences $\mathbb{B}^\infty$. Both $\mathbb{P}$ and $\mathcal{E}$ are defined using the Carathéodory's Extension theorem, which ensures that $\mathcal{E}$ is a σ-algebra: closed under complements and countable unions.

A random variable, which is one of the core concepts in probabilistic analysis, is fundamentally a probabilistic function and thus can be modeled in higher-order logic as a deterministic function, which accepts the infinite Boolean sequence as an argument. These deterministic functions make random choices based on the result of popping the top most bit in the infinite Boolean sequence and may pop as many random bits as they need for their computation. When the functions terminate, they return the result along with the remaining portion of the infinite Boolean sequence to be used by other programs. Thus, a random variable which takes a parameter of type α and ranges over values of type β can be represented in HOL by the function $\mathcal{F}$.

$$\mathcal{F} : \alpha \to B^\infty \to \beta \times B^\infty$$

As an example, consider the Bernoulli($\frac{1}{2}$) random variable that returns 1 or 0 with equal probability $\frac{1}{2}$. It can be formalized in HOL as follow [34]

$\vdash$ `bit = (λs.  if shd s then 1 else 0, stl s)`

It accepts an infinite Boolean sequence, `s`, where `shd` and `stl` are the sequence equivalents of the list operation *'head'* and *'tail'*. The formalized $\mathbb{P}$ and $\mathcal{E}$ can be used to verify the basic laws of probability as well as probabilistic properties regarding random variables in the HOL theorem prover. For example:

$\vdash \mathbb{P}$ `{s | fst (bit s) = 1}` $= \frac{1}{2}$

where the HOL function `fst` selects the first component of a pair and $\{x|C(x)\}$ represents a set of all x that satisfy the condition C. It is important to note here that, since the probability measure $\mathbb{P}$ is only defined on sets in $\mathcal{E}$, it is absolutely necessary to verify that the set that appears in a probabilistic property is in $\mathcal{E}$ before we can formally verify that property in HOL. For the above example, this condition translates to the verification of `{s | fst (bit s) = 1}` $\in \mathcal{E}$.

The above approach has been successfully used to formalize and verify most of the commonly used discrete random variables [34].

In this work, a discrete random variable is an algorithm which satisfies probabilistic termination. Probabilistic termination refers to the fact that an algorithm terminates with a probability of one. Hurd formalized four probabilistic algorithms using well formed recursive functions and probabilistic programming constructs such as probabilistic while and until loops [34]. These probabilistic algorithms have uniform, bernoulli, binomial, and geometric probability mass functions. Hasan [29], Building on Hurd's work, formalized a standard uniform random variable as a special case of

the discrete version of a uniform random variable, as given in Equation 2.6.

$$\lim_{n\to\infty}(\lambda n.\sum_{k=0}^{n-1}(\frac{1}{2})^{k+1}X_k) \tag{2.6}$$

where $(\lambda n.\sum_{k=0}^{n-1}(\frac{1}{2})^{k+1}X_k)$ represents the discrete uniform random variable. Hasan's formal specification of the standard uniform random variable in HOL is given in Definition 2.1, and is based on Equation 2.6.

Definition: 2.1 *Standard Uniform Random Variable* [29]

$\vdash \forall$ `s.  std_unif_cont s =` lim `(λn.  fst (std_unif_disc n s))`

The function `std_unif_disc` is a standard discrete uniform random variable in HOL. It takes two arguments, a natural number (`n`:num) and an infinite sequence of random bits (`s`:num→bool). The function utilizes these two arguments and returns a pair of type (real, num→bool). The real value corresponds to the value of the random variable and the second element in the pair is the unused portion of the infinite boolean sequence. The function `fst` takes a pair as input and returns the first element of the pair, and the function `lim P` in HOL is the formalization of the limit of a real sequence `P`.

Building upon the above mentioned probability theory framework, an approach for the formalization of continuous random variables has been presented in [29]. The main idea is based on the concept of the Inverse Transform Method (ITM) [20], according to which, the random variable X, for any continuous cumulative distribution function (CDF) F, can be defined as $X = F^{-1}(U)$, where F^{-1} is the inverse function of F, and U represents the Standard Uniform random variable. The formal proof of this proposition is based on the CDF characteristic of the Standard Uniform random variable and some of the CDF properties [29]. ITM allows us to formalize any continuous random variable, which has a well-defined CDF, in terms of a formalized

Standard Uniform random variable (`std_unif_rv`). Based on this approach, the CDFs and higher-order-logic definitions of three continuous random variables are given in Table 2.4 [29].

Distribution	**CDF**	**Formalized Random Variable**
Uniform(a, b)	$\begin{cases} 0 & \text{if } x \leq a; \\ \frac{x-a}{b-a} & \text{if } a < x \leq b; \\ 1 & \text{if } b < x. \end{cases}$	$\vdash \forall s\ l.\ uniform\_rv\ a\ b\ s\ = (b-a)(std\_unif\_rv\ s) + a$
Triangular$(0, a)$	$\begin{cases} 0 & \text{if } x \leq 0; \\ (\frac{2}{a}(x - \frac{x^2}{2a})) & \text{if } x < a; \\ 1 & \text{if } a \leq x. \end{cases}$	$\vdash \forall s\ a\ .\ triangular\_rv\ l\ s\ = a(1 - \sqrt{1 - std\_unif\_rv\ s})$
Exponential(l)	$\begin{cases} 0 & \text{if } x \leq 0; \\ 1 - e^{-lx} & \text{if } 0 < x. \end{cases}$	$\vdash \forall s\ l.\ exp\_rv\ l\ s\ = -\frac{1}{l} ln(1 - std\_unif\_rv\ s)$

Table 2.4: Continuous random variables in HOL

2.7 Lebesgue Integration in HOL

Lebesgue integration is based on the concept of measure and is defined for a class of functions called *measurable functions*, which are well-behaved functions between measurable spaces. The higher-order-logic definition of the Lebesgue integral utilizes the concepts of *indicator function*, *positive simple-function* and *measurable functions* [24].

In HOL Lebesgue integration theory [45], a function f defined over a measure space (Ω, Σ, μ) is considered integrable if and only if $\int_\Omega |f| d\mu < \infty$ or equivalently $\int_\Omega f^+ d\mu < \infty$ and $\int_\Omega f^- d\mu < \infty$. Positive continuous random variables in HOL are such well-behaved functions. We utilize the following convergence of a non-negative integrable function f property to verify the first and second moment relation in Chapter 3.

Theorem: *If f is any non-negative integrable function, there exists a sequence of*

positive simple functions (f_n) *such that* $\forall\ n\ x.\ f_n(x) \leq f_{n+1}(x) \leq f(x)$ *and* $\forall\ x.\ f_n(x) \to f(x)$, *and*

$$\int_{\Omega} f d\mu = \lim_{n} \int_{\Omega} f_n d\mu \tag{2.7}$$

In the next chapter, we will present formalization of statistical properties of continuous random variables and their verification for well-known and commonly used bounded and unbounded continuous random variables.

Chapter 3

Statistical Properties of Continuous Random Variables

Reliability and lifetime behaviour of engineering systems is modeled using positive valued continuous random variables. Their probabilistic and statistical properties are needed in the overall reliability analysis of a system. In this chapter, the higher-order logic formalization of statistical properties of continuous random variables is presented. We also describe the methodology we used for the verification of statistical properties of well-known and commonly used bounded (Uniform and Triangular) and unbounded (Exponential) continuous random variables in a theorem proving environment.

First we verify general relations for the expectation and the second moment for bounded and unbounded random variables. These relations then allow us to verify the statistical properties such as expectation, second moment and variance of continuous random variables used in the reliability analysis in the sound core of a theorem prover.

3.1 Introduction

The main idea of conducting probabilistic analysis of systems using theorem proving, initially proposed in [29], consists of modeling of the system and its unpredictable environment using formalized discrete and continuous random variables. The probabilistic and statistical properties of random variables are then used to reason about system characteristics, such as downtime, availability, number of failures, capacity, and cost, in a theorem prover. The analysis carried out in this way is free from any approximation issues or flaws due to the mathematical nature of the models and the inherent soundness of the theorem proving approach.

The milestones achieved so far, in this endeavor of developing a complete theorem proving based probabilistic analysis framework that is capable of analyzing any hardware or software system, include the formalization of probability theory [34], the ability to formalize discrete and continuous random variables and verify their probabilistic properties [34, 29] and the ability to verify statistical properties of discrete random variables [29].

One of the contributions of this thesis is that it presents a higher-order logic formalization of statistical properties of continuous random variables. These statistical properties, such as expectation or first moment of a random variable, play a major role in decision making as they tend to summarize the probability distribution characteristics of a random variable in a single number. Thus, the contribution of this chapter paves the way to formally analyze many engineering and physical science systems with continuous random components in a theorem prover. Some of the interesting examples include the performance analysis of *computer arithmetic systems* like floating-point arithmetic [64], where the Uniform random variable can be used to model the roundoff error, algorithms that utilize continuous random variables, such as

the *Balls and Bins with feedback* [46] and network protocols by modeling the request arrival rates by the exponential random variables.

The most commonly used definition of expectation, for a continuous random variable X, is the probability density-weighted integral over the real line [46].

$$E[X] = \int_{-\infty}^{+\infty} x f_X(x) dx \tag{3.1}$$

The function f_X in the above equation represents the probability density function (PDF) of X and the integral is the well-known Reimann integral. The above definition is only limited to continuous random variables that have a well-defined PDF. A more general, but not so commonly used, definition of expectation for a random variable X, defined on a probability space (Ω, Σ, P) [24], is as follows:

$$E[X] = \int_{\Omega} X dP \tag{3.2}$$

This definition utilizes the Lebesgue integral and is general enough to cater for both discrete and continuous random variables. The reason behind its limited usage in the probabilistic analysis domain is the complexity of solving the Lebesgue integral, which takes its foundations from the measure theory that most engineers and computer scientists are not familiar with.

The obvious advantage of using Equation (3.1) is the user familiarity with Reimann integral that usually facilitates the reasoning process regarding the expectation properties in the theorem proving based probabilistic analysis approach. On the other hand, it requires extended real numbers, $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$, whereas all the foundational work regarding theorem proving based probabilistic analysis has been built upon the standard real numbers $\mathbb{R}$, formalized by Harrison [28]. Thus,

the formalization of the expectation definition, given in Equation (3.1), and making it compatible with the available formal probabilistic analysis infrastructure would require creating a new data type $\overline{\mathbb{R}}$, and re-verifying the already proven results in a theorem prover for this new data-type, which is a considerable amount of work. The expectation definition, given in Equation (3.2), does not involve extended real numbers; it accommodates infinite limits with ease due to the inherent nature of the Lebesgue integral. It also offers a more general solution. The limitation, however, is the compromise on the interactive reasoning effort, as it is not a straightforward task for a user to build on this definition to formally verify the expectation of a random variable.

In this chapter, we address the above mentioned limitation of using Lebesgue integration for defining expectation and higher moments. Starting from Equation (3.2), we mainly utilize the properties of the Lebesgue integral to formally verify two simplified expressions for the expectation. The first one is for the case when the random variable X is bounded in the positive interval $[a, b]$

$$E[X] = \lim_{n\to\infty}\left[\sum_{i=0}^{2^n-1}(a+\frac{i}{2^n}(b-a))P\left\{a+\frac{i}{2^n}(b-a) \le X < a+\frac{i+1}{2^n}(b-a)\right\}\right] \tag{3.3}$$

and the second one is for an unbounded positive random variable [24].

$$E[X] = \lim_{n\to\infty}\left[\sum_{i=0}^{n2^n-1}\frac{i}{2^n}P\left\{\frac{i}{2^n} \le X < \frac{i+1}{2^n}\right\} + nP(X \ge n)\right] \tag{3.4}$$

Both of the above expressions do not involve any concepts from Lebesgue integration theory and are based on the well-known arithmetic operations like summation, limit of a real sequence, etc. Thus, users can simply utilize them, instead of Equation (3.2), to reason about the expectation properties of their random variables and gain

the benefits of the original Lebesgue based definition. It is also important to note that we have a different expression for the bounded case in order to facilitate the formal reasoning about the probability term, which becomes very challenging to reason about if the unbounded expectation equation is used for a bounded random variable.

Similarly, we also verified two similar simplified expressions for the second moments (E[X^2]) of bounded and unbounded random variables given in Equations 3.5 and 3.6.

$$E[X^2] = \lim_{n\to\infty}\left[\sum_{i=0}^{2^n-1}(a+\frac{i}{2^n}(b-a))^2 P\left\{a+\frac{i}{2^n}(b-a) \le X < a+\frac{i+1}{2^n}(b-a)\right\}\right] \tag{3.5}$$

$$E[X^2] = \lim_{n\to\infty}\left[\sum_{i=0}^{n2^n-1}(\frac{i}{2^n})^2 P\left\{\frac{i}{2^n} \le X < \frac{i+1}{2^n}\right\} + nP(X \ge n)\right] \tag{3.6}$$

To demonstrate the effectiveness of the above expressions, we utilize them for the formal verification of the expected values and second moments for the commonly used continuous random variables Uniform, Triangular and Exponential. Besides being illustrative examples, these results can be essentially utilized in conducting the formal performance analysis of many systems that utilize these random variables.

The work described in this chapter is done using the HOL theorem prover [26], which is based on higher-order logic. The main motivation behind this choice is the fact that most of the work that we build upon is developed in HOL, such as the formalization of the real number theory [28], probability theory [34], continuous random variables [29] and Lebesgue integration [14]. Though, it is important to note here that the ideas presented in this chapter are not specific to the HOL theorem prover and can be adapted to any other higher-order-logic theorem prover as well, such as Isabelle, Coq or PVS.

The rest of the chapter is organized as follows: Section 3.2 presents the formalization of the definitions of important statistical properties of random variables in HOL. Section 3.3 describes the verification of the simplified expressions for the expectation and the second moment of random variables. Section 3.4 describes the verification of the expectation, the second moment, and the variance of of Uniform, Triangular and Exponential random variables. The chapter concludes with a summary of conclusions in Section 3.5.

3.2 Formalization of Statistical Properties of Continuous Random Variables

In this section, we present the formalization of the definitions of several important statistical properties of random variables in HOL. Statistical properties such as moments and variances are often used in reliability theory to summarize the properties of systems lifetime distributions. The most commonly known statistical property, the first moment or expectation, is also known as the mean-time-to-failure or MTTF in reliability theory. The expectation and higher moments are all measures of central tendency.

These statistical properties are summarized in Table 3.1. In these formalized definitions, rv is a random variable. m represents a probability space defined as: $m = (\mathcal{U}, \mathcal{E}, \mathbb{P})$, where $\mathcal{U}$ is a sample space, $\mathcal{E}$ is a set of events, and $\mathbb{P}$ is the probability measure. The function *expec* represents the expectation or the first moment of the random variable.

The verification of the expectation, second moment and variance relations for the bounded and unbounded random variables begins with the definition of expectation

and second moment given in the second and third row of Table3.1. The functions `expec` and `second_moment` accept a probability space, $(\mathcal{U}, \mathcal{E}, \mathbb{P})$, and a random variable rv that maps infinite Boolean sequences to real numbers. In Hurd's formalization of the probability space $(\mathcal{U}, \mathcal{E}, \mathbb{P})$, $\mathcal{U}$ represents the universal set of all Boolean sequences, as outlined in [29].

Property	**Definition**	**HOL Formalization**
expec. X	$\mathrm{E[X]}=\int_{\mathcal{U}} X d\mathbb{P}$	⊢ ∀m rv. expec m rv = fn_integral m (λx. rv x)
expec. h(X)	$\mathrm{E[h(X)]}=\int_{\mathcal{U}} h(X) d\mathbb{P}$	⊢ ∀m h rv. fun_rv m h rv = expec m (λx. h (rv x))
first moment	$\mu=\mathrm{E[X]}=\int_{\mathcal{U}} X d\mathbb{P}$	⊢ ∀m rv. first_moment m rv = expec m (λx. rv x)
second moment	$\mu_2=\mathrm{E}[X^2]=\int_{\mathcal{U}} X^2 d\mathbb{P}$	⊢ ∀m rv. second_moment m rv = expec m (λx. (rv x) pow 2)
Nth moment	$\mu_N=\mathrm{E}[X^N]=\int_{\mathcal{U}} X^N d\mathbb{P}$	⊢ ∀m rv N. nth_moment m rv N = expec m (λx. (rv x) pow N)
variance	$\sigma^2=\mathrm{E}[(\mathrm{X}\text{-}\mu)^2]$	⊢ ∀m rv. variance m rv = expec m (λx. ((rv x) - expec m rv) pow 2)
standard deviation	σ	⊢ ∀m rv. std_dev m rv = sqrt(variance m rv)
coef. of variation	$\frac{\sigma}{\mu}$	⊢ ∀m rv. coef_of_var m rv = (std_dev m rv)/(expec m rv)
mean absolute deviation	$\mathrm{E}[\lvert X-\mu\rvert]$	⊢ ∀m rv. m_abs_dev m rv = expec m (λx. abs((rv x) - expec m rv))
coef. of skewness	$\alpha_3 = \mathrm{E}[(\frac{X-\mu}{\sigma})^3]$	⊢ ∀m rv. skew m rv = expec m (λx. ((rv x) - expec m rv) pow 3) /((std_dev m rv) pow 3)
coef. of kurtosis	$\alpha_4 = \mathrm{E}[(\frac{X-\mu}{\sigma})^4]$	⊢ ∀m rv. kurt m rv = expec m (λx. ((rv x) - expec m rv) pow 4) /((std_dev m rv) pow 4)

Table 3.1: Statistical properties and their HOL formalizations

3.3 Verification of Expectation and Second Moment Relations

In this section, we utilize the probability and Lebesgue integration theories, described in the previous chapter, to formally verify the expectation and second moment relations for the bounded and unbounded random variables, given in Equations (3.3), (3.4), and (3.5), (3.6), respectively.

We use the definitions of expectation and second moment given in Table 3.1 to reason about the expectation and the second moment of random variables formalized in [34, 29].

The expectation property of bounded random variable is expressed as a higher-order-logic theorem as follows:

Theorem 3.1: *Expectation of Bounded Random Variables*

$$\begin{aligned}
&\vdash \forall\ \mathtt{a\ b\ rv.}\ \ (\mathtt{0} \leq \mathtt{a}) \wedge (\mathtt{a} < \mathtt{b}) \wedge (\forall\ \mathtt{s.}\ \ \mathtt{a} \leq \mathtt{rv\ s} \leq \mathtt{b}) \wedge \\
&\quad (\forall\ \mathtt{x\ y.}\ \ \mathtt{x} < \mathtt{y} \Rightarrow \{\mathtt{s} \mid \mathtt{x} \leq \mathtt{rv\ s} < \mathtt{y}\} \in \mathcal{E}) \Rightarrow \\
&\Bigg(\mathtt{expec}\ (\mathcal{U}, \mathcal{E}, \mathbb{P})\ \mathtt{rv} = \\
&\lim_{\mathtt{n}\to\infty} \left[\sum_{\mathtt{i}=0}^{2^{\mathtt{n}}-1} (\mathtt{a} + \tfrac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a}))\mathbb{P}\left\{\mathtt{s} \;\middle|\; \mathtt{a} + \tfrac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a}) \leq \mathtt{rv\ s} < \mathtt{a} + \tfrac{\mathtt{i}+1}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\right\}\right]\Bigg)
\end{aligned}$$

The first three assumptions state that the random variable rv is bounded in the positive interval $[a, b]$. Whereas, the fourth assumption states that the set involved in this verification is measurable. It is assumed that the sequence (rv_n) is defined as:

$$\mathtt{rv_n(x)} = \sum_{\mathtt{i}=0}^{2^{\mathtt{n}}-1} (\mathtt{a} + \frac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a}))\mathbb{I}_{\left\{\mathtt{s} \;\middle|\; \mathtt{a}+\frac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a}) \leq \mathtt{rv\ s} < \mathtt{a}+\frac{\mathtt{i}+1}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\right\}}(\mathtt{x}) \tag{3.7}$$

where $\mathbb{I}_A(x)$ is a real-valued function of a set A, such that: $\mathbb{I}_A(x) = 1$ if $x \in A$, and $\mathbb{I}_A(x) = 0$ if $x \notin A$.

In order to utilize any definition or property of Lebesgue integration theory with the above theorem, we first need to show that the triple $(\mathcal{U}, \mathcal{E}, \mathbb{P})$ is a measure space with a positive measure. We verified these conditions based on the corresponding theorems available in Hurd's formalization of the probability space $(\mathcal{E}, \mathbb{P})$ along with the definition of measure in [14] under the given assumptions.

The convergence of a positive measurable function to the Lebesgue integral property [14] and the Modus Ponens (MP) rule are then used to split the proof goal of Theorem 3.1 into the following seven subgoals. They correspond to the monotonicity and positive simple-function requirement on rv_n and five other conditions described below [14]:

$$\texttt{mono\_increasing}\left[\sum_{\texttt{i}=0}^{2^{\texttt{n}}-1}(\texttt{a}+\frac{\texttt{i}}{2^{\texttt{n}}}(\texttt{b}-\texttt{a}))\mathbb{I}_{\left\{\texttt{s}\;\middle|\;\texttt{a}+\frac{\texttt{i}}{2^{\texttt{n}}}(\texttt{b}-\texttt{a})\leq\texttt{rv s}<\texttt{a}+\frac{\texttt{i}+1}{2^{\texttt{n}}}(\texttt{b}-\texttt{a})\right\}}(\texttt{x})\right] \tag{3.8}$$

$$\left(\forall \texttt{i}.(\texttt{i}<2^{\texttt{n}})\Rightarrow\left\{\texttt{s}\;\middle|\;\texttt{a}+\frac{\texttt{i}}{2^{\texttt{n}}}(\texttt{b}-\texttt{a})\leq\texttt{rv s}<\texttt{a}+\frac{\texttt{i}+1}{2^{\texttt{n}}}(\texttt{b}-\texttt{a})\right\}\in\mathcal{E}\right) \tag{3.9}$$

$$\left(\forall \texttt{i}.0\leq\texttt{a}+\frac{\texttt{i}}{2^{\texttt{n}}}(\texttt{b}-\texttt{a})\right) \tag{3.10}$$

$$\left(\texttt{FINITE}\{\texttt{i}|\texttt{i}<2^{\texttt{n}}\}\right) \tag{3.11}$$

$$\left[\sum_{\texttt{i}=0}^{2^{\texttt{n}}-1}(\texttt{a}+\frac{\texttt{i}}{2^{\texttt{n}}}(\texttt{b}-\texttt{a}))\mathbb{I}_{\left\{\texttt{s}\;\middle|\;\texttt{a}+\frac{\texttt{i}}{2^{\texttt{n}}}(\texttt{b}-\texttt{a})\leq\texttt{rv s}<\texttt{a}+\frac{\texttt{i}+1}{2^{\texttt{n}}}(\texttt{b}-\texttt{a})\right\}}(\texttt{x})\right]\leq\texttt{rv}(\texttt{x}) \tag{3.12}$$

$$\lim_{\texttt{n}\to\infty}\left[\sum_{\texttt{i}=0}^{2^{\texttt{n}}-1}(\texttt{a}+\frac{\texttt{i}}{2^{\texttt{n}}}(\texttt{b}-\texttt{a}))\mathbb{I}_{\left\{\texttt{s}\;\middle|\;\texttt{a}+\frac{\texttt{i}}{2^{\texttt{n}}}(\texttt{b}-\texttt{a})\leq\texttt{rv s}<\texttt{a}+\frac{\texttt{i}+1}{2^{\texttt{n}}}(\texttt{b}-\texttt{a})\right\}}(\texttt{x})\right]=\texttt{rv}(\texttt{x}) \tag{3.13}$$

$$\exists \mathtt{y}.\ \lim_{\mathtt{n}\to\infty}\left[\sum_{\mathtt{i}=0}^{2^{\mathtt{n}}-1}(\mathtt{a}+\frac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a}))\mathbb{P}\left\{\mathtt{s}\ \middle|\ \mathtt{a}+\frac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\leq \mathtt{rvs} < \mathtt{a}+\frac{\mathtt{i}+1}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\right\}\right] = \mathtt{y} \tag{3.14}$$

The monotonically increasing property in the first subgoal (Equation 3.8) can be verified based on the facts that (1) the indicator function only becomes 1 for one interval or one particular value of i and (2) as the argument of the sequence, i.e., n, increases the intervals become finer and thus the resulting value of the sequence becomes greater and close to the value $rv\ x$. The term multiplied by the indicator function in the summation is in direct proportion with the argument of the sequence n.

The second, third, and fourth subgoals (Equations 3.9, 3.10 and 3.11) correspond to the pre-conditions for the function rv_n to be a positive simple-function. These three subgoals can be discharged based on the fourth assumption of Theorem 3.1, arithmetic reasoning and set theory principles, respectively. The fifth subgoal (Equation 3.12) is true as there is only one i, say i', for which the real value of $rv\ x$ would fall in the interval $[a + \frac{i}{2^n}(b-a), a + \frac{i+1}{2^n}(b-a))$ out of all 2^n possible values for i. Thus the indicator function would be 1 for this particular i only and 0 otherwise, which means that the summation would be equal to $(a + \frac{i'}{2^n}(b-a))$. Now, substituting this value for the summation in the fifth subgoal along with the fact that $rv\ x$ lies in the interval $[a + \frac{i'}{2^n}(b-a), a + \frac{i'+1}{2^n}(b-a))$ leads to its verification. The sixth subgoal (Equation 3.13) can also be discharged based on the reasoning used to discharge the previous subgoal along with the monotonicity of the given sequence and the definition of limit of a real sequence. Finally, the real sequence in the seventh subgoal (Equation 3.14) can be verified to be convergent by verifying that it is monotonic, just like the sequence in the first subgoal since the probability term will only be non-zero for one

particular value of i, and has an upper bound b, since the value of i is always less than 2^n and the maximum value that the probability term can take is 1. This also concludes the verification of Theorem 3.1.

The second moment relation for a bounded random variable, given in Equation 3.5, is verified in Theorem 3.2, as follows:

Theorem 3.2: *Second Moment of Bounded Random Variables*

$$\begin{aligned}
&\vdash \forall\ \mathtt{a\ b\ rv.}\ \ (\mathtt{0} \leq \mathtt{a}) \wedge (\mathtt{a} < \mathtt{b}) \wedge (\forall\ \mathtt{s.}\ \ \mathtt{a} \leq \mathtt{rv\ s} \leq \mathtt{b}) \wedge \\
&\quad (\forall\ \mathtt{x\ y.}\ \ \mathtt{x} < \mathtt{y} \Rightarrow \{\mathtt{s} \mid \mathtt{x} \leq \mathtt{rv\ s} < \mathtt{y}\} \in \mathcal{E}) \Rightarrow \\
&\Big(\mathtt{second_moment}\ (\mathcal{U}, \mathcal{E}, \mathbb{P})\ \mathtt{rv} = \\
&\lim_{\mathtt{n}\to\infty}\left[\sum_{\mathtt{i}=0}^{2^{\mathtt{n}}-1}(\mathtt{a} + \tfrac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a}))^2 \mathbb{P}\left\{\mathtt{s} \;\middle|\; \mathtt{a} + \tfrac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a}) \leq \mathtt{rv\ s} < \mathtt{a} + \tfrac{\mathtt{i}+1}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\right\}\right]\Big)
\end{aligned}$$

The detailed proof steps for the verification of the second moment relation for a bounded continuous random variable, given in Theorem 3.2, are described in [2] is as follows:

The expectation relation for an unbounded random variable, given in Equation 3.4, is verified in Theorem 3.3 as follows:

Theorem 3.3: *Expectation of an Unbounded Random Variable*

$$\begin{aligned}
&\vdash \forall\ \mathtt{rv.}\ \ (\forall\ \mathtt{s.}\ \ \mathtt{0} \leq \mathtt{rv\ s}) \wedge (\forall\ \mathtt{x.}\ \ \{\mathtt{s} \mid \mathtt{rv\ s} \geq \mathtt{x}\} \in \mathcal{E}) \\
&\quad (\forall\ \mathtt{x\ y.}\ \ \mathtt{x} < \mathtt{y} \Rightarrow \{\mathtt{s} \mid \mathtt{x} \leq \mathtt{rv\ s} < \mathtt{y}\} \in \mathcal{E}) \Rightarrow \\
&\Big(\mathtt{expec}\ (\mathcal{U}, \mathcal{E}, \mathbb{P})\ \mathtt{rv} = \\
&\lim_{\mathtt{n}\to\infty}\left[\sum_{\mathtt{i}=0}^{\mathtt{n}2^{\mathtt{n}}-1}(\tfrac{\mathtt{i}}{2^{\mathtt{n}}})\mathbb{P}\left\{\mathtt{s} \;\middle|\; \tfrac{\mathtt{i}}{2^{\mathtt{n}}} \leq \mathtt{rv\ s} < \tfrac{\mathtt{i}+1}{2^{\mathtt{n}}}\right\} + \mathtt{n}\mathbb{P}\left\{\mathtt{s} \;\middle|\; \mathtt{rv\ s} \geq\ \mathtt{n}\right\}\right]\Big)
\end{aligned}$$

As in Theorem 3.1, the function `expec` accepts a probability space, $(\mathcal{U}, \mathcal{E}, \mathbb{P})$, and a random variable rv that maps infinite Boolean sequences to real numbers [29]. A detailed description of the proof can be found in [2]

Similarly, the second moment relation for an unbounded random variable, given in Equation 3.6, is verified in Theorem 3.4, as follows:

Theorem 3.4: *Second Moment of an Unbounded Random Variable*

$$\vdash \forall\ \mathtt{rv}.\ \ (\forall\ \mathtt{s}.\ \ 0 \leq \mathtt{rv\ s}) \wedge (\forall\ \mathtt{x}.\ \ \{\mathtt{s} \mid \mathtt{rv\ s} \geq \mathtt{x}\} \in \mathcal{E})$$
$$(\forall\ \mathtt{x\ y}.\ \ \mathtt{x} < \mathtt{y} \Rightarrow \{\mathtt{s} \mid \mathtt{x} \leq \mathtt{rv\ s} < \mathtt{y}\} \in \mathcal{E}) \Rightarrow$$
$$\Bigg(\mathtt{second\_moment}\ (\mathcal{U}, \mathcal{E}, \mathbb{P})\ \mathtt{rv} =$$
$$\lim_{\mathtt{n}\to\infty}\left[\sum_{\mathtt{i}=0}^{\mathtt{n}2^{\mathtt{n}}-1}\left(\frac{\mathtt{i}}{2^{\mathtt{n}}}\right)^2 \mathbb{P}\left\{\mathtt{s} \;\middle|\; \frac{\mathtt{i}}{2^{\mathtt{n}}} \leq \mathtt{rv\ s} < \frac{\mathtt{i}+1}{2^{\mathtt{n}}}\right\} + \mathtt{n}\mathbb{P}\left\{\mathtt{s} \;\middle|\; \mathtt{rv\ s} \geq\ \mathtt{n}\right\}\right]\Bigg)$$

The detailed proof steps of Theorem 3.4 are very similar to Theorem 3.2 as verification of both the expressions required very similar reasoning [2].

Both the bounded and unbounded random variables play an important role in the modeling of the lifetime behavior of engineering system components. The expressions formally verified in this section do not involve any concepts from Lebesgue integration theory and are based on the well-known arithmetic operations like summation, limit of a real sequence, etcetera. This allows us to formally reason about the statistical properties of random variables commonly used in reliability analysis in a relatively simple manner while at the same time gain the benefits of the original rather complicated Lebesgue based definition.

3.4 Expectation, Second Moment and Variance of Continuous Random Variables

To illustrate the effectiveness of the expectation and the second moment relations, proved in the previous section, we now utilize them to verify the expectation, second moment and variance of three continuous random variables, i.e., Uniform, Triangular and Exponential.

3.4.1 Uniform Random Variable

The expectation relation for the continuous Uniform random variable bounded in the interval $[a, b]$ can be formalized as follows:

Theorem 3.5: *Expectation of the Uniform(a,b) Random Variable*

$$\vdash \forall\ \texttt{a b.}\quad \texttt{(0} \leq \texttt{a)} \wedge \texttt{(a} < \texttt{b)} \Rightarrow$$
$$\left(\texttt{expec}\ (\mathcal{U}, \mathcal{E}, \mathbb{P})\ \texttt{(uniform\_rv a b) =}\ \tfrac{a+b}{2}\right)$$

In Theorem 3.5, `uniform_rv` represents the Uniform random variable formalized using inverse transform method [20] as:

0 if $x \leq a$; $\frac{x-a}{b-a}$ if $a < x \leq b$; 1 if $b < x$.

$$\vdash \forall s\ l.\ uniform\_rv\ a\ b\ s\ =\ \ (b-a)(std\_unif\_rv\ s) + a$$

where `std_unif_rv` is the standard Uniform random variable formalized in [29]. Details of its formalization are briefly described in Chapter 2, Section 2.6 (Table 2.4) of this thesis.

In order to utilize Theorem 3.1 to reason about the correctness of the above theorem, we first verify that the Uniform random variable satisfies all pre-conditions, given in Theorem 3.1, based on the theorems given in [29]. Next, we rewrite the probability term in Theorem 3.1, using the CDF properties of the Uniform random variable to simplify our proof goal as follows:

$$\lim_{\texttt{n}\to\infty}\left[\sum_{\texttt{i=0}}^{2^{\texttt{n}}-1}(\texttt{a} + \frac{\texttt{i}}{2^{\texttt{n}}}(\texttt{b}-\texttt{a}))\left(\frac{\texttt{a} + \frac{\texttt{i+1}}{2^{\texttt{n}}}(\texttt{b}-\texttt{a}) - \texttt{a}}{\texttt{b}-\texttt{a}} - \frac{\texttt{a} + \frac{\texttt{i}}{2^{\texttt{n}}}(\texttt{b}-\texttt{a}) - \texttt{a}}{\texttt{b}-\texttt{a}}\right)\right] = \frac{\texttt{a}+\texttt{b}}{2} \tag{3.15}$$

The above subgoal can now be discharged using arithmetic reasoning, along with the properties of summation of a real sequence and the limit of a real sequence. This also concludes the verification of Theorem 3.5.

Theorem 3.6: *Second Moment of the Uniform(a,b) Random Variable*

$$\vdash \forall\ \mathtt{a\ b.}\quad (\mathtt{0} \leq \mathtt{a}) \wedge (\mathtt{a} < \mathtt{b}) \Rightarrow \left(\mathtt{second\_moment}\ (\mathcal{U}, \mathcal{E}, \mathbb{P})\ (\mathtt{uniform\_rv\ a\ b}) = \frac{a^2+ab+b^2}{3}\right)$$

We start the proof process by rewriting the left hand side of the proof goal of Theorem 3.6 using the general second moment theorem for bounded random variables (Theorem 3.1).

$$\lim_{\mathtt{n}\to\infty}\left[\sum_{\mathtt{i}=0}^{2^{\mathtt{n}}-1}(\mathtt{a}+\tfrac{(\mathtt{b}-\mathtt{a})\mathtt{i}}{2^{\mathtt{n}}})^2\mathbb{P}\left\{\mathtt{s}\ \middle|\ \mathtt{a}+\tfrac{(\mathtt{b}-\mathtt{a})\mathtt{i}}{2^{\mathtt{n}}} \leq (\mathtt{uniform\_rv\ a\ b})\ \mathtt{s} < \mathtt{a}+\tfrac{(\mathtt{b}-\mathtt{a})(\mathtt{i}+1)}{2^{\mathtt{n}}}\right\}\right] = \tfrac{\mathtt{a}^2+\mathtt{ab}+\mathtt{b}^2}{3}$$

Then using set theory properties and the definition of `CDF` of the continuous Uniform random variable, we show that

$$\mathbb{P}\left\{\mathtt{s}\ \middle|\ \mathtt{a}+\tfrac{(\mathtt{b}-\mathtt{a})\mathtt{i}}{2^{\mathtt{n}}} \leq (\mathtt{uniform\_rv\ a\ b})\ \mathtt{s} < \mathtt{a}+\tfrac{(\mathtt{b}-\mathtt{a})(\mathtt{i}+1)}{2^{\mathtt{n}}}\right\} = \left[\frac{\mathtt{a}+\frac{(\mathtt{b}-\mathtt{a})(\mathtt{i}+1)}{2^{\mathtt{n}}}-\mathtt{a}}{(\mathtt{b}-\mathtt{a})} - \frac{\mathtt{a}+\frac{(\mathtt{b}-\mathtt{a})(\mathtt{i})}{2^{\mathtt{n}}}-\mathtt{a}}{(\mathtt{b}-\mathtt{a})}\right]$$

We then rewrite the left hand side of the subgoal with the above result and arrive at the following subgoal.

$$\lim_{\mathtt{n}\to\infty}\left[\sum_{\mathtt{i}=0}^{2^{\mathtt{n}}-1}(\mathtt{a}+\tfrac{(\mathtt{b}-\mathtt{a})\mathtt{i}}{2^{\mathtt{n}}})^2\left[\frac{\mathtt{a}+\frac{(\mathtt{b}-\mathtt{a})(\mathtt{i}+1)}{2^{\mathtt{n}}}-\mathtt{a}}{(\mathtt{b}-\mathtt{a})} - \frac{\mathtt{a}+\frac{(\mathtt{b}-\mathtt{a})(\mathtt{i})}{2^{\mathtt{n}}}-\mathtt{a}}{(\mathtt{b}-\mathtt{a})}\right]\right] = \tfrac{\mathtt{a}^2+\mathtt{ab}+\mathtt{b}^2}{3}$$

This subgoal involves limit and summation on the left hand side. Using the property of square of sum of two functions, we further simplify the left hand side and reduce it to a sum of the following three limit expressions.

$$\lim_{\mathtt{n}\to\infty}\sum_{\mathtt{i}=0}^{2^{\mathtt{n}}-1}\ \tfrac{\mathtt{a}^2}{2^{\mathtt{n}}} + \lim_{\mathtt{n}\to\infty}\sum_{\mathtt{i}=0}^{2^{\mathtt{n}}-1}\ \tfrac{2\mathtt{a}(\mathtt{b}-\mathtt{a})\mathtt{i}}{2^{2\mathtt{n}}} + \lim_{\mathtt{n}\to\infty}\sum_{\mathtt{i}=0}^{2^{\mathtt{n}}-1}\ \tfrac{(\mathtt{b}-\mathtt{a})^2\mathtt{i}^2}{2^{3\mathtt{n}}} = \tfrac{\mathtt{a}^2+\mathtt{ab}+\mathtt{b}^2}{3}$$

Then we show that these three limits exist and are given by:

$\lim_{n\to\infty} \sum_{i=0}^{2^n-1} \frac{a^2}{2^n} = a^2$, $\lim_{n\to\infty} \sum_{i=0}^{2^n-1} \frac{2a(b-a)i}{2^{2n}} = ab - a^2$, and

$\lim_{n\to\infty} \sum_{i=0}^{2^n-1} \frac{(b-a)^2 i^2}{2^{3n}} = \frac{(b-a)^2}{3}$ respectively.

The proof of the above three limit expressions involved real, arithmetic and limit theories in HOL. Now using these three results we reduce the left hand side of the subgoal to

$$a^2 + ab - a^2 + \frac{(b-a)^2}{3} = \frac{a^2+ab+b^2}{3}$$

which is easily shown to be equal to the right hand side thus completing the proof.

Theorem 3.7: *Variance of the Uniform(a,b) Random Variable*

$$\vdash \forall\ a\ b.\quad (0 \leq a) \wedge (a < b) \Rightarrow \left(\texttt{variance}\ (\mathcal{U}, \mathcal{E}, \mathbb{P})\ \texttt{(uniform\_rv a b)} = \frac{(b-a)^2}{12}\right)$$

We verified the variance relation for the continuous Uniform random variable by first rewriting the left hand side of the proof goal with the variance of continuous random variable property. Then the resulting subgoal was rewritten with the expectation [30] and the second moment of the Uniform random variable (Theorem 3.6). This reduced the left hand side to:

$$\frac{a^2+ab+b^2}{3} - \left(\frac{a+b}{2}\right)^2 = \frac{(b-a)^2}{12}$$

The above equation was then shown to be true. This completed the proof of the variance of the positive valued continuous Uniform random variable.

3.4.2 Triangular Random Variable

The expectation relation for the continuous Triangular random variable bounded in the interval $[0, b]$ can be formalized as follows:

Theorem 3.8: *Expectation of the Triangular(b) Random Variable*

$$\vdash \forall\ \mathtt{b}.\quad (\mathtt{0} < \mathtt{b}) \Rightarrow \left(\mathtt{expec}\ (\mathcal{U}, \mathcal{E}, \mathbb{P})\ \mathtt{(triangular\_rv\ b)} = \frac{b}{3}\right)$$

In Theorem 3.8, `triangular_rv` represents the Triangular random variable formalized using inverse transform method [20] as:

$$0 \text{ if } x \leq 0;\ (\tfrac{2}{a}(x - \tfrac{x^2}{2a})) \text{if } x < a;\ 1 \text{ if } a \leq x$$

$$\vdash \forall s\ a\ .\ triangular\_rv\ l\ s\ =\ \ a(1 - \sqrt{1 - std\_unif\_rv\ s})$$

where `std_unif_rv` is the standard Uniform random variable. More details of its formalization can be found in Chapter 2 of this thesis.

The verification steps are similar to the ones for Theorem 3.5 and are primarily based on Theorem 3.1 and the CDF of the Triangular random variable.

Theorem 3.9: *Second Moment of the Triangular(b) Random Variable*

$$\vdash \forall\ \mathtt{b}.\quad (\mathtt{0} < \mathtt{b}) \Rightarrow$$
$$\left(\mathtt{second\_moment}\ (\mathcal{U}, \mathcal{E}, \mathbb{P})\ \mathtt{(triangular\_rv\ b)} = \frac{b^2}{6}\right)$$

The Theorem 3.9 proof process begins by rewriting the left hand side of the goal using the second moment theorem for bounded random variables (Theorem 3.2).

$$\lim_{\mathtt{n}\to\infty}\left[\sum_{\mathtt{i}=0}^{2^{\mathtt{n}}-1}(\tfrac{\mathtt{ib}}{2^{\mathtt{n}}})^2\mathbb{P}\left\{\mathtt{s}\ \middle|\ \tfrac{\mathtt{ib}}{2^{\mathtt{n}}} \leq (\mathtt{triangular\_rv\ b})\ \mathtt{s} < \tfrac{(\mathtt{i}+1)\mathtt{b}}{2^{\mathtt{n}}}\right\}\right] = \tfrac{\mathtt{b}^2}{6}$$

Then using set theory properties and the definition of `CDF` of the triangular random variable, we show that

$$\mathbb{P}\left\{\mathtt{s}\ \middle|\ \tfrac{\mathtt{i}}{2^{\mathtt{n}}}\mathtt{b} \leq (\mathtt{triangular\_rv\ b})\ \mathtt{s} < \tfrac{(\mathtt{i}+1)}{2^{\mathtt{n}}}\mathtt{b}\right\}$$
$$= \left[(1 - \tfrac{\mathtt{b}^2(1-\frac{\mathtt{i}+1}{2^{\mathtt{n}}})^2}{\mathtt{b}^2}) - (1 - \tfrac{\mathtt{b}^2(1-\frac{\mathtt{i}}{2^{\mathtt{n}}})^2}{\mathtt{b}^2})\right]$$

We then rewrite the left hand side of the subgoal with the above result and arrive at the following subgoal.

$$\lim_{n\to\infty}\left[\sum_{i=0}^{2^n-1}(\frac{i}{2^n}b)^2\left[(1-\frac{b^2(1-\frac{i+1}{2^n})^2}{b^2})-(1-\frac{b^2(1-\frac{i}{2^n})^2}{b^2})\right]\right]=\frac{b^2}{6}$$

This subgoal involves limit and summation on the left hand side. Using the limit and real theories of HOL, the left hand side of the proof goal was reduced to a sum of the following three limit expressions.

$$\lim_{n\to\infty}\sum_{i=0}^{2^n-1}(-2ib^2)\frac{i^3}{2^{4n}}+\lim_{n\to\infty}\sum_{i=0}^{2^n-1}(-b^2)\frac{i^2}{2^{4n}}+\lim_{n\to\infty}\sum_{i=0}^{2^n-1}(2b^2)\frac{i^2}{2^{3n}}=\frac{b^2}{6}$$

Next we showed these three limits exist and are given by:

$\lim_{n\to\infty}\sum_{i=0}^{2^n-1}(-2ib^2)\frac{i^3}{2^{4n}}=\frac{-b^2}{2}$, $\lim_{n\to\infty}\sum_{i=0}^{2^n-1}(-b^2)\frac{i^2}{2^{4n}}=0$, and
$\lim_{n\to\infty}\sum_{i=0}^{2^n-1}(2b^2)\frac{i^2}{2^{3n}}=\frac{2b^2}{3}$ respectively.

The proof of the above three limit expressions involved real, arithmetic and limit theories in HOL. Then using these three results we reduced the left hand side of the subgoal to

$$\frac{-b^2}{2}+0+\frac{2b^2}{3}=\frac{b^2}{6}$$

which was easily shown to be equal to the right hand side and thus completes the proof.

Theorem 3.10: *Variance of the Triangular(b) Random Variable*

$$\vdash\ \forall\ b.\quad (0<b)\ \Rightarrow\ \left(\texttt{variance}\ (\mathcal{U},\mathcal{E},\mathbb{P})\ \texttt{(triangular\_rv b) =}\ \frac{b^2}{18}\right)$$

The variance relation for the continuous triangular random variable was verified by first rewriting the left hand side with the variance of continuous random variable property. Then the resulting subgoal was rewritten with the expectation and the second moment properties of the triangular random variable. This reduced the left hand side to:

$$\frac{b^2}{6}-(\frac{b}{3})^2=\frac{b^2}{6}$$

The above equation was then shown to be true with some rewriting. This completed the proof of the variance of a continuous triangular random variable.

3.4.3 Exponential Random Variable

The expectation for the continuous Exponential random variable, which is unbounded at the upper end, that is, defined in $[0, \infty)$, can be formalized as follows:

Theorem 3.11: *Expectation of the Exponential(l) Random Variable*

$$\vdash \forall\ \mathtt{a}.\quad (\mathtt{0} < \mathtt{a}) \Rightarrow \left(\mathtt{expec}\ (\mathcal{U}, \mathcal{E}, \mathbb{P})\ \mathtt{(exp\_rv\ a)} = \tfrac{1}{\mathtt{a}}\right)$$

In Theorem 3.11, `exp_rv` represents the Exponential random variable formalized using inverse transform method [20] as:

0 if $x \leq 0$; 1 - e^{-lx} if $0 < x$

$$\vdash \forall s\ l.\ exp\_rv\ l\ s\ =\ -\tfrac{1}{l} ln(1 - std\_unif\_rv\ s)$$

where `std_unif_rv` is the standard Uniform random variable. Chapter 2 of this thesis contains more details of its formalization.

Due to its unbounded nature, we use Theorem 3.3 to reason about the expectation of Exponential random variable. Now, after rewriting the probability term and some arithmetic simplification, we get the following subgoal:

$$\lim_{\mathtt{n}\to\infty} \left[\left(1 - \mathtt{e}^{-\frac{\mathtt{a}}{2^{\mathtt{n}}}}\right)\left(\sum_{\mathtt{i}=0}^{\mathtt{n}2^{\mathtt{n}}-1} \frac{\mathtt{i}}{2^{\mathtt{n}}}\mathtt{e}^{-\mathtt{a}\frac{\mathtt{i}}{2^{\mathtt{n}}}}\right) + \mathtt{n}\mathtt{e}^{-\mathtt{an}}\right] = \frac{1}{\mathtt{a}} \tag{3.16}$$

which can be broken into the following two subgoals.

$$\lim_{\mathtt{n}\to\infty} \left(\mathtt{n}\mathtt{e}^{-\mathtt{an}}\right) = 0 \tag{3.17}$$

$$\lim_{\mathtt{n}\to\infty} \left[\left(\frac{1 - \mathtt{e}^{-\frac{\mathtt{a}}{2^{\mathtt{n}}}}}{2^{\mathtt{n}}}\right)\left(\sum_{\mathtt{i}=0}^{\mathtt{n}2^{\mathtt{n}}-1} \mathtt{i}(\mathtt{e}^{-\frac{\mathtt{a}}{2^{\mathtt{n}}}})^{\mathtt{i}}\right)\right] = \frac{1}{\mathtt{a}} \tag{3.18}$$

We proceed with the verification of the first subgoal by rewriting the exponential term e^{-an} as $(1+x)^{-n}$, where $x > 0$. Next, we verify that the term $(1+x)^n$ is greater than $1 + nx + \frac{1}{2}n(n-1)x^2$, for all values of n, as the latter represents a truncated form of its Binomial expansion. This fact leads us to verify that the value of the real sequence $(\lambda n.n(1+x)^{-n})$ will be less than the real sequence $(\lambda n.n(\frac{1}{2}n(n-1)x^2)^{-1})$ for all values of n. This reasoning allows us to discharge the first subgoal, given in Equation (3.17), as the limit value of the real sequence $(\lambda n.n(\frac{1}{2}n(n-1)x^2)^{-1}) = (\lambda n.\frac{2}{x^2(n-1)})$ is 0.

In order to simplify the verification of the second subgoal, given in Equation (3.18), we first evaluate the summation term by verifying the summation of a finite arithmetic-geometric series in HOL.

$$\sum_{k=0}^{n} kq^k = \frac{q}{(1-q)^2}(1-q^n) - \frac{nq^{n+1}}{1-q} \tag{3.19}$$

The above relationship allows us to rewrite the second subgoal as follows:

$$\lim_{n\to\infty}\left(\frac{e^{-\frac{a}{2^n}}(1-e^{-an})}{2^n(1-e^{-\frac{a}{2^n}})} - ne^{-an}\right) = \frac{1}{a} \tag{3.20}$$

Now, Equation (3.17) and the already proved fact that the limit value of the real sequence $(\lambda n.e^{-ln})$ is 0 allows us to simplify the above subgoal as follows.

$$\lim_{n\to\infty}\left(\frac{e^{-\frac{a}{2^n}}}{2^n(1-e^{-\frac{a}{2^n}})}\right) = \frac{1}{a} \tag{3.21}$$

We reason about the correctness of the above limit by first evaluating the following limit relationship.

$$\lim_{x\to 0}\left(\frac{xe^{-ax}}{(1-e^{-ax})}\right) = \frac{1}{a} \tag{3.22}$$

The proof of the above equation is primarily based on the L'Hopital's Rule, which we also verified in HOL as part of this thesis. Now, the variable `x` in Equation (3.22) can be specialized to $\frac{1}{2^n}$. This expression along with the definitions of limit of a real sequence and the limit of a function when its arguments approaches a real value leads to the verification of the remaining subgoal, given in Equation (3.21). This also concludes the proof of Theorem 3.11.

Theorem 3.12: *Second Moment of the Exponential(m) Random Variable*

$$\vdash \forall\ \mathtt{m}.\quad (\mathtt{0} < \mathtt{m}) \Rightarrow \left(\mathtt{second\_moment}\ (\mathcal{U}, \mathcal{E}, \mathbb{P})\ \mathtt{(exp\_rv\ m)} = \tfrac{2}{\mathtt{m}^2}\right)$$

We start the proof process by rewriting the left hand side using the general second moment theorem for the unbounded random variables (Theorem 3.4).

$$\lim_{\mathtt{n}\to\infty} \sum_{\mathtt{i}=0}^{\mathtt{n}2^{\mathtt{n}}-1} (\tfrac{\mathtt{i}}{2^{\mathtt{n}}})^2 \mathbb{P}\left\{\mathtt{s} \;\middle|\; \tfrac{\mathtt{i}}{2^{\mathtt{n}}} \leq (\mathtt{exp\_rv\ m})\ \mathtt{s} < \tfrac{\mathtt{i}+1}{2^{\mathtt{n}}}\right\}$$
$$+\mathbb{P}\left\{\mathtt{s} \;\middle|\; \mathtt{n} \leq (\mathtt{exp\_rv\ m})\ \mathtt{s}\right\} = \tfrac{2}{\mathtt{m}^2}$$

Then using set theory properties and the definition of CDF of the Exponential random variable, we show that

$$\mathbb{P}\left\{\mathtt{s} \;\middle|\; \tfrac{\mathtt{i}}{2^{\mathtt{n}}} \leq (\mathtt{exp\_rv\ m})\ \mathtt{s} < \tfrac{\mathtt{i}+1}{2^{\mathtt{n}}}\right\} + \mathtt{n}\mathbb{P}\left\{\mathtt{s} \;\middle|\; \mathtt{n} \leq (\mathtt{exp\_rv\ m})\ \mathtt{s}\right\}$$
$$= \left[(\mathtt{e}^{-\mathtt{m}\frac{\mathtt{i}}{2^{\mathtt{n}}}})(\mathtt{1} - \mathtt{e}^{-\frac{\mathtt{m}}{2^{\mathtt{n}}}}) + \mathtt{n}\mathtt{e}^{-\mathtt{m}\mathtt{n}}\right]$$

We then rewrite the left hand side of the subgoal with the above result and arrive at the following subgoal.

$$\lim_{\mathtt{n}\to\infty} \left[\sum_{\mathtt{i}=0}^{\mathtt{n}2^{\mathtt{n}}-1} (\tfrac{\mathtt{i}}{2^{\mathtt{n}}})^2 (\mathtt{e}^{-\mathtt{m}\frac{\mathtt{i}}{2^{\mathtt{n}}}})(\mathtt{1} - \mathtt{e}^{-\frac{\mathtt{m}}{2^{\mathtt{n}}}}) + \mathtt{n}\mathtt{e}^{-\mathtt{m}\mathtt{n}}\right] = \tfrac{2}{\mathtt{m}^2}$$

In order to evaluate the limit terms, we first prove the following sum of a sequence containing terms of type $(\mathtt{i}^2\mathtt{P}^{\mathtt{i}})$.

$$\sum_{i=0}^{M-1}(i^2P^i) = \frac{P^M(M^2P^2-2M^2P+M^2-2MP^2+2MP+P^2+P)}{(P-1)^3} - \frac{P(P+1)}{(P-1)^3}$$

We then specialize this result for the case when $M = n2^n$ and $P = e^{\frac{-m}{2^n}}$ as follows:

$$\sum_{i=0}^{n2^n-1} i^2(e^{-\frac{m}{2^n}})^i = \frac{n^2 2^{2n} e^{\frac{-m}{2^n}(n2^n)}}{(e^{-\frac{m}{2^n}}-1)} - \frac{2(n2^n)(e^{\frac{-m}{2^n}(n2^n+1)})}{(e^{-\frac{m}{2^n}}-1)^2} + \frac{(e^{\frac{-m}{2^n}(n2^n)}-1)(e^{\frac{-m}{2^n}})(e^{\frac{-m}{2^n}}+1)}{(e^{-\frac{m}{2^n}}-1)^3}$$

Using the above results along with some real analysis properties , we arrive at the following subgoal.

$$\lim_{n\to\infty}[-n^2e^{-mn}] + \lim_{n\to\infty}\left[-\frac{2ne^{-mn}e^{\frac{-m}{2^n}}}{2^n(1-e^{\frac{-m}{2^n}})}\right] + \lim_{n\to\infty}\left[-\frac{(e^{-mn}-1)(e^{\frac{-m}{2^n}})(e^{\frac{-m}{2^n}}+1)}{2^{2n}(1-e^{\frac{-m}{2^n}})^2}\right]$$
$$+\lim_{n\to\infty}[ne^{-mn}] = \frac{2}{m^2}$$

We then show that the first and fourth terms on the left hand side of the above subgoal approach zero as n tends to ∞, that is, $\lim_{n\to\infty}[-n^2e^{-mn}] = 0$ and $\lim_{n\to\infty}[ne^{-mn}] = 0$

The evaluation of the second and third limit terms required a lot of rewriting effort in HOL, and the proof steps are explained in the following. First we prove the following two limit expressions in HOL using L'hopital's rule.

$$\lim_{x\to0}\left[\frac{xe^{mx}}{1-e^{-mx}}\right] = \lim_{x\to0}\left[\frac{x(-me^{mx})+e^{mx}}{0-(-me^{-mx})}\right] = \frac{1}{m}, \text{ and}$$

$$\lim_{x\to0}\left[\frac{x}{1-e^{-mx}}\right] = \lim_{x\to0}\left[\frac{1}{0-(-me^{-mx})}\right] = \frac{1}{m}$$

Then we specialize the above two results for the case when $x = \frac{1}{2^n}$ and show that $\lim_{n\to\infty}\left[\frac{e^{\frac{-m}{2^n}}}{2^n(1-e^{\frac{-m}{2^n}})}\right] = \frac{1}{m}$ and $\lim_{n\to\infty}\left[\frac{1}{2^n(1-e^{\frac{-m}{2^n}})}\right] = \frac{1}{m}$

Then using the sum and product limit theorem we rewrite the second and third limit terms as follows:

$$\lim_{n\to\infty}\left[2ne^{-mn}\frac{e^{\frac{-m}{2^n}}}{2^n(1-e^{\frac{-m}{2^n}})}\right] = (2)\left(\lim_{n\to\infty}[ne^{-mn}]\right)\left(\lim_{n\to\infty}\left[\frac{e^{\frac{-m}{2^n}}}{2^n(1-e^{\frac{-m}{2^n}})}\right]\right)$$
$$= (2)(0)(\tfrac{1}{m}) = 0$$

$$\lim_{n\to\infty}\left[-\frac{(e^{-mn}-1)(e^{\frac{-m}{2^n}})(e^{\frac{-m}{2^n}}+1)}{2^{2n}(1-e^{\frac{-m}{2^n}})^2}\right] =$$
$$\lim_{n\to\infty}[-(e^{-mn}-1)]\lim_{n\to\infty}\left[\frac{e^{-mn}}{2^n(1-e^{\frac{-m}{2^n}})}\right]\left(\lim_{n\to\infty}\left[\frac{e^{-mn}}{2^n(1-e^{\frac{-m}{2^n}})}\right]+\lim_{n\to\infty}\left[\frac{1}{2^n(1-e^{\frac{-m}{2^n}})}\right]\right) =$$
$$(1)(\tfrac{1}{m})(\tfrac{1}{m}+\tfrac{1}{m}) = \tfrac{2}{m^2}$$

Finally, we substitute these limits in the above subgoal and show that the left hand side is equal to the right hand side, which completes the proof of the second moment of the Exponential random variable.

Theorem 3.13: *Variance of the Exponential(m) Random Variable*

$\vdash \forall\ m.\quad (0 < m) \Rightarrow \left(\texttt{variance}\ (\mathcal{U},\mathcal{E},\mathbb{P})\ \texttt{(exp\_rv m)} = \frac{1}{m^2}\right)$

The verification steps for the variance of the Exponential random variable involve some rewriting using the definition of the variance and the expectation and the second moment theorems. The resulting subgoal $(\frac{2}{m^2}) - (\frac{1}{m})^2 = \frac{1}{m^2}$ is easily shown to be true, based on arithmetic reasoning, thus completing the proof of the variance of the Exponential random variable.

The verification of the expectation, second moment, and variance properties did not involve any reasoning based on the Lebesgue integral. As a consequence, the verification process, which just took around 80 man hours with approximately 3500 lines of HOL code. It was very straightforward and quick in comparison to the verification of Theorems 3.1, 3.2, 3.3, and 3.4, which took around 350 man-hours and approximately 5000 lines. This clearly demonstrates the strength of our work, which is to provide the ability to build upon Theorems 3.1, 3.2, 3.3 and 3.4, and reduce the interactive reasoning efforts regarding the expectation properties of continuous

random variables. Also, our theorems are quite general and can be built upon to reason about expected values of many other random variables as well, such as the Rayleigh and Pareto.

3.5 Summary

In this chapter, we have presented an infrastructure to reason about statistical properties of continuous random variables using a higher-order-logic theorem prover. This capability allows us to conduct formal statistical analysis of systems with continuous random components, which is not supported by most of the existing probabilistic analysis tools at this time.

We built upon a formalized Lebesgue integration theory to define expectation and based on this definition we verified four alternate expectation and second moment relations. These relations do not involve any concepts from the mathematically complex Lebesgue integration theory and thus facilitate reasoning about statistical properties of continuous random variables significantly. We utilized these relations to verify the expected values and second moments of the Uniform, Triangular and Exponential random variables. To the best of our knowledge, this is the first time that the formal reasoning about the expectation, second moment and variance of these continuous random variables has been presented in a higher-order-logic theorem prover. These verified properties can now be utilized in the verification of statistical properties of lifetimes of individual components in a system and also in other engineering analysis problems such as the round of error analysis of floating point numbers.

Moreover, in many applications, what is measured or observed is not what we are interested in, but, we can learn about what we are interested in through what we can measure. For example, consider that we are interested in learning about random

variable X, but we can only measure or observe random variable Y, where random variable Y may be a function of random variable X. Our developed infrastructure supports reasoning about probabilistic and statistical properties of such functions of random variables.

In the next chapter, we present the formalization of multiple continuous random variables and the verification of their probabilistic properties.

Chapter 4

Probability Distribution Properties of Multiple Random Variables

Reliability analysis often requires use of positive valued random variables with different distributions such as Exponential and Weibull distributions. Sometimes random variables with the same distribution function but different distribution parameters are required. At other times multiple random variables with different distribution functions are required. In this chapter, we describes formalization of multiple random variables. We also define and verify the CDF properties of random variable lists in higher-order logic. Moreover, we formalize the notion of independence of multiple random variables.

4.1 Introduction

We use the existing infrastructure in HOL to formalize multiple random variables. Hurd [34] formalized a probability space based on a measure space defined using sets of boolean sequences. He defined the notion of discrete random variables as

probabilistic algorithms that utilize a finite number of bits for their computation from a random boolean sequence. In this formalization, in order to guarantee the property of independence, the bits used by one probabilistic algorithm are never re used. This is accomplished by passing the boolean sequence to the first probabilistic algorithm, then passing the remaining portion of random bits in the sequence to the second probabilistic algorithm, and so on, until the last probabilistic algorithm, so that all the probabilistic algorithms receive a disjoint segment of the random boolean sequence. He then showed that this approach of using disjoint segment of random boolean sequence guarantees independence.

Hasan's formalization of continuous random variables builds on Hurd's formalization of probabilistic algorithms with a standard discrete uniform probability distribution. In this formalization, a standard continuous random variable is defined as a standard discrete uniform random variable that utilizes a very large number of random bits from the sequence that in limit approach infinity. Then using inverse transform method, random variables with various distributions for which inverse cumulative distribution function exists in a closed form, are formalized. One limitation of this approach is that it cannot be used for modeling more than one continuous random variables as it exhausts all the bits when modeling a standard continuous random variable. At best, it is possible to model multiple discrete random variables and a maximum of a single continuous random variable as this method exhausts the complete sequence of random bits in the standard continuous random variable. Therefore, this technique of passing remaining portion of the boolean sequence from one discrete random variable to the other, that works very well for multiple discrete random variable case, cannot be used for the formalization of multiple continuous random variables.

We build on these foundations and extend them to solve this problem of infinite boolean sequence exhaustion, by splitting it in to a finite number of disjoint boolean sequences first. For example, one possible way is to split a given infinite random boolean sequence into several disjoint boolean sequences. One possible way to split a boolean sequence into two sequences is by picking the even and the odd elements from the original sequence and then constructing two infinite random boolean sequences from it. In general using this technique, a given random boolean sequence can be split into a finite number of disjoint infinite random boolean sequences. Then using Hasan's formalization of continuous random variables, we can model multiple continuous random variables. We use this approach in our formalization and ensure that each random variable receives a disjoint segment of the random boolean sequence. This guarantees independence of random variables. To achieve this goal, we first define several higher-order logic functions that take a random boolean sequence and returns a list of disjoint random boolean sequences by selectively picking certain bits from the original random boolean sequence. Then, when we define random variable lists, we pass these disjoint segments of random boolean sequences to each corresponding element of the list of random variables. This ensures that the resulting random variables will be independent.

In the rest of this chapter, we present the formalization of the CDF of a list of random variables and verify its properties. We also present the formalization of multiple continuous random variable lists with different distributions. Finally, we describe the formalization of the notion of independence of multiple random variables using the method based on splitting of the random boolean sequence.

4.2 Formal Specification of CDF of Lists of Random Variables

In order to formally specify the CDF of a list of random variables in higher-order logic, we first define two list functions. They are `rv_val` and `rv_lf`. The higher-order logic recursive definitions of the two functions `rv_lf` and `rv_val` are as follows:

Definition: 4.1 *Random Variable Logical Formula Function*

$\vdash \forall$`s.  rv_val [] s = [] ` $\wedge$

$\forall$ `h L s.  rv_val (h ::  L) s = h s ::  rv_val L s`

The function `rv_val` takes a list of random variables, `X`, and the random boolean sequence, `s`, and returns a list of real values. The function `rv_lf` takes two real lists as input and returns a boolean expression consisting of conjunction of several terms formed from the corresponding elements of the two input lists. Each inequality in this boolean expression is of the form `( (EL X i) s` $\leq$ `(EL x i) )`. The function `EL` takes a list and a natural number as input arguments (for example, `EL Y i`) and returns the corresponding element of the list as output (in this case it would return `i`th element of the list `Y`). Definition 4.2 describes the random variable value function `rv_lf`.

Definition: 4.2 *Random Variable Value Function*

$\vdash$ `(rv_lf [] [] = T)` $\wedge$

`(rv_lf (h1 ::  t1) (h2 ::  t2) = h1` $\leq$ `h2` $\wedge$ `rv_lf t1 t2)`

Now using Definitions 4.1 and 4.2, we formally specify the joint CDF of a list of random variables in Definition 4.3.

Definition: 4.3 *Joint CDF of a List of Random Variables*

$\vdash \forall$`X x.  mcrv_cdf X x =`

`prob bern {s | rv_lf (rv_val X s) x}`

where `X` is a list of random variables of type `(((num→bool)→real) list)`, and `x` is a list of real numbers of type `(real list)`. For example, if the list of random variables `X` and the list of real values `x` both have four elements given by `[ X0; X1; X2; X3 ]` and `[ x0; x1; x2; x3 ]`, respectively, then the joint CDF function of the list of random variables, X, is given by `mcrv_cdf X x = prob bern {s | rv_lf (rv_val X s) x }` . The right hand side of the equation can be expanded to `mcrv_cdf X x = prob bern {s | (X0 s ≤ x0) ∧ (X1 s ≤ x1) ∧ (X2 s ≤ x2) ∧ (X3 s ≤ x3) }` by using the definitions of the `rv_lf` and `rv_val`, which is the standard textbook definition of CDF of a vector of four random variables.

4.3 Formal Verification of CDF of Lists of CRVs

Using the formal specification of the CDF function for a list of random variables, we have formally verified the classical properties of the CDF of a list of random variables. These properties are verified under the assumption that the set `{s | R s x}`, where `R` represents a list of random variables under consideration, is measurable for all values of the list. The formal proofs for these properties confirm our formalized specifications of the CDF of a list of random variables.

In order to formalize and prove properties of the CDF of lists of random variables, we first define a few new list operations. These operations include picking an arbitrary element from the list, dropping an arbitrary element from the list, replacing an arbitrary element from the list and filling the list with arbitrary elements. These operations are defined using the basic list operators such as TAKE, DROP, HD, TL,

APPEND, and concatenate (::) operators. The details and use of these new operations will be given in the descriptions of the proof of the properties of CDF of lists of random variables. These list operations are defined in Table 5.8

List Operation	HOL definition
ITH_EL	⊢ ∀x i a. ITH_EL x i a = TAKE (i - 1) x ++ [a] ++ DROP i x
FILL_LIST	⊢ ∀n. FILL_LIST [] [] ∧ ∀h t n. FILL_LIST (h::t) n = [& n] ++ FILL_LIST t n
ITH_EL_DROP	⊢ ∀X i. ITH_EL_DROP X i = TAKE (i - 1) X ++ DROP i X

Table 4.1: New list operations

The list function ITH_EL takes three arguments. The first argument is a list of real numbers. The second argument is a natural number i. The third argument is a real value a. The function ITH_EL replaces the ith element of list x with the real number a.

The function FILL_LIST fills the real list x with real values "&n", and finally, the function ITH_EL_DROP takes a real list, drops its ith element and returns remaining list. Here n is a natural number and & is a function of type (num→real). In addition to the above new operations defined on the lists, we have verified a rich set theorems involving functions rv_val, rv_lf, ITH_EL_LIST, FILL_LIST, and ITH_EL_DROP. The proofs of these theorems was not trivial and involved the principle of induction on lists, and basic list theorems related to splitting and appending lists. These general list theorems also significantly facilitated the proofs of the properties of cumulative distribution function of multiple random variable described in the rest of this section.

Theorem 4.1 through 4.5 describe the properties of CDF of a list of random variables. Each CDF property of the list of random variables is mathematically described first, followed by its HOL formalization. Following each of the property we provide a detailed proof sketch of each of the property.

CDF Bounds

This property states that for a list of random variables `X`, and a list of real numbers `x`, the CDF function is bounded between `0` and `1`. The property is mathematically described as:

$$0 \leq F_{X_1,\ldots,X_n}(x_1,\ldots,x_n) \leq 1$$

Theorem: 4.1 *CDF Bounded*

```
⊢ ∀X x. (∀ Y y.  {s | rv_lf (rv_val Y s) y} IN events bern) ⇒
                                ( (0 ≤ mcrv_cdf X x) ∧ (mcrv_cdf X x ≤ 1) )
```

where `(X :((num → bool) → real) list)` and `(Y :((num → bool) → real) list)` in Theorem 4.1 represent lists of random variables. `(x :real list)` and `(y :real list)` are two lists of real numbers and `(s :num → bool)` represents an infinite boolean sequence. The proof of this property follows from the definition of joint CDF function of list of multiple random variables and the fact that joint CDF function represents the probability measure.

Multiple Random Variable CDF is Monotonic and Non-decreasing

The joint CDF function of a list of multiple random variable is a monotonically non-decreasing function in each variable. For any two real numbers (`a` $<$ `b`), this property is mathematically expressed as:

$$F_{X_1,\ldots,X_i,\ldots,X_n}(x_1,\ldots,a,\ldots,x_n) \leq F_{X_1,\ldots,X_i,\ldots,X_n}(x_1,\ldots,b,\ldots,x_n)$$

This fact is formally stated and verified in Theorem 4.2. In this theorem, `X` is a list of random variables. `x` and `y` are lists of real numbers. The assumptions formally state that all lists `X`, `x` and `y` have same length. All elements of real lists `x` and `y` are equal except for the `i`th element. The `i`th element of the list `y` is greater than the `i`th element of list `x`. All events of the form {`s | rv_lf (rv_val Y s) y`} are measurable events in the probability space. Under these conditions the joint

cumulative distribution function of the list of random variables `X` is monotonic and non-decreasing. The above result is true for all values of `i`.

Theorem: 4.2 *Multiple Continuous Random Variable CDF is Monotonic and Non-decreasing*

```
⊢ ∀X x y i.  (i ≤ LENGTH x) ∧ (LENGTH X = LENGTH x) ∧
  (LENGTH x = LENGTH y) ∧ (EL i x < EL i y) ∧
  (∀j.  1 ≤ j ∧ j ≤ LENGTH X ∧ (¬(i = j) ⇒ (EL j x = EL j y))) ∧
  (∀Y y.  {s | rv_lf (rv_val Y s) y} IN events bern) ⇒
                                        mcrv_cdf X x ≤ mcrv_cdf X y
```

We start the proof by rewriting the conclusion of the goal with the definition of multiple random variable CDF (`mcrv_cdf`). Then using the Monotone property of probabilities, that is for all measurable events `A` and `B` in the probability space, `(A ⊆ B) ⇒ P(A)≤P(B)`, along with modus ponens rule of inference, we reduce the proof goal to the following subgoal.

```
prob_space bern ∧
{s | rv_lf (rv_val X s) x} IN events bern ∧
{s | rv_lf (rv_val X s) y} IN events bern ∧
{s | rv_lf (rv_val X s) x} ⊆ {s | rv_lf (rv_val X s) y}
```

This subgoal of the proof consists of a conjunction of four terms. The first assumption states that `bern` is a measure space such that measure of universe in this measure space is `1`, that is, `bern` is a probability space. The second and the third subgoals state that the events `{s | rv_lf (rv_val X s) x}` and `{s | rv_lf (rv_val X s) y}` are measurable events in the probability space `bern`. These three subgoals are proved to be true by using reasoning from the probability theory and the assumptions of Theorem 4.2. The fourth and the final subgoal is first rewritten

in predicate notation as given below.

```
rv_lf (rv_val X s) x ⇒ rv_lf (rv_val X s) y
```

Both the antecedent and the consequent of this goal consist of conjunction of logical terms. All the corresponding logical terms in the antecedent and consequent are the same except for the `i`th term. In order to prove this subgoal, first we divide both the antecedent and consequent of the subgoal into conjunction of three terms each by splitting the lists `rv_val X s`, `x` and `y`. The three logical terms consist of 1) the terms up to and not including the `i`th term, 2) the `i`th term and 3) the remaining terms starting from the `(i+1)`th term all the way to the end of the list. Then using case analysis and reasoning from propositional logic on the first and third logical terms, we reduce the subgoal to the following:

```
( ((EL i X) s) ≤ (EL i x) ) ⇒ ( ((EL i X) s) ≤ (EL i y) )
```

Now the proof is completed using the fourth and the fifth assumptions of the theorem, that is, `((∀j. (1 ≤ j) ∧ (j ≤ LENGTH X) ∧ (¬(i = j) ⇒ (EL j x = EL j y)))` and `(EL i x < EL i y)`) and the less than equal to transitivity property of real numbers (`∀x y z. (x ≤ y) ∧ (y ≤ z) ⇒ (x ≤ z)`).

Marginal CDF property of List of Random Variables

Joint distribution function can be used to uniquely determine the marginal distribution of the individual random variables. This property is mathematically stated as:

$$\lim_{x_i \to \infty} F_{X_1,\ldots,X_{i-1},X_i,X_{i+1},\ldots,X_n}(x_1,\ldots,x_{i-1},x_i,x_{i+1},\ldots,x_n) = F_{X_1,\ldots,X_{i-1},X_{i+1},\ldots,X_n}(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)$$

In Theorem 4.3, we have proved the standard Marginal CDF property for a list of random variables. This property states that the distribution of individual random variable $\mathtt{X}_i$ can be obtained from the knowledge of their joint distribution function.

Theorem: 4.3 *Marginal CDF Property of List of Random Variables*

$\vdash \forall$i. (1 $\leq$ i) $\wedge$ (i $\leq$ LENGTH x) $\wedge$ (LENGTH X = LENGTH x) $\wedge$

($\forall$n. { s | rv_lf (rv_val X s) (ITH_EL x i (&n))} IN events bern) $\Rightarrow$

(lim (λn. mcrv_cdf X (ITH_EL x i n)) =

mcrv_cdf (ITH_EL_DROP X i) (ITH_EL_DROP x i))

We begin the proof process by rewriting with the definitions of the CDF of multiple random variables, mcrv_cdf, and reduce the proof goal to:

prob bern o (λn. {s | rv_lf (rv_val X s) (ITH_EL x i n)}) $\rightarrow$

prob bern {s | rv_lf (rv_val (ITH_EL_DROP X i) s) (ITH_EL_DROP x i)}

where the operator $\rightarrow$ is the limit of a sequence operator and the operator o is the function composition operator. We then utilize the continuity property of probabilities of expanding sequences of sets to simplify the above subgoal. This property states that for an increasing sequence of measurable events A_n in the probability space, such that, $\forall$n. $A_n \subseteq A_{n+1}$ in the sample space S implies $\lim_{n\to\infty} A_n$ = $\bigcup_{n=1}^{\infty} A_n$ = S.

This increasing sequence of events in this case are expressed in lambda calculus as: (λn. {s | rv_lf (rv_val X s) (ITH_EL x i n)}). Here n is a natural number. Using the property of expanding sequence of sets and the property of continuity of probability, we reduce the proof goal to the following four subgoals:

prob_space bern $\wedge$

(λn. {s | rv_lf (rv_val X s) (ITH_EL x i n)}) $\in$ (UNIV->events bern) $\wedge$

($\forall$n. (λn. {s | rv_lf (rv_val X s) (ITH_EL x i n)}) n $\subseteq$

(λn. {s | rv_lf (rv_val X s) (ITH_EL x i n)}) (SUC n)) $\wedge$

({s | rv_lf (rv_val (ITH_EL_DROP X i) s) (ITH_EL_DROP x i)} =

BIGUNION (IMAGE (λn. {s | rv_lf (rv_val X s) (ITH_EL x i n)}) UNIV))

The first subgoal states that bern is a probability space. The second subgoal

ensures that the events {s | rv_lf (rv_val X s) (ITH_EL x i n)} are measurable events in the probability space. The first two subgoals are discharged using the fact that bern is a probability space and from the fact that all events of type { s | rv_lf (rv_val X s) (ITH_EL x i (&n))} are measurable as stated in the fourth assumption of Theorem 4.3.

The third subgoal states that the sequence of events (λn.{s | rv_lf (rv_val X s) (ITH_EL x i n)}) are an expanding sequence of sets or

(∀n. (λn. {s | rv_lf (rv_val X s) (ITH_EL x i n)}) n ⊆
(λn. {s | rv_lf (rv_val X s) (ITH_EL x i n)}) (SUC n)).

We prove this subgoal by first rewriting with the definition of subset and reasoning from list theory to split the antecedent and the conclusion into three logical terms each. We then perform case analysis on the equal logical terms to reduce the proof goal to:

(EL i (X s) ≤ &n) ⇒ (EL i (X s) ≤ &(SUC n))

This is shown to be true using the less than and equal to transitivity property of the real numbers.

Finally, the fourth subgoal is first rewritten with the definitions of IMAGE and BIGNUION. The higher-order logic definitions of IMAGE and BIGUNION are ∀f s. IMAGE f s = {f x | x ∈ s} and ∀P. BIGUNION P = {x | ∃s. s ∈ P ∧ x ∈ s} , respectively. The resulting subgoal expressed in predicate calculus is as:

rv_lf (rv_val (ITH_EL_DROP X i) s) (ITH_EL_DROP x i) =
∃n. rv_lf (rv_val X s) (ITH_EL x i n)

This subgoal states that the logical expression on the left hand side of the equation is equal to the logical expression on the right hand side for at least one value of natural number n. There is a corresponding equal logic expression on both left and right hand

sides of this the above subgoal. As before, we split the logical expression into three subexpressions using Boolean and List theories in HOL. Then, we remove the equal logical expressions from either side of the equation using cases analysis, discharging the false case and simplifying the true case, which leads to the following subgoal.

$\exists$n. (EL i X) s $\leq$ &n

We then pick an n = $\lceil$((EL i X) s)$\rceil$ + 1 and show that the subgoal is true using the less than and equal transitivity property of real numbers and this step finally concludes the proof of Theorem 4.3.

Multiple Random Variable CDF at Positive Infinity

This property can be mathematically stated as:

$$\lim_{x_1 \to \infty}, \ldots, \lim_{x_n \to \infty} F_{X_1,\ldots,X_n}(x_1, \ldots, x_n) = F_{X_1,\ldots,X_n}(\infty, \ldots, \infty) = 1$$

This property formally states that when real numbers x_1, x_2, ..., x_n increase and tend to ∞, then the joint CDF function of the random variables approaches unity.

Theorem: 4.4 *Multiple Random Variable CDF at Positive Infinity*

$\vdash \forall$i. (1 $\leq$ i) $\wedge$ (i $\leq$ LENGTH x) $\wedge$ (LENGTH X = LENGTH x) $\wedge$
($\forall$n. { s | rv_lf (rv_val X s) (FILL_LIST x n)} IN events bern) $\Rightarrow$
(lim (λn. prob bern {s | rv_lf (rv_val X s) (FILL_LIST x n)})= 1)

We begin the proof of this theorem by rewriting with the definition of mcrv_cdf and the limit of a sequence lim and arrives at the following subgoal:

prob bern o (λn. {s | rv_lf (rv_val X s) (FILL_LIST x n)}) $\rightarrow$ 1

The proof of this subgoal utilizes the fact that for an expanding sequence of events A_n, that is, ($\forall$n. $A_n \subseteq A_{n+1}$) of S, $\lim_{n\to\infty} A_n$ = $\bigcup_{n=1}^{\infty} A_n$ = S. Now using the fact that the sequence of events (λn. {s | rv_lf (rv_val X s) (FILL_LIST x n)}) approach the sample space (UNIV) as n becomes very large, we reduce the proof goal to the following four subgoals:

```
 prob_space bern ∧
(λn.  {s | rv_lf (rv_val X s) (FILL_LIST x n)}) ∈ (UNIV->events bern) ∧
(∀n.  (λn.  {s | rv_lf (rv_val X s) (FILL_LIST x n)}) n ⊆
(λn.  {s | rv_lf (rv_val X s) (FILL_LIST x n)}) (SUC n)) ∧
(UNIV =
BIGUNION (IMAGE (λn.  {s | rv_lf (rv_val X s) (FILL_LIST x n)}) UNIV))
```

The first two subgoals are shown to be true using reasoning from probability theory and the fourth assumption of Theorem 4.4.

```
 {s | rv_lf (rv_val X s) (FILL_LIST x n)} ⊆
{s | rv_lf (rv_val X s) (FILL_LIST x (SUC n))}
```

The third subgoal is proved by rewriting with the definition of subset and less than equal to transitivity property of real numbers.

Finally, the fourth subgoal is first rewritten with the definitions of `IMAGE` and `BIGNUION`. The resulting subgoal expressed in predicate calculus is given below.

```
 ∃n.  rv_lf (rv_val X s) (FILL_LIST x n)
```

The subgoal states that there exists an `n` such that `&n` is less than or equal to every element of list `(X s)`. This subgoal is proven to be true by selecting an `n`, such that `n` is equal to the ceiling of the maximum of the elements of the list `X s`. This completes the proof of Theorem 4.4.

Multiple Random Variable CDF at Negative Infinity

This property of the distribution function states that for any `i`,

$$\lim_{x_i \to -\infty} F_{X_1,\ldots,X_i,\ldots,X_n}(x_1,\ldots,x_i,\ldots,x_n) =$$
$$F_{X_1,\ldots,X_i,\ldots,X_n}(x_1,\ldots,-\infty,\ldots,x_n) = 0$$

This property formally states that the CDF function approaches zero as the real numbers x_1, x_2, ..., x_n approach $-\infty$.

Theorem: 4.5 *Multiple Random Variable CDF at Negative Infinity*

```
⊢ ∀i.  (1 ≤ i) ∧ (i ≤ LENGTH x) ∧ (LENGTH X = LENGTH x) ∧
(∀n.{ s | rv_lf (rv_val X s) (ITH_EL x i (-&n))} IN events bern) ∧ ⇒
 (lim (λn.  prob bern {s | rv_lf (rv_val X s) (ITH_EL x i (-&n))})= 0)
```

We begin the proof of this theorem by rewriting with the definition of CDF of multiple random variables (`mcrv_cdf`) and the limit of a sequence (`lim`) arriving at the following subgoal:

```
prob bern o (λn.  {s | rv_lf (rv_val X s) (ITH_EL x i (-&n))}) → 0
```

For the proof of this subgoal we utilize the continuity property of probabilities of contracting sequences of sets. The property states that, for all events $\mathtt{A}_n$ in the probability space, $\lim_{n\to\infty} P(A_n)$ = $P(\bigcap_n^\infty A_n)$. This helps us in reducing the above subgoal to the following three subgoals:

```
 (λn.  {s | rv_lf (rv_val X s) (ITH_EL x i (-(&n)))})
∈ (UNIV->events bern) ∧
(∀n.  (λn.  {s | rv_lf (rv_val X s) (ITH_EL x i (-&n))}) (SUC n) ⊆
(λn.  {s | rv_lf (rv_val X s) (ITH_EL x i (-&n))}) n) ∧
{} =
BIGINTER (IMAGE (λn.  {s | rv_lf (rv_val X s) (ITH_EL x i (-&n))}) UNIV)
```

The first subgoal is discharged using the fourth assumption of Theorem 4.5. We simplify the second subgoal with the definition of subset and then using reasoning from list theory followed by case analysis, we reduce the subgoal to the form, `(EL i (X s) ≤ -(SUC n)) ⇒ (EL i (X s) ≤ -n)`, which is shown to be true using the less than and equal to transitivity property of real numbers.

Finally, the fourth subgoal is first rewritten with the definitions of `IMAGE` and

BIGINTER, ∀f s. IMAGE f s = {f x | x ∈ s} and ∀P. BIGINTER P = {x | ∀s. s ∈ P ⇒ x ∈ s} , respectively. The resulting subgoal expressed in predicate calculus is given below.

∃n. ¬ rv_lf (rv_val X s) (ITH_EL x i (-(&n)))

The subgoal states that there exists an n, such that the logical expression is false. We proceed by splitting the logical expression into three logical terms. Then, we show that there exists an n such that the logical negation of the ith term ∃n. ¬((EL i (X s)) ≤ -&n) is true by picking n = (⌈(X s)⌉ + 1 and then using the less than equal transitivity property of real numbers and the definition of ceiling of a real number to finish the proof of this subgoal. This also completes the proof of Theorem 4.5.

In this section standard properties of cumulative distribution function were verified. These properties will be used later in defining basic notions of reliability of a system. Each random variable in the list of random variables can be used to model the reliability behavior of a component of the system. In the next section, the formalization of the notion of independence of multiple continuous random variables is described.

4.4 Independent Random Variables

In many engineering applications independent random behaviour needs to be modeled. The notion of independence for a list of random variables X = [X_0; X_1; X_2; ... ; $X_{(N-1)}$] is defined as:

P($X_0 \leq x_0 \wedge X_1 \leq x_1 \wedge \ldots \wedge X_{N-1} \leq x_{N-1}$) = $\Pi_{i=0}^{i=N-1}$ P($X_i \leq x_i$)

where x = [x_0; x_1; x_2; ... ; $x_{(N-1)}$] is a list of real numbers. The subscript in the above equation represents the index of the random variable in the list. N represents

the length of the list of random variables `X`.

In order to formalize a list of independent continuous random variables, we first define the notion of a list of disjoint random boolean sequences using higher-order logic functions `s_arb` and `s_split` in Definitions 4.4 and 4.5 respectively.

Definition: 4.4 *Boolean Sequence Split Function*

```
⊢(∀s M i.  s_arb s M i 0 = s i) ∧
  ∀s n M i.  s_arb s M i (SUC n) = s (M * SUC n + i)
```

The function `s_arb` takes three arguments. The first argument is a boolean sequence `s`. The second and third arguments are natural numbers `M` and `i`. The function `s_arb` can split the input boolean sequence `s` into `M` disjoint boolean sequences. The third argument `i` is used to pick every `i`th element from the input infinite boolean sequence and the function `s_arb` returns that boolean sequence as output. This way we can provide each random variable in the list of random variables with a different infinite random boolean sequence. This fact also guarantees independence of random variables in the list [65].

Definition: 4.5 *List of Disjoint Boolean Sequences*

```
⊢ ∀M s.  s_split 0 M s = [(λx.  s_arb s x M) 0]) ∧
  ∀N M s.  s_split (SUC N) M s =
                          (λx.  s_arb s x M) (SUC N) ::  s_split N M s
```

The function `s_split` takes a boolean sequence as input and returns a list consisting of `M+1` disjoint boolean sequences. For example, `s_split 2 2 s` would return a list of three disjoint boolean sequences given by `[s_arb s 2 2; s_arb s 1 2; s_arb s 0 2]`.

In order to define the notion of independence of a list of random variables, we first define a list function that we call `rv_val_indep`. This function merges two lists element by element and generates a list. The first list argument of this function is a list of random variables of type `((num->bool)->real) list` and the second list argument is a list consisting of random boolean sequences of type `((num->bool) list)`. The function merges the two lists element by element and returns a list of real independent random variables.

Definition: 4.6 *List function rv_val_indep*

```
⊢ (rv_val_indep [] [] = []) ∧
  (rv_val_indep (h1::t1) (h2::t2) = h1 h2::rv_val_indep t1 t2)
```

As an example, consider a list of three random variables `[X0; X1; X2]` and random boolean sequence `s`. The expression `rv_lf (rv_val_indep [X0; X1; X2] (s_split (PRE (LENGTH [X1; X2; X3])) (LENGTH [X1; X2; X3]) s)) [x1; x2; x3]` returns the following expression upon simplification. `(X0 (s_arb s 2 3) ≤ x1) ∧ (X1 (s_arb s 1 3) ≤ x2) ∧ (X2 (s_arb s 0 3) ≤ x3)` The function `s_split` splits the boolean sequence `s` into three disjoint sequences and returns them as a list of three element. Then each corresponding random variable is passed a corresponding disjoint segment of the input boolean sequence `s` using the function `rv_val_indep`. This guarantees the independence of random variables [65].

Finally, the HOL formalization of the notion of independence is given in Definition 4.7.

Definition: 4.7 *Independent Random Variable List*

```
⊢ ∀X x.  indep_rv_list X x =
  (prob bern {s | rv_lf
  (rv_val_indep X (s_split (PRE (LENGTH X)) (LENGTH X) s)) x} =
   prod1 (0,LENGTH X) (λi.  prob bern {s |
    EL i (rv_val_indep X
    (s_split (PRE (LENGTH X)) (LENGTH X) s)) ≤ EL i x})) ∧
  {s | rv_lf (rv_val_indep X
   (s_split (PRE (LENGTH X)) (LENGTH X) s)) x} IN events bern ∧
  ∀i.  {s | EL i (rv_val_indep X
   (s_split (PRE (LENGTH X)) (LENGTH X) s)) ≤ EL i x} IN events bern
```

where `X` and `x` are of types `(((num -> bool) -> real) list)` and `(real list)` respectively. `prod1` is a product of a sequence function and represents the big pi operator (Π). The function `s_split` splits the random boolean sequence `s` and returns a list of disjoint random boolean sequences. `PRE` is a function of type `(num->num)` and is defined as: `∀m.  PRE m = (if m = 0 then 0 else @n.  m = SUC n)`, where `@` is the hilbert's choice operator. The list function `EL` takes two arguments, a natural number and a list. The function returns the `i`th element of the list. The second and the third logical terms in Definition 4.7 state that the respective events are measurable in the probability space. Definitions 4.8 through to 4.12 show our formalization of lists of random variables with various distributions.

Definition: 4.8 *List of Weibull random variables*

```
⊢  (WB_RV_LIST [] [] = []) ∧
   (WB_RV_LIST (ah::at) (bh::bt)
   = [(λa b s.  weibull_rv a b s) ah bh] ++ WB_RV_LIST at bt)
```

Definition: 4.9 *List of Exponential random variables*

```
⊢ (EXP_RV_LIST [] = []) ∧
   ∀ah at.  EXP_RV_LIST (ah::at)
            = [(λa s.  exp_rv a s) ah] ++ EXP_RV_LIST at
```

Definition: 4.10 *List of Rayleigh random variables*

```
⊢ (RAYLEIGH_RV_LIST [] = []) ∧
   ∀ah at.  RAYLEIGH_RV_LIST (ah::at)
            = [(λa s.  rayleigh_rv a s) ah] ++ RAYLEIGH_RV_LIST at
```

Definition: 4.11 *List of Uniform random variables*

```
⊢ (UNIFORM_RV_LIST [] [] = []) ∧
   (UNIFORM_RV_LIST (ah::at) (bh::bt)
    = [(λa s.  uniform_rv a b s) ah bh] ++ UNIFORM_RV_LIST at bt)
```

Definition: 4.12 *List of Triangle random variables*

```
⊢ (TRIANGLE_RV_LIST [] = []) ∧
   ∀ah at.  TRIANGLE_RV_LIST (ah::at)
            = [(λa s.  triangular_rv a s) ah] ++ TRIANGLE_RV_LIST at
```

Note that we build on Hasan's [29] formalization of continuous random variables. This formalization was briefly described in Chapter 2 of this thesis. In these formalizations, the list of a random variables is constructed recursively using a random variable with a given distribution. If random variables with different distributions are required in a single list, then the two random variable lists shall be constructed separately. Then these two lists will be appended to construct the desired list of random variables. Then using function such as `rv_val_indep` and `s_split`, it can be guaranteed that each of the random variable in the list will receive a disjoint segment of

the boolean sequence. This guarantees the independence of random variables in the constructed list of random variables.

We demonstrate this with the help of a simple example in the following. In this example, we construct list of 6 random variables. The first and the last two random variables are of type Exponential, and the second, the third and the fourth random variables are of type Weibull. For this purpose, first we construct three lists. The first list consists of one Exponential random variable, the second list consists of three Weibull random variables and the last list consists of two Exponential random variables. The following shows a specification of the list.

```
 rv_val_indep
((EXP_RV_LIST [a0]) ++ (WB_RV_LIST [a1; a2; a3] [b1; b2; b3]) ++
(EXP_RV_LIST [a4; a5]))
(s_split
(PRE (LENGTH ((EXP_RV_LIST [a0]) ++
(WB_RV_LIST [a1; a2; a3] [b1; b2; b3]) ++ (EXP_RV_LIST [a4; a5]))))
(LENGTH ((EXP_RV_LIST [a0]) ++
(WB_RV_LIST [a1; a2; a3] [b1; b2; b3]) ++ (EXP_RV_LIST [a4; a5]))) s)
```

which upon rewriting with the definitions of `rv_val_indep`, `EXP_RV_LIST`, `WB_RV_LIST`, `s_split`, and `PRE` and `LENGTH` gives a list of 6 independent random variables with the desired distributions.

```
 [exp_rv a0 (s_arb s 5 6); weibull_rv a1 b1 (s_arb s 4 6);
weibull_rv a2 b2 (s_arb s 3 6); weibull_rv a3 b3 (s_arb s 2 6);
exp_rv a4 (s_arb s 1 6); exp_rv a5 (s_arb s 0 6)]
```

In the following, in Theorem 4.6 and 4.7, we verify the CDF properties of independent Exponential and Weibull random variables, respectively.

Theorem: 4.6 *CDF of a list of Independent Exponential random variables*

```
⊢ ∀ a.  (∀i.  1 ≤ i ∧ i ≤ LENGTH a ⇒ 0 < EL i a) ∧
  ¬(LENGTH a = 0) ∧ (LENGTH a = LENGTH (EXP_RV_LIST a)) ∧
  (LENGTH a = LENGTH x) ∧ indep_rv_list (EXP_RV_LIST a) x ⇒
  (prob bern {s | rv_lf
   (rv_val_indep (EXP_RV_LIST a)
   (s_split (PRE (LENGTH a)) (LENGTH a) s)) x} =
   prod1 (0,LENGTH a) (λi.  1 - exp (-EL i a * EL i x)))
```

The first assumption in Theorem 4.6 states that the parameters of the Exponential random variable list are all greater than zero. The second, third and the fourth assumptions state that the list of Exponential random variables and their parameter list are non empty and of equal size. The fifth and the final assumption states that the exponential random variables in the list `EXP_RV_LIST` are independent.

The proof of the Theorem 4.7 also involved the principle of list induction and some other relevant lemmas involving the recursive list function `rv_val_indep`.

Theorem: 4.7 *CDF of a list of Independent Weibull random variables*

```
⊢ ∀ a b.  (∀i.  1 ≤ i ∧ i ≤ LENGTH a ⇒ 0 < EL i a) ∧
  ¬(LENGTH a = 0) ∧ (LENGTH a = LENGTH b) ∧
  (LENGTH a = LENGTH (EXP_RV_LIST a)) ∧ (LENGTH a = LENGTH x) ∧
  indep_rv_list (WB_RV_LIST a b) x ⇒
  (prob bern {s | rv_lf (rv_val_indep (WB_RV_LIST a b)
   (s_split (PRE (LENGTH a)) (LENGTH a) s)) x} =
  prod1 (0,LENGTH a) (λi.  1 - exp -((EL i a * EL i x) powr EL i b)))
```

The proof of Theorem 4.7 also involved the principle of list induction and is similar to the proof of Theorem 4.6. These useful theorems will be helpful in the

formal reliability analysis of multi-component systems whose lifetime behaviour modeling requires that independent random variables be used as in real life the system components can fail independent of each other.

Vectors of random variables with same or different distributions and parameter values are often needed in reliability analysis. Our formalization of multiple random variables allows the flexibility of having independent random variables with same or different distribution functions. In the case when random variables have same distribution type, it is possible to have same or different parameters.

The formalization results presented in this section are completely general. Traditionally, in simulation based schemes, independence of random variables requires that independent random number generators be used. Our proposed approach provides a formal alternative to this traditional approach and at the same time guarantees independence.

4.5 Summary

In this chapter, we described the formalization of multiple continuous random variables. We also formalized important concept of cumulative distribution function and verified its important properties. Moreover, we defined the notion of independence of random variables. The formalization presented in this chapter consists of over 4900 lines of HOL code and took over 310 man-hours to complete.

The formalization described in this chapter can be used to formalize a gaussian random variable pair using two independent and identically distributed standard continuous random variables and the box-muller method. Such formalization would allow reasoning about problems involving the use of gaussian random variable.

In the next chapter, we introduce the basic reliability theory concepts. They

include some of the commonly used quantitative measures of reliability and provides means for modeling and analysis of multiple component systems.

Chapter 5

Reliability Theory Formalization

In this chapter, basic concepts of reliability theory are described and their higher-order logic formalization is presented. Important properties of these reliability concepts are formally verified using the HOL theorem prover. The relationships for system reliability for various possible system configurations are also verified.

5.1 Introduction

Different lifetime distribution representations have been used in the past depending upon the specific needs of a lifetime reliability analysis problem. For example, sometimes the probability of failure is of interest at a certain time (Survival function), whereas, in other application, such as in planning for serviceability and maintainability of a system, the total amount of risk associated with a system up to a given time (Cumulative Hazard function) may be required [37]. Two other commonly used important reliability properties are the Hazard function and the Fractile function. The hazard function expresses the failure risk at a given time and the Fractile function allows resoning about the times of failure corresponding to a given probability of

failure [43]. The survival function $S_T(t)$ is defined as:

$$S_T(t) = 1 - F_T(t) \tag{5.1}$$

where $F_T(t)$ is the cumulative distribution function of the random variable T. The hazard function, $h_T(t)$, is defined as:

$$h_T(t) = -\frac{\frac{dS_T(t)}{dt}}{S_T(t)} = \lim_{h \to 0} \frac{S_T(t) - S_T(t+h)}{hS_T(t)} \tag{5.2}$$

and the cumulative hazard function, $H_T(t)$, is defined as:

$$H_T(t) = \int_0^t h_T(\tau) d\tau \tag{5.3}$$

and finally the p-th fractile $t_T(p)$ of a random variable T is defined as:

$$t_T(p) = F_T^{-1}(p) \tag{5.4}$$

The contributions of this chapter lie in the formalization of these reliability concepts and proof of their important properties using higher-order logic. This chapter also formalizes concepts related to the various commonly used system configurations that would facilitate formal reliability analysis of systems in a theorem proving environment.

5.2 Formalization of Reliability Concepts

In this section, we present the formalization of the concepts of survival function, hazard function, cumulative hazard function and the fractile function of various lifetime distributions.

5.2.1 Survival Function

The survival function represents the probability that a component is functioning at one particular time t and is formalized in HOL as follows:

Definition 5.1: *Survival Function*

$\vdash$ $\forall$rv. survival_function rv = (λt. 1 - CDF rv t)

where CDF is the cumulative distribution function of random variable rv. Both survival function and CDF in HOL are of type (((num $\rightarrow$ bool) $\rightarrow$ real) $\rightarrow$ real $\rightarrow$ real).

Using the above formalization of the survival function, we formally verified three important existence properties of the survival function in HOL. They are:

1) Survival function at time 0 is equal to 1

Theorem 5.1: *Survival function at time 0 is equal to 1*

$\vdash$ $\forall$rv. ($\forall$x. CDF_in_events_bern rv x) $\Rightarrow$

(survival_function rv 0 = 1)

where the assumption of Theorem 5.1 ensures that events of the type $\{s|rv\ s \leq x\}$, which define the CDF, are measurable.

The proof involved rewriting with the definition of the survival function and properties of the cumulative distribution function of the random variable rv.

2) Survival function approaches 0 for very large values of times

Theorem 5.2: *Survival function approaches 0 for very large values of times*

$\vdash$ $\forall$rv. ($\forall$x. CDF_in_events_bern rv x) $\Rightarrow$

lim (λn. survival_function rv &n) = 0

The proof of Theorem 5.2 involved rewriting with the definition of survival function, real analysis and CDF properties of the random variable rv.

3) Survival function is a non increasing function

Theorem 5.3: *Survival function is a non increasing function*

$\vdash$ $\forall$rv a b. (a<b) $\wedge$ ($\forall$x. CDF_in_events_bern rv x) $\Rightarrow$

(survival_function rv b $\leq$ survival_function rv a)

The proof of Theorem 5.3 also involved rewriting with the definition of the survival function and the properties of the CDF of a random variable.

Besides the above mentioned three properties, we verified survival function relations for random variables that are commonly used in reliability analysis.

Theorem 5.4: *Survival Function, Exponential(m) Random Variable*

$\vdash \forall$ `m t.` $(0 < m) \wedge (0 \leq t) \Rightarrow$

`(survival_function (`λ`s.` `exp_rv m s) t =` e^{-mt})

Theorem 5.4 was verified using the definitions of survival function and CDF of the Exponential random variable together with set theory properties. If T represents the Time-to-Failure of an electronic system component, for example, then using Theorem 5.4, we can now formally reason about probabilities of failure events at any time t i.e., $\mathtt{P}\{T \leq t\}$, or between any two times t_1 and t_2, i.e., $\mathtt{P}\{t_1 \leq T \leq t_2\}$.

Distribution	**Survivor Function,** $S(t)$
Uniform	$\vdash \forall$ a b t. $(0 \leq a) \wedge (a < b) \wedge (0 \leq t) \Rightarrow$ survival_function (λs. uniform_rv a b s) t = $\left(\frac{b-t}{b-a}\right)$
Triangular	$\vdash \forall$ b t. $(0 < b) \wedge (0 \leq t) \Rightarrow$ survival_function (λs. triangle_rv b s) t = $1 - \frac{2}{b}(t - \frac{t^2}{2b})$
Exponential	$\vdash \forall$ m t. $(0 < m) \wedge (0 \leq t) \Rightarrow$ survival_function (λs. exp_rv m s) t = e^{-mt}
Weibull	$\vdash \forall$ a m t. $(0 < a) \wedge (0 < m) \wedge (0 \leq t) \Rightarrow$ survival_function (λs. weibull_rv a m s) t = $e^{-(mt)^a}$

Table 5.1: Formally verified survival function relations for commonly used life time distributions

Table 5.1 presents the formally verified survival function relations for commonly used life time distributions.

5.2.2 Hazard Function

The hazard function or instantaneous failure rate is used to model the amount of risk associated with a component at a given time t and is formalized in HOL as follows:

Definition 5.2: *Hazard Function*

```
⊢ ∀rv t.  hazard_function rv t = @l.
   ((λa.  (survival_function rv t - survival_function rv (t + a))
                          / ((a) (survival_function rv t))) → l) 0
```

The HOL function `hazard_function` takes as input a random variable rv and a real value t and returns a real value l such that the incremental parameter a in the above definition approaches zero. The operator "@" is the hilbert's choice operator, and the operator "→" is a limit of sequence operator in HOL. The expression (`lim P = L`) is equivalent to (`(λn.  P n) → L`) in HOL and both express that the limit of a sequence P as n tends to infinity is equal to a real value L. Using Definition 5.2, we formally verified the following important property of the hazard function in HOL.

1) Hazard function is a positive function

Theorem 5.5: *Hazard function is a positive function*

```
⊢ ∀rv t.  (∀x.  CDF_in_events_bern rv x) ⇒ (0 ≤ hazard_function rv x)
```

The proof of this property involved rewriting with the definition of the hazard function and the fact that the survival function of the random variable rv is continuous and a non-increasing function (Theorem 5.4).

Using the definitions of hazard function, survival function, and CDF of random variable, we also formally verified the hazard function of Uniform, Triangle, Exponential and Weibull random variables. For example, the well known result that the

hazard function of an Exponential random variable is constant and is given by its parameter m is verified in Theorem 5.6.

Theorem 5.6: *Hazard Function, Exponential(m) Random Variable*

$\vdash \forall$ `m t.` `(0 <` $\wedge$ `m)` $\wedge$ `(0` $\leq$ `t)` $\Rightarrow$

`(hazard_function (`λ`s. exp_rv m s) t =` m`)`

The hazard function gives an indication of how a component ages. Its units are usually given as the number of failures per unit time. A larger hazard function suggests that the component is under greater risk of failure. Using Theorem 5.6, we can now formally reason about the amount of failure risk associated with a component when operating under certain stress conditions. The results presented in this section are 100% accurate, completely general and exhaustive as opposed to simulation based techniques where approximate numerical results are available for a very restricted set of parameters.

Table 5.2 summarizes the hazard function relations for the Uniform, Triangle, Exponential, and Weibull random variables.

Distribution	**Hazard Function,** $h(t)$
Uniform	$\vdash \forall$ a b t. $(0 \leq a) \wedge (a < b) \wedge (0 \leq t) \Rightarrow$ hazard_function (λs. uniform_rv a b s) t $= \frac{1}{b-t}$
Triangular	$\vdash \forall$ b t. $(0 < b) \wedge (0 \leq t) \Rightarrow$ hazard_function (λs. triangle_rv b s) t $= \frac{\frac{2}{b}(1-\frac{t}{b})}{1-\frac{2}{b}(t-\frac{t^2}{2b})}$
Exponential	$\vdash \forall$ m t. $(0 < m) \wedge (0 \leq t) \Rightarrow$ hazard_function (λs. exp_rv m s) t $= m$
Weibull	$\vdash \forall$ a b t. $(0 < a) \wedge (0 < m) \wedge (0 \leq t) \Rightarrow$ hazard_function (λs. weibull_rv a m s) t $= am^a t^{a-1}$

Table 5.2: Formally verified hazard function relations for commonly used life time distributions

5.2.3 Cumulative Hazard Function

The cumulative hazard function is used to model the total amount of risk associated with a component up to a given time t. It is defined as:

$$H_X(t) = \int_0^t h_X(\tau)d\tau \tag{5.5}$$

Its HOL formalization is given in Definition 5.3:

Definition 5.3: *Cumulative Hazard Function*

```
⊢ ∀rv t.  cumu_haz_function rv t = @l.
                        (Dint (0,t) (λa.  hazard_function rv a) l)
```

The HOL function `cumu_haz_function` takes as input a random variable rv and a real value t and returns a real value l such that l is the definite integral of the *hazard_function* over the closed interval $[a,b]$. We verified three important properties of the cumulative hazard function in HOL. They are:

1) Cumulative Hazard function at time zero is equal to zero

This property is mathematically expressed as:

$$H_X(0) = 0 \tag{5.6}$$

The HOL formalization of this property is given in Property 5.5.

Theorem 5.7: *Cumulative Hazard function at time zero is equal to zero*

```
⊢ ∀rv t.  (∀x.  CDF_in_events_bern rv x) ⇒
                        (0 = cumu_haz_function rv 0)
```

The proof of Theorem 5.7 involves rewriting with the definition of the accumulated hazard function and the properties of the definite integral when t is set to zero in Definition 5.3.

2) Cumulative Hazard function is a positive function

Hazard function is a positive function and thus its integral over the positive interval is also positive, which is mathematically expressed as:

$$0 \leq H_X(t) \tag{5.7}$$

the HOL formalization is given in Theorem 5.8.

Theorem 5.8: *Cumulative Hazard function is a positive function*

```
⊢ ∀rv t.  (∀x.  CDF_in_events_bern rv x) ⇒
                              (0 ≤ cumu_haz_function rv t)
```

The proof of Theorem 5.8 involved rewriting with the definition of accumulated function and Theorems 5.5 and 5.7.

3) Cumulative Hazard function is a monotonically increasing function

A valid cumulative hazard function must also satisfy the monotonically increasing property, which can be mathematically stated as:

$$t_1 \leq t_2 \Rightarrow H_X(t_1) \leq H_X(t_2) \tag{5.8}$$

The HOL formalization of this property is given in Theorem 5.9.

Theorem 5.9: *Cumulative Hazard function is a monotonically increasing function*

```
⊢ ∀rv  t1  t2.  ( t1 ≤ t2) ∧(∀x.  CDF_in_events_bern rv x) ⇒
                        (cumu_haz_function rv t1 ≤ cumu_haz_function rv t2)
```

The proof of Theorem 5.9 involved reasoning from Theorem 5.7 and 5.8, and the fact that for $t_1 \leq t_2$ the definite integral $\int_0^{t_2} h_X(\tau)d\tau$ can be split into a sum of two definite integrals $\int_0^{t_1} h_X(\tau)d\tau + \int_{t_1}^{t_2} h_X(\tau)d\tau$. We formally verified this and some other related basic properties of definite integrals in HOL which are not part of standard HOL

distribution. The proofs of these and other basic properties utilize the definite integral formalization of the gauge integral, theory of derivatives, fundamental theorem of calculus and the property of uniqueness of definite integral [28, 26].

Distribution	**Cumulative Hazard Function,** $H(t)$
Uniform	$\vdash \forall$ a b t. $(0 \leq a) \wedge (a < b) \wedge (0 \leq t) \Rightarrow$ cumu_haz_function (λs. uniform_rv a b s) t $= \ln\left(\frac{b-a}{b-t}\right)$
Triangular	$\vdash \forall$ b t. $(0 < b) \wedge (0 \leq t) \Rightarrow$ cumu_haz_function (λs. triangle_rv b s) t $= 2ln\left(\frac{b}{b-t}\right)$
Exponential	$\vdash \forall$ m t. $(0 < m) \wedge (0 \leq t) \Rightarrow$ cumu_haz_function (λs. exp_rv m s) t $= mt$
Weibull	$\vdash \forall$ a m t. $(0 < a) \wedge (0 < m) \wedge (0 \leq t) \Rightarrow$ cumu_haz_function (λs. weibull_rv a m s) t $= (mt)^a$

Table 5.3: Formally verified cumulative hazard function relations for commonly used life time distributions

Table 5.3 summarizes the cumulative hazard function relations for some commonly used random variables that we formally verified using Definition 5.3 and Theorems 5.7, 5.8 and 5.9.

5.2.4 Fractile Function

The p-th fractile of a distribution is the time at which the probability of failure is given by p. The p-th fractile of a lifetime distribution is given by the inverse cumulative distribution function and is formalized in HOL as follows:

Definition 5.4: *Inverse CDF function*

```
⊢ ∀f g. inverse_cdf_fun f g =
        (∀x.  (g x = 0) ⇒ x ≤ f (g x)) ∧
        (∀x.  (g x = 1) ⇒ f (g x) ≤ x) ∧
        (∀x.  0 < g x ∧ g x < 1 ⇒
              (f (g x) = x) ∧ ∀x.  0 < x ∧ x < 1 ⇒ (g (f x) = x))
```

Definition 5.5: *p-th Fractile of a life time distribution*

```
⊢ ∀rv. fractile rv = @l.  (inverse_cdf_fun l (CDF rv))
```

The HOL function `fractile` takes as input a random variable rv and returns a function l such that l is the inverse CDF function of the random variable rv. Table 5.4 lists the p-th fractile functions that we formally verified in HOL for Uniform, Triangle, Exponential, and Weibull random variables.

Distribution	**p-th Fractile**
Uniform	$\vdash \forall$ a b p t. (0 $\leq$ a) $\wedge$ (a $<$ b) $\wedge$ (0 $<$ p) $\wedge$ (p $<$ 1) $\Rightarrow$ fractile (λs. uniform_rv a b s) p = (a+p(b-a))
Triangular	$\vdash \forall$ b p t. (0 $<$ b) $\wedge$ (0 $<$ p) $\wedge$ (p $<$ 1) $\Rightarrow$ fractile (λs. triangle_rv b s) p = $b(1+\sqrt{1-p^2})$
Exponential	$\vdash \forall$ m p t. (0 $<$ m) $\wedge$ (0 $<$ p) $\wedge$ (p $<$ 1) $\Rightarrow$ fractile (λs. exp_rv m s) p = $-\frac{1}{m}ln(1-p)$
Weibull	$\vdash \forall$ a m p t. (0 $<$ a) $\wedge$ (0 $<$ m) $\wedge$ (0 $<$ p) $\wedge$ (p $<$ 1) $\Rightarrow$ fractile (λs. weibull_rv a m s) p = $\frac{1}{m}\left(-ln(1-p)\right)^{\frac{1}{a}}$

Table 5.4: Formally verified p-th fractile function relations for commonly used life time distributions

Some of the important special cases of the fractile function are the percentile, decile and quartiles. Percentile and Decile correspond to probabilities of `0.01` and `0.1`, respectively. The first, the second and the third quartiles correspond to probabilities of `0.25`, `0.50` and `0.75`, respectively. Median that separates the upper half of the distribution from the lower half of the distribution is defined as second quartile of the distribution function of a random variable. Percentile, decile and quartile are commonly used measures of reliability in electrical and mechanical engineering.

Table 5.5 lists the formalization a few fractile functions and their HOL formalization.

Using the HOL formalizations of Tables 5.4 and 5.5, we have verified a several standard properties of fractile functions of random variables used in reliability

Fractile Function	HOL Formalization
median	⊢ ∀rv. median_rv rv = fractile rv (1 / 2)
tertile	⊢ ∀rv k. kth_tertile_rv rv k = fractile rv (& k / 3)
quartile	⊢ ∀rv k. kth_quartile_rv rv k = fractile rv (& k / 4)
quintile	⊢ ∀rv k. kth_quintile_rv rv k = fractile rv (& k / 5)
sextile	⊢ ∀rv k. kth_sextile_rv rv k = fractile rv (& k / 6)
deciles	⊢ ∀rv k. kth_decile_rv rv k = fractile rv (& k / 10)
duodecile	⊢ ∀rv k. kth_duodecile_rv rv k = fractile rv (& k / 12)
vigintile	⊢ ∀rv k. kth_vigintile_rv rv k = fractile rv (& k / 20)
Percentile	⊢ ∀rv k. kth_percentile_rv rv k = fractile rv (& k / 100)
Permille	⊢ ∀rv k. kth_permille_rv rv k = fractile rv (& k / 1000)

Table 5.5: HOL definitions of commonly used fractile functions

analysis. Theorem 5.10 is presented here as an illustrative example. The median of a continuous uniform random variable `U(a,b)` is given by $\frac{(a+b)}{2}$. The HOL formalization is given in Theorem 5.10.

Theorem 5.10: *Median of a continuous uniform random variable*

⊢ ∀a b. median_rv (λs. uniform_rv a b s) = (a + b) / 2

The proof of Theorem 5.10 involved rewriting with the definition of median and `p`-th fractile of uniform random variable, given in Tables 5.4 and 5.5 respectively, and then specializing it for `p` equal to `0.5`.

In this section, we presented formalization of four important life time distribution representations, namely, the survival function, the hazard function, the cumulative hazard function and the fractile function. We also verified the lifetime distribution relations four commonly continuous random variables, namely, the Uniform, the Triangular, the Exponential and the Weibull random variables.

The lifetime distributions can be defined in other ways as well. For example, the Mellin transform [48], the moment generating function [33], the total time to test transform [6, 17], the probability density function [43], the mean residual life functions [43], the reversed hazard rate [9], and the density quartile functions [54] to name a

few. Formalization of these concepts is possible using our proposed approach and the existing theories in HOL theorem prover and the ones we have developed and described in this chapter.

The higher order logic formalization of basic reliability theory concepts, described in this section, can be used for accurate modeling and analysis of reliability problems in engineering, biostatistics, actuarial and other applied sciences. In the next section, we consider the analysis of complex systems which may contains more than one component and may be connected in an arbitrary way.

5.3 Reliability Analysis of Complex Systems

Engineering systems are usually built by connecting various functional components together to perform a particular task. The structure of the system is also determined by non functional requirements such as its reliability and maintainability. Many complex series and parallel connected systems configurations are thus possible and are carefully considered in the reliability analysis. Present day engineering designs are extremely complex consisting of hundred's of thousands of components and some time millions of components such as power plants and terrestrial and extra terrestrial vehicles such as modern speed commuter trains and the space shuttle. This increase in complexity trend is expected to increase in the forseable future. The increase in the design complexity also increases the complexity of reliability analysis and the task of making sure that such an analysis is accurate is an important concerns for engineers. Suppose a system consists of several sub systems connected in some arbitrary way. It can be shown that the reliability of such a system can be computed in terms of the reliability of its sub components, provided the components are assumed to fail independent of each other.

In reliability analysis, the system lifetimes are modeled using positive valued continuous random variables with an appropriate distribution. The events of interest are usually of type $\{T \leq t\}$ or $\{t < T\}$. Where T represents the lifetime of a system component and is a positive random variable and t is a positive real value. Let A_{sys} be the event a "system is functioning at time t". Then reliability or the probability that the system is functioning at time t is mathematically expressed as:

$$R(t) = P\{A_{sys}\} \tag{5.9}$$

List functions for Modeling of multi component system

We build on the formalization of multiple continuous random variables described in Chapter 4. In this section, we formalize behavior of various structures in higher-order logic. For modeling the behavior of multi component systems, we utilize lists of random variables with various distributions. In order to model the structure and reliability behavior of multi component systems, we first define a few list functions in higher-order logic. These higher-order logic functions are given in Table 5.6, 5.7, and 5.8 and will be explained as they appear in the formalization described in the rest of this chapter. The table also provides some of the basic list operator definitions and some of the list functions that were earlier described in Chapter 4 and are reproduced here for ease of reference.

In the rest of this section, we describe analysis of systems connected using series, parallel, series parallel, and parallel series connections. We also formalize their reliability properties and verify important system reliability results that facilitate reliability analysis of complex systems in the sound core of the HOL theorem prover.

List Functions	HOL definition
list_conj_gt	⊢ (list_conj_gt [] [] = T) ∧ (list_conj_gt (h1::t1) (h2::t2) = (h2 < h1) ∧ list_conj_gt t1 t2)
list_disj_gt	⊢ (list_disj_gt [] [] = F) ∧ (list_disj_gt (h1::t1) (h2::t2) = (h2 < h1) ∨ list_disj_gt t1 t2)
min_seq	⊢ (∀f. min_seq f 0 = f 1) ∧ ∀f n. min_seq f (SUC n) = min (f (SUC n)) (min_seq f n)
FILL_LIST_N	⊢ (∀n. FILL_LIST_N [] n = []) ∧ ∀h t n. FILL_LIST_N (h::t) n = [n] ++ FILL_LIST_N t n
FILL_LIST_NM	⊢ (∀M. FILL_LIST_NM M 0 = []) ∧ ∀M N. FILL_LIST_NM M (SUC N) = M::FILL_LIST_NM M N
FILL_LIST_R	⊢ (∀a. FILL_LIST_R [] a = []) ∧ (∀h t a. FILL_LIST_R (h::t) a = [a] ++ FILL_LIST_R t a)
LIST_SPLIT	⊢ (∀M. LIST_SPLIT [] M = []) ∧ ∀hN tN M. LIST_SPLIT (hN::tN) M = TAKE hN M::LIST_SPLIT tN (DROP hN M)
LENGTH_LIST_OF_LISTS	⊢ (LENGTH_LIST_OF_LISTS [] = []) ∧ ∀h t.LENGTH_LIST_OF_LISTS (h::t) = LENGTH h::LENGTH_LIST_OF_LISTS t
ELEL	⊢ ELEL = (λi j L. EL i (EL j L))

Table 5.6: List and Sequence Functions

List Functions	HOL definition
LENGTH	⊢ (LENGTH [] = 0) ∧ ∀h t. LENGTH (h::t) = SUC (LENGTH t)
FLAT	⊢ (FLAT [] = []) ∧ ∀h t. FLAT (h::t) = h ++ FLAT t
HD	⊢ ∀h t. HD (h::t) = h
TL	⊢ ∀h t. TL (h::t) = t
EL	⊢ (∀l. EL 0 l = HD l) ∧ ∀l n. EL (SUC n) l = EL n (TL l)

Table 5.7: HOL basic list functions and operators

List Functions	HOL definition
rv_val_indep	⊢ (rv_val_indep [] [] = []) ∧ (rv_val_indep (h1::t1) (h2::t2) = h1 h2::rv_val_indep t1 t2)
s_split	⊢ (∀M s. s_split 0 M s = [(λx. s_arb s x M) 0]) ∧ ∀N M s. s_split (SUC N) M s = (λx. s_arb s x M) (SUC N)::s_split N M s
s_arb	⊢ (∀s M i. s_arb s 0 M i = s i) ∧ ∀s n M i. s_arb s (SUC n) M i = s (M * SUC n + i)

Table 5.8: List and sequence functions defined in Chapter 4

5.3.1 Series Connected Systems

In a series connected system with N components, the system functions as long as all its components are functioning. As soon as any of the system component fails, the system fails as well. In a series connected system, the event that the system is functioning at time t is given by the intersection of events that each of the individual elements of the system is functioning at time t, that is, $A_{sys} = A_1 \cap A_2 \cap A_3 \cap ... \cap A_N$. Where A_j is the event that the "jth component of the system is functioning at time t".

Using the property of independence of multiple continuous random variables, it can be shown that:

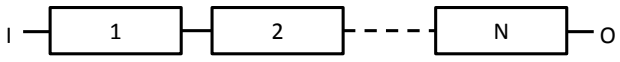

Figure 5.1: Reliability of series connected systems.

$$R(t) = P\{A_{sys}\} = P\{A_1 \cap A_2 \cap ... \cap A_n\} = P\{A_1\}P\{A_2\}...P\{A_n\} \tag{5.10}$$

$$R(t) = R_1(t)R_2(t)...R_n(t) = \Pi_{i=1}^{N} R_i(t) \tag{5.11}$$

Since $P\{A_j\}$ is the reliability of the jth component and is between zero and one, therefore the system can be no more reliable than the least reliable component in the series connected system, that is:

$$R(t) \leq \min_j R_j(t) \tag{5.12}$$

If N components of a system are connected in series and if the component lifetimes are modeled using exponential random variables with rates λ_1, λ_2, λ_3, ..., λ_N, then the overall system reliability of a series connected system is given by:

$$R(t) = R_1(t)R_2(t)...R_n(t) = \Pi_{i=1}^{N} R_i(t) \tag{5.13}$$

$$R(t) = e^{-\lambda_1 t}e^{-\lambda_2 t}....e^{-\lambda_N t} \tag{5.14}$$

$$R(t) = e^{-(\sum_{i=1}^{i=N} \lambda_i)t} \tag{5.15}$$

In such situations, the system reliability is also exponentially distributed with rate $\lambda = \lambda_1 + \lambda_2 + ... + \lambda_N = (\sum_{i=1}^{i=N} \lambda_i)$

We have formally verified these basic concepts and results in higher-order logic using the HOL theorem prover and some of the infra structure developed in this thesis.

HOL Formalization of Series Connected Systems

A series connected system consisting of a number of subcomponents is modeled using a list of random variables of type `((num->bool)->real) list`. The function `rv_val_indep` takes two lists as arguments and constructs a single list. The first argument of this function is the list of random variables `L`. The second argument is

another list. This list is generated by the function `s_split`. This generated list consists of disjoint segments of the boolean sequence `s`. Finally, `list_conj_gt` constructs a conjunction of logical terms, each of which is a greater than inequality and consists of corresponding terms from its two list arguments. Both the list arguments of `list_conj_gt` are real lists. The second argument of `list_conj_gt` is constructed by the list function `LIST_FILL_R`, which fills the list `x` with a real value `t`.

Definition 5.6: *Series System Structure Function*

```
⊢ ∀L x s t.  series_system L x s t = list_conj_gt (rv_val_indep L
(s_split (PRE (LENGTH L)) (LENGTH L) s)) (FILL_LIST_R x t)
```

Definition 5.7: *N Series System Structure Function*

```
⊢ ∀L x s t N. N_series_system L x s t N = list_conj_gt (rv_val_indep L
(s_split (PRE N) N s)) (FILL_LIST_R x t)
```

In Definition 5.7, we define a series system structure that consists of N components. Now using Definitions 5.6 and 5.7 , we define the survival function of a series connected system and a N series connected system, respectively.

Definition 5.8: *Series System Survival Function*

```
⊢ ∀X x.  series_survival_function X x = (λt.  prob bern
   {s | list_conj_gt (rv_val_indep X
       (s_split (PRE (LENGTH X)) (LENGTH X) s)) (FILL_LIST_R x t)})
```

Definition 5.9: *N Series System Survival Function*

```
⊢ ∀X x N. N_series_survival_function X x N = (λt.  prob bern {s |
list_conj_gt (rv_val_indep X (s_split (PRE N) N s)) (FILL_LIST_R x t)})
```

In Theorems 5.11 and 5.12, we verify the series connected and the N series system reliability properties.

Theorem 5.11: *Series System Reliability*

```
⊢ ∀X x t.  indep_rv_list X (FILL_LIST_R x t) ⇒
  (series_survival_function X x t = (λt.  prod1 (0,LENGTH X) (λi.
   prob bern {s | t < EL i (rv_val_indep X
                 (s_split (PRE (LENGTH X)) (LENGTH X) s))})) t)
```

Theorem 5.12: *N Series System Reliability*

```
⊢ ∀X x t N. indep_rv_list X (FILL_LIST_R x t) ⇒
  (N_series_survival_function X x N t = (λt.  prod1 (0,N) (λi.
   prob bern {s | t < EL i (rv_val_indep X
                 (s_split (PRE N) N s))})) t)
```

This proof of these two theorems follows from the definitions of the series survival function and the independence of a list of random variables. In theorems 5.13 and 5.14, we verify the reliability lower bound for a series connected system.

Theorem 5.13: *Series System Reliability Lower Bound*

```
⊢ ∀X x t.  indep_rv_list X (FILL_LIST_R x t) ⇒
   series_survival_function X x t ≤
   min_seq (λi.  prob bern {s | t < EL i (rv_val_indep X
           (s_split (PRE (LENGTH X)) (LENGTH X) s))}) (LENGTH X)
```

Theorem 5.14 corresponds to a system with N components connected in series.

Theorem 5.14: *N Series System Reliability Lower Bound*

```
⊢ ∀X x t N. indep_rv_list X (FILL_LIST_R x t) ⇒
   N_series_survival_function X x N t ≤
   min_seq (λi.  prob bern {s | t < EL i (rv_val_indep X
           (s_split (PRE N) N s))}) N
```

The recursive function `min_seq` takes two arguments, a real sequence and a natural number that represents the number of elements in the sequence and returns the minimum element of the sequence. In Theorems 5.13 and 5.14, we formally verify that the reliability of a series connected system is less than or equal to the minimum of the survival functions of the components in the series connected system. That in other words means that a series system reliability is less than the least reliable component in the series system. The proof of this theorem used Theorem 5.11 and 5.12, the definition of the survival function, the survival function of the series connected system and the definition of the independence of a list of random variables.

In Theorem 5.15 and 5.16, we verify the series system reliability modeled using exponential random variables.

Theorem 5.15: *Series System Reliability - Exponential Random Variables*

```
⊢ ∀t x a.  indep_rv_list (EXP_RV_LIST a) (FILL_LIST_R x t) ∧
  (∀i.  0 ≤ i ∧ i < LENGTH a ⇒ 0 < EL i a) ⇒
  (series_survival_function (EXP_RV_LIST a) x t =
   exp (-sum (0,LENGTH (EXP_RV_LIST a)) (λi.  EL i a) * t))
```

Theorem 5.16: *N Series System Reliability - Exponential Random Variables*

```
⊢ ∀t x a.  indep_rv_list (EXP_RV_LIST a) (FILL_LIST_R x t) ∧
  (∀i.  0 ≤ i ∧ i < N ⇒ 0 < EL i a) ⇒
  (N_series_survival_function (EXP_RV_LIST a) x t =
   exp (-sum (0,N) (λi.  EL i a) * t))
```

The proof of Theorem 5.15 and 5.16 utilizes Theorem 5.6, the definitions of the survival function, the series system survival function, and the independence of a list of random variables, the exponential random variable `CDF` and the survival function

of the exponential random variable. The proof of this theorem also utilized reasoning from real, measure, probability, and set theories in the HOL theorem prover. The product of sequence of theory did not exist in HOL theorem prover libraries and we developed this theory and proved several standard results [1]. This theory simplified the proof effort for this theorem.

5.3.2 Parallel Connected Systems

If N components of a system are connected in parallel, the system will function properly as long as at least one of the components is functioning. The system will stop functioning when all the system components fail. Let Ap be an event that all the components in the parallel connected system have failed at time t, and Asys be the event that the system is functioning at time t, then $A_p = A_{sys}$. A_p is then given by the intersection of the complements of N events, A_i, where A_i represents an event that the ith component in the parallel system is functioning at time t.

$$P\{A_p\} = P\{A_s^c\} = P\{A_1^c \cap A_2^c \cap ... \cap A_N^c\} = P\{A_1^c\}P\{A_2^c\}...P\{A_N^c\} \tag{5.16}$$

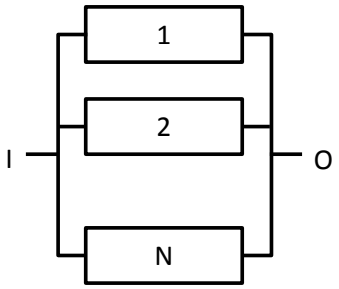

Figure 5.2: Reliability of parallel connected systems.

Using the basic probability theory properties, it can be shown that:

$$1 - P\{A_{sys}\} = (1 - P\{A_1\})(1 - P\{A_2\})...(1 - P\{A_N\}) \tag{5.17}$$

Which by the definition of reliability of a system component can be written as:

$$1 - R(t) = (1 - R_1(t))(1 - R_2(t))...(1 - R_N(t)) = \Pi_{i=1}^{N}(1 - R_i(t)) \tag{5.18}$$

and finally, it can be shown that:

$$R(t) = 1 - [(1 - R_1(t))(1 - R_2(t))...(1 - R_N(t))] = 1 - \Pi_{i=1}^{N}(1 - R_i(t)) \tag{5.19}$$

Equation 5.19 presents an important result for the reliability of a system composed of N individual components connected in parallel.

If N components of a system are connected in parallel and if the component lifetimes are modeled using exponential random variables with rates $\lambda_1 = \lambda_2 = \lambda_3 = ... = \lambda_N = \lambda$, then the overall system reliability is given by:

$$R(t) = 1 - \Pi_{i=1}^{N}(1 - R_i(t)) = 1 - \Pi_{i=1}^{N}(1 - e^{-\lambda_i t}) = 1 - (1 - e^{-\lambda t})^N \tag{5.20}$$

We have formally verified these results and concepts in higher-order logic using the infrastructure developed in this thesis research.

HOL Formalization of Parallel Connected Systems

Similar to the formalization of the series connected system, we begin the description of formalization of the parallel connected system with the definition of the parallel system survival function. In Definitions 5.10 and 5.11 the parallel system structure function is formalized.

Definition 5.10: *Parallel System Structure Function*

```
⊢ ∀L x s t.  parallel_system L x s t = list_disj_gt (rv_val_indep L
(s_split (PRE (LENGTH L)) (LENGTH L) s)) (FILL_LIST_R x t)
```

In these definitions,`rv_val_indep` constructs a list of independent random variables as described in the case of series connected systems. The function `list_disj_gt` constructs a disjunction of logical terms, each of which is greater than inequality and consists of corresponding terms from its two list arguments.

Definition 5.11: *N Parallel System Structure Function*

```
⊢ ∀L x s t N. N_parallel_system L x s t N = list_disj_gt (rv_val_indep
L (s_split (PRE N) N s)) (FILL_LIST_R x t)
```

Definition 5.12 describes the survival function of a parallel connected system.

Definition 5.12: *Parallel System Survival Function*

```
⊢ ∀X x.  parallel_survival_function X x =
  (λt.  prob bern {s | list_disj_gt (rv_val_indep X
  (s_split (PRE (LENGTH X)) (LENGTH X) s)) (FILL_LIST_R x t)})
```

In Definition 5.13, we define a parallel connected system with N element.

Definition 5.13: *N Parallel System Survival Function*

```
⊢ ∀X x N. N_parallel_survival_function X x N = (λt.  prob bern {s |
list_disj_gt (rv_val_indep X (s_split (PRE N) N s)) (FILL_LIST_R x t)})
```

Definitions 5.12 and 5.13 formally describes the parallel connected system survival functions. These function takes two and three arguments, respectively. The first argument is a list of random variables of type `((num->bool)->real) list`. The function `list_disj_gt` takes to lists as arguments and creates a logical expression that consists of disjunction of greater than inequalities involving the corresponding terms of the two input lists. The first list `(rv_val_indep X (s_split (PRE (LENGTH`

X)) (LENGTH X) s)) argument of list_disj_gt is a list of real random variables constructed in a similar manner as explained in Definition 5.6. The function FILL_LIST_R returns the list x after filling it with the variable t. Definition 5.13 describes the survival functions of a N parallel system. The third argument N represents the number of components in the parallel reliability structure.

The reliability expression for a parallel connected system and a N parallel connected system is verified in Theorem 5.17 and 5.18.

Theorem 5.17: *Parallel System Reliability*

```
⊢ ∀t X x.  indep_rv_list X (FILL_LIST_R x t) ⇒
  (parallel_survival_function X x t = 1 - prod1 (0,LENGTH X)
  (λi.  1 - prob bern {s | t < EL i (rv_val_indep X
                      (s_split (PRE (LENGTH X)) (LENGTH X) s))}))
```

Theorem 5.18: *N Parallel System Reliability*

```
⊢ ∀t X x.  indep_rv_list X (FILL_LIST_R x t) ⇒
  (N_parallel_survival_function X x N t = 1 - prod1 (0,N)
  (λi.  1 - prob bern {s | t < EL i (rv_val_indep X
                      (s_split (PRE N) N s))}))
```

The proof of this theorem begins with the rewriting of the goal of the theorem with the definitions of parallel system survival function, survival function, and the independence of list of random variables. The proof also utilized basic properties and some reasoning from the set theory the HOL theorem prover.

The reliability expression for a parallel system modeled using exponential random variables is verified in Theorem 5.19.

Theorem 5.19: *Parallel System Reliability - Exponential Random Variables*

```
⊢ ∀t m x y.  (0 < m) ∧
  indep_rv_list (EXP_RV_LIST (FILL_LIST_R y m)) (FILL_LIST_R x t) ⇒
  (parallel_survival_function (EXP_RV_LIST (FILL_LIST_R y m)) x t =
              1 - (1 - exp (-m * t)) pow LENGTH (FILL_LIST_R x t))
```

Theorem 5.20: *N Parallel System Reliability - Exponential Random Variables*

```
⊢ ∀t m x y N. (0 < m) ∧
  indep_rv_list (EXP_RV_LIST (FILL_LIST_R y m)) (FILL_LIST_R x t) ⇒
  (parallel_survival_function (EXP_RV_LIST (FILL_LIST_R y m)) x t =
              1 - (1 - exp (-m * t)) pow N)
```

The proof of Theorem 5.19 and 5.20 begins by rewriting with the definitions of parallel connected system survival function. All the exponential random variables are independent and identically distributed with the parameter `m`. The proof of this theorem also utilized reasoning from probability and set theories along with some real analysis.

5.3.3 Series Parallel Connected Systems

If a system consists of M components in parallel, where each of such parallel connected component has N components connected in series then such a system is called a series-parallel system. One such example is shown in Figure 5.3 and the reliability of such a system is given by:

$$R_{SP}(t) = 1 - \Pi_{i=1}^{N}(1 - \Pi_{j=1}^{M} R_{ij}(t)) \tag{5.21}$$

Where R_{ij} is the reliability of the jth component in the ith branch of the system.

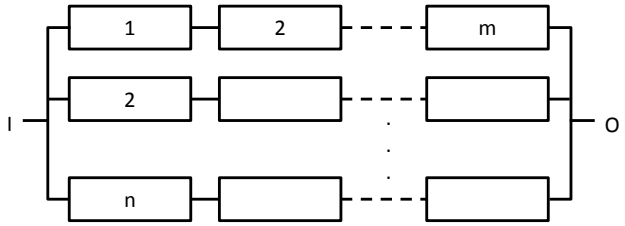

Figure 5.3: Reliability of series-parallel connected systems.

Such a system configuration is typically used to enhance the reliability at the system level.

HOL Formalization

A series parallel connected system is modeled using a list of lists. Each list in the list of lists corresponds to each of the parallel connected component. Each element of these sub lists then corresponds to the individual series component. Each element of this list is a random variable of type `(num->bool)->real` and can be chosen to have an appropriate probability distribution function.

Definition 5.14 formally describes a series parallel connected system structure.

Definition 5.14: *Series Parallel System Structure Function*

```
⊢ (∀t.  series_parallel_system [] t = F) ∧
   ∀hL tL t.  series_parallel_system (hL::tL) t =
   list_conj_gt hL (FILL_LIST_R hL t) ∨ series_parallel_system tL t
```

The function `series_parallel_system` takes two arguments, a list of lists that contains the random variables describing the series parallel system and another variable t, and recursively computes the disjunction of terms generated by the function `list_conj_gt`. List function `list_conj_gt` operates on the elements of the list of lists each of which corresponds to the series connected part of the series parallel system. The function `FILL_LIST_R` takes a list and a the variable t as arguments. It then

returns the list after filling it with the variable t. In order to illustrate the function of Definition 5.15, consider a system that consists of a parallel connection of three series connected systems. Lets assume that the first parallel component has two sub components in series, the second parallel component has three sub components in series and the third parallel component has two sub components in series. Such a system can be modeled using a lists of three lists given by `[[a1; a2]; [a3; a4; a5]; [kk; a6]]`. In this list each of the elements is a random variable that models the corresponding element in the series parallel system. The expression ⊢ `series_parallel_system [[a1; a2]; [a3; a4; a5]; [kk; a6]] t` evaluates to `((t < a1) ∧ (t < a2)) ∨ ((t < a3) ∧ (t < a4) ∧ (t < a5)) ∨ ((t < kk) ∧ (t < a6))`.

Now using the structure function of the series parallel system formalized in Definition 5.14, we define the survival function of the series parallel connected system in Definition 5.15.

Definition 5.15: *Series Parallel System Survival Function*

```
⊢ ∀L. series_parallel_survival_function L = (λt.  prob bern
  {s | series_parallel_system (LIST_SPLIT (LENGTH_LIST_OF_LISTS L)
  (rv_val_indep (FLAT L)
  (s_split (PRE (LENGTH (FLAT L))) (LENGTH (FLAT L)) s))) t})
```

The first argument of the function `series_parallel_system` is a list `(LIST_SPLIT (LENGTH_LIST_OF_LISTS L) (rv_val_indep (FLAT L) (s_split (PRE (LENGTH (FLAT L))) (LENGTH (FLAT L)) s)))`. In the construction of the list several list functions and lists are used and are briefly described in the following. The list `(s_split (PRE (LENGTH (FLAT L))) (LENGTH (FLAT L)) s)` is generated by the function `s_split` and is a list of disjoint random boolean sequences of length `(LENGTH (FLAT L))` generated from the boolean sequence `s`. In this list expression the list function `FLAT`

converts a list of lists `L` into a list that contains the elements of all the sub lists. In this conversion the order of elements in the lists is maintained. This is done by appending each of the elements of the sub lists with each other starting from the head of the list. The higher-order logic definition of this function is given in Table 5.6. The function `LENGTH_LIST_OF_LISTS` takes a list of lists as an argument and returns a list that consists of lengths of each of the lists in the list of lists. So for example, `LENGTH_LIST_OF_LISTS [[a1; a2]; [a3; a4; a5]; [kk; a6]]` returns a `[2; 3; 2]`.

The function `rv_val_indep` takes `(FLAT L)` and `(s_split (PRE (LENGTH (FLAT L))) (LENGTH (FLAT L)) s)` as inputs and generates a list that consists of independent random variables. Finally, the function `LIST_SPLIT` reconstructs the lists of lists of the parallel series system such that now each list in the lists consists of independent random variables. The second argument of the function `series_parallel_system` is the real value `t`.

To illustrate how this definition facilitates the specification of the series parallel system survival function, we construct the survival function of the series parallel system we described earlier in this section. The expression `series_parallel_survival_function [[a1; a2]; [a3; a4; a5]; [kk; a6]]` returns `(λt. prob bern {s | (t < a1 (s_arb s 6 7)) ∧ (t < a2 (s_arb s 5 7)) ∨ (t < a3 (s_arb s 4 7)) ∧ (t < a4 (s_arb s 3 7)) ∧ (t < a5 (s_arb s 2 7)) ∨ (t < kk (s_arb s 1 7)) ∧ (t < a6 (s_arb s 0 7))})`. Note that each random variable receives a disjoint segment of the random boolean sequence and that the structure of the system is series parallel is indicated by the conjunction and disjunction of various greater than inequalities.

An `N x M` series parallel structure has `N` components connected in parallel such that each of these components has `M` sub components connected in series. Definition

5.16 shows how such a system structure function can be formally specified.

Definition 5.16: *N x M Series Parallel System Structure Function*

```
⊢ ∀N M L s.  NxM_series_parallel_system N M L s =
   LIST_SPLIT (FILL_LIST_NM M N)
   (rv_val_indep (FLAT L) (s_split (PRE (N * M)) (N * M) s))
```

As an example, consider a `2 x 3` series parallel system and it needs to be specified using random variables given in the list of lists `[[a1; a2; a3]; [b1; b2; b3]]`. Definition 5.17 allows us to specify such a system as: `[[a1 (s_arb s 5 6); a2 (s_arb s 4 6); a3 (s_arb s 3 6)]; [b1 (s_arb s 2 6); b2 (s_arb s 1 6); b3 (s_arb s 0 6)]]`. Note that in this specification all the random variables receive a disjoint segment of the random boolean sequence `s`.

Definition 5.17 formally describes the series parallel survival function of a `N x M` system.

Definition 5.17: *N x M Series Parallel System Survival Function*

```
⊢ ∀L N M. NxM_series_parallel_survival_function L N M = (λt.  prob bern
  {s | series_parallel_system (LIST_SPLIT (FILL_LIST_NM M N)
  (rv_val_indep (FLAT L)
  (s_split (PRE (LENGTH (FLAT L))) (LENGTH (FLAT L)) s))) t s})
```

Lets consider a `3 x 2` parallel series system described using a list of lists given by: `[[a1; a2]; [b1; b2]; [c1; c2]]`.
The survival function of the system `NxM_series_parallel_survival_function [[a1; a2]; [b1; b2]; [c1; c2]] 3 2` is given by: `(λt.  prob bern {s | (t < a1 (s_arb s 5 6)) ∧ (t < a2 (s_arb s 4 6)) ∨ (t < b1 (s_arb s 3 6)) ∧ (t < b2 (s_arb s 2 6)) ∨ (t < c1 (s_arb s 1 6)) ∧ (t < c2 (s_arb s 0 6))})`

The reliability expression for a `N x M` parallel series system is verified in Theorem 5.21.

Theorem 5.21: *Series Parallel System Reliability*

```
⊢ ∀t x a.  (∀ L x t.  indep_rv_list (FLAT L) (FILL_LIST_R x t)) ⇒
  NxM_series_parallel_survival_function L N M t =
  1 - prod1 (0,N) (λi.  1 - prod1 (0,M)
  (λj.  prob bern {s | t < ELEL i j (LIST_SPLIT (FILL_LIST_NM M N)
  (rv_val_indep (FLAT L) (s_split (PRE (N * M)) (N * M) s)))}))
```

The proof of this theorem involved rewriting with the definitions of the NxM series parallel system survival function and the independence of a list of random variables, Theorem 5.14 and 5.18 for the series and parallel connected systems, and reasoning from the probability theory.

5.3.4 Parallel Series Connected Systems

If a system consists of M components connected in series such that each of the series component consists of N sub components connected in parallel. Such a system is called a parallel-series system and is shown in Figure 5.4.

The reliability of such a system is given by:

$$R_{PS}(t) = \Pi_{j=1}^{M}(1 - \Pi_{i=1}^{N}(1 - R_{ij}(t))) \tag{5.22}$$

Where R_{ij} is the reliability of the ijth component of the system.

Parallel-series connections can be considered as introducing component level redundancy. It can be shown mathematically that such a redundancy improves the reliability of the system more than the system level redundancy.

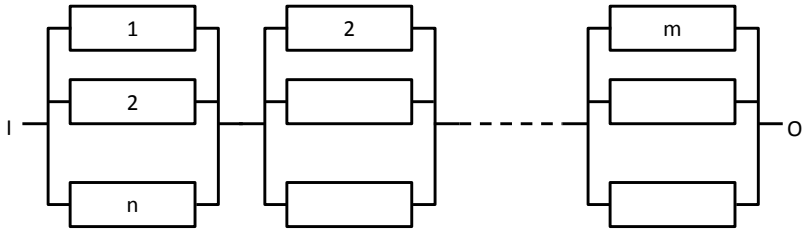

Figure 5.4: Reliability of parallel-series connected systems.

HOL Formalization of Parallel Series Connected Systems

A parallel series connected system is modeled using a list of lists. Each list in the list of lists corresponds to each of the series connected component. Each element of these lists then corresponds to the individual parallel component. Each element of this list is a random variable of type `(num->bool)->real` and can be chosen to have an appropriate probability distribution function.

Definition 5.18 describes a parallel series connected system structure.

Definition 5.18: *Parallel Series System Structure Function*

```
⊢ (∀t s.  parallel_series_system [] t = T) ∧
   ∀hL tL t.  parallel_series_system (hL::tL) t =
   list_disj_gt hL (FILL_LIST_R hL t) ∧ parallel_series_system tL t
```

Note that the function `parallel_series_system` takes two arguments, a list of lists that contains the random variables describing the parallel series system and another variable t, and recursively computes the conjunction of terms generated by the function `list_disj_gt`. List function `list_disj_gt` operates on the elements of the list of lists each of which corresponds to the parallel connected part of the parallel series system. The function `FILL_LIST_R` takes a list and a the variable t as arguments. It then returns the list after filling it with the variable t. In order to illustrate the function of Definition 5.18, consider a system that consists of a series connection of three parallel connected systems. Lets assume that the first series component has two sub

components in parallel, the second series component has three sub components in parallel and the third series component has two sub components in parallel. Such a system can be modeled using a lists of three lists given by `[[a1; a2]; [a3; a4; a5]; [kk; a6]]`. In this list each of the elements is a random variable that models the corresponding element in the parallel series system. The expression `parallel_series_system [[a1; a2]; [a3; a4; a5]; [kk; a6]] t` evaluates to `((t < a1) ∨ (t < a2)) ∧ ((t < a3) ∨ (t < a4) ∨ (t < a5)) ∧ ((t < kk) ∨ (t < a6))`.

Now using the structure function of the parallel series system formalized in Definition 5.18, we define the survival function of the parallel series connected system in Definition 5.19.

Definition 5.19: *Parallel Series System Survival Function*

```
⊢ ∀L. parallel_series_survival_function L = (λt.  prob bern
  {s | parallel_series_system (LIST_SPLIT (LENGTH_LIST_OF_LISTS L)
  (rv_val_indep (FLAT L)
  (s_split (PRE (LENGTH (FLAT L))) (LENGTH (FLAT L)) s))) t})
```

The first argument of the function `parallel_series_system` is a list `(LIST_SPLIT (LENGTH_LIST_OF_LISTS L) (rv_val_indep (FLAT L) (s_split (PRE (LENGTH (FLAT L))) (LENGTH (FLAT L)) s)))`. In the construction of the list several list function and lists are used and are briefly described in the following. The list `(s_split (PRE (LENGTH (FLAT L))) (LENGTH (FLAT L)) s)` is generated by the function `s_split` and is a list of disjoint random boolean sequences of length `(LENGTH (FLAT L))` generated from the boolean sequence `s`. In this list expression the list function `FLAT` converts a list of lists `L` into a list that contains the elements of all the sub lists. In this conversion the order of elements in the lists is maintained. This is done by appending each of the elements of the sub lists with each other starting from the

head of the list. The higher-order logic definition of this function is given in Table 5.6. The function `LENGTH_LIST_OF_LISTS` takes a list of lists as an argument and returns a list that consists of lengths of each of the lists in the list of lists. So for example, `LENGTH_LIST_OF_LISTS [[a1; a2]; [a3; a4; a5]; [kk; a6]]` returns a `[2; 3; 2]`.

The function `rv_val_indep` takes `(FLAT L)` and `(s_split (PRE (LENGTH (FLAT L))) (LENGTH (FLAT L)) s)` as inputs and generates a list that consists of independent random variables. Finally, the function `LIST_SPLIT` reconstructs the lists of lists of the parallel series system such that now each list in the lists consists of independent random variables. The second argument is the real value `t`.

To illustrate how this definition facilitates the specification of the parallel series system survival function, we construct the survival function of the parallel series system we described earlier in this section.

The expression `parallel_series_survival_function [[a1; a2]; [a3; a4; a5]; [kk; a6]]` returns `(λt. prob bern {s | (t < a1 (s_arb s 6 7) ∨ t < a2 (s_arb s 5 7)) ∧ (t < a3 (s_arb s 4 7) ∨ t < a4 (s_arb s 3 7) ∨ t < a5 (s_arb s 2 7)) ∧ (t < kk (s_arb s 1 7) ∨ t < a6 (s_arb s 0 7))})` .

Note that each random variable receives a disjoint segment of the random boolean sequence and that the structure of the system is parallel series indicated by the conjunction and disjunction of various greater than inequalities.

An `N x M` parallel series structure has been formally described in Definition 5.20.

Definition 5.20: *NxM Parallel Series System Structure Function*

```
⊢ ∀N M L s.  NxM_parallel_series_system N M L s =
  LIST_SPLIT (FILL_LIST_NM M N)
  (rv_val_indep (FLAT L) (s_split (PRE (N * M)) (N * M) s))
```

An `N x M` parallel series structure`M` components connected in series such that each of these components has `N` sub components.

As an example, consider a `2 x 3` parallel series system needs to be specified using random variables given in the list of lists `[[a1; a2; a3]; [b1; b2; b3]]`. Definition 5.20 allows us to specify such a system as: `[[a1 (s_arb s 5 6); a2 (s_arb s 4 6); a3 (s_arb s 3 6)]; [b1 (s_arb s 2 6); b2 (s_arb s 1 6); b3 (s_arb s 0 6)]]`. Note that in this specification all the random variables receive a disjoint segment of the random boolean sequence `s`.

Definition 5.21 formally describes the parallel series survival function of a `N x M` system.

Definition 5.21: *NxM Parallel Series System Survival Function*

```
⊢ ∀L N M. NxM_parallel_series_survival_function L N M =
  (λt.  prob bern {s | parallel_series_system
  (LIST_SPLIT (FILL_LIST_NM M N) (rv_val_indep (FLAT L)
  (s_split (PRE (LENGTH (FLAT L))) (LENGTH (FLAT L)) s))) t s})
```

Lets consider a `3 x 2` parallel series system described using a list of lists given by: `[[a1; a2]; [b1; b2]; [c1; c2]]`. Its survival function of the system described earlier is given by: `⊢NxM_parallel_series_survival_function [[a1; a2]; [b1; b2]; [c1; c2]] 3 2` is given by: `(λt.  prob bern {s | (t < a1 (s_arb s 5 6) ∨ t < a2 (s_arb s 4 6)) ∧ (t < b1 (s_arb s 3 6) ∨ t < b2 (s_arb s 2 6)) ∧ (t < c1 (s_arb s 1 6) ∨ t < c2 (s_arb s 0 6))})`

The reliability expression for a `N x M` parallel series system is verified in Theorem 5.22.

Theorem 5.22: *N x M Parallel Series System Reliability*

```
⊢ ∀t x a.  (∀ L x t.  indep_rv_list (FLAT L) (FILL_LIST_R x t)) ⇒
  NxM_parallel_series_survival_function L N M t =
  prod1 (0,M) (λj.  1 - prod1 (0,N)
  (λi.  1 - prob bern {s | t < ELEL i j (LIST_SPLIT (FILL_LIST_NM M N)
  (rv_val_indep (FLAT L) (s_split (PRE (N * M)) (N * M) s)))}))
```

The proof of this theorem required reasoning from probability, set, measure, boolean, and real theories and the definition of independence of random variables. The principle of induction on variables N and M was used to prove some intermediate results needed in this proof.

5.3.5 Reliability of K out of N Configurations

In many practical situations, a K out of N configuration must hold for the system to meet certain reliability requirement. Such a system connection consists of N components and K out of the N components must be operating or functional at any time for the system to be considered operating properly.

One can find many real life examples where systems consist of identical components with identical failure rates. However the failure mechanism is completely independent. Binomial distribution can be used when N components are independent and identical. For a constant failure rate, and an exponential distribution for the component lifetime, the reliability of a K-out-of-N system configuration can be mathematically expressed as:

$$R(t) = \sum_{i=K}^{N} \begin{pmatrix} N \\ i \end{pmatrix} (e^{-\lambda t})^i (1 - e^{-\lambda t})^{N-i} \tag{5.23}$$

HOL Formalization The HOL formalization of a K-out-of-N system is given in Definition 5.22.

Definition 5.22: *K out of N Parallel System Survival Function*

```
⊢ ∀X K N. parallel_K_of_N_survival_function X K N =
  (λt.  sum (K,N) (λi.  & (binomial N i) *
  (1 - prob bern {s | t < EL i (rv_val_indep X
          (s_split (PRE (LENGTH X)) (LENGTH X) s))}) pow (N - i) *
  (prob bern {s | t < EL i (rv_val_indep X
          (s_split (PRE (LENGTH X)) (LENGTH X) s))}) pow i))
```

For a parallel connected system with N components in parallel, the reliability of the system with K out of N components in working condition is verified in Theorem 5.23.

Theorem 5.23: *K-out-of-N Parallel Connected System Reliability*

```
⊢ ∀a t.  (∀X t.  {s | t < EL i (rv_val_indep X
  (s_split (PRE (LENGTH X)) (LENGTH X) s))} ∈ events bern) ∧
  (∀X t.  {s | EL i (rv_val_indep X
  (s_split (PRE (LENGTH X)) (LENGTH X) s)) ≤ t} ∈ events bern) ⇒
  (parallel_K_of_N_survival_function (EXP_RV_LIST a) K N t =
   sum (K,N) (λi.  & (binomial N i) *
   exp (-(EL i a) * t) pow (N - i) * (1 - exp (-(EL i a) * t)) pow i))
```

The proof of this theorem required rewriting with the CDF of exponential random variable along with some real analysis.

The higher-order logic formalization presented in this section of the chapter enables analysis of reliability behavior of many simple and complex engineering systems.

For example, a battery of storage cells in a renewable energy system may consist of N cells, in which a minimum of K cells must be operational for maintaining required line voltage and to provide desired current/power to the load. Such sub systems are an essential part of back up system in many industries and safety critical systems such as power generation and process industry and life support systems for vehicles meant for manned air and space flights. Accurate reliability analysis of such systems is essential. With the help of the infrastructure we have developed, we can reason about the reliability of such problems and construct formal correctness proofs and generalized reliability expressions.

Using the results presented in this chapter, reliability analysis of complex structures can be performed. Complex reliability structures can first be transformed into a combination of the four basic types of structures. Then, using the formalized results for these basic sub structures, over all reliability of complex structures can be determined. Such analysis has traditionally been done using computer simulations and suffers from accuracy problems. Moreover, it is not possible to model true independent random behavior in computer simulations. This advancement in the area of reliability analysis helps alleviate both of these limitations and such analysis was not possible before the contribution of this thesis.

5.4 Summary

In this chapter, we presented an approach for the reliability analysis of engineering systems in the sound environment of the HOL theorem prover. The approach builds upon existing formalizations of continuous random variables and the formalization of multiple continuous random variables described in Chapter 4. We presented the

formalization of commonly used lifetime distribution representations, namely the Survival function, the Hazard function, the Cumulative Hazard function and the Fractile function. We also presented the verification of several statistical properties of important lifetime distributions. The formalization described in this chapter consists of over 6000 lines of HOL code and took over 400 man-hours to complete.

The work presented in this chapter, makes it possible to perform accurate lifetime reliability modeling and analysis for the very first time in the sound environment of a theorem prover. Our proposed approach, though interactive, is very flexible and allows modeling of lifetime behavior using single and multiple parameter, bounded and unbounded continuous random variables. This allows us to model increasing, constant and decreasing failure rates together with both short and long term lifetime behaviors. In fact, at this time any random variable with a closed form CDF expression is supported and can be formally reasoned about. This ability makes it suitable for a large set of reliability analysis problems in safety-critical engineering systems.

Using this work, applications where the reliability structure of the system is series, parallel, series-parallel or parallel-series can also be modeled formally in higher-order logic and their reliability analysis can be performed in the sound core of the HOL theorem prover.

In the next chapter, we present the reliability analysis of a few applications using the infrastructure we have developed during this thesis research.

Chapter 6

Reliability Analysis Applications

In this chapter, we present three applications. The analysis described in these applications was not possible in the sound core of a theorem prover before the research presented in this thesis. Traditionally such analysis has been done using simulation based techniques. The first application deals with the analysis of lifetime behavior of electronic system components. The second application describes and formally analyzes the complex aging behavior of insulated power transmission and distribution cables that operate in harsh environments. We construct formal models of these electrical and electronic system components and then verify their useful lifetime reliability properties. The third application analyzes an important multi component mechanical engineering sub system, an automotive transmission. The analysis utilizes our multiple continuous random variable formalization.

6.1 Electronic System Components

Capacitors are an essential component of many electrical systems ranging from basic electronics used in medical devices to avionics used in aircrafts, artificial satellites

and space shuttles. Uninterruptable power supplies and inverters commonly used in renewable energy power systems contain capacitors for filtering and smoothing of rectified power line voltages. Moreover, they are used in electrical power transmission and distributions networks for power factor correction. Their reliability is absolutely essential for correct behavior of electronics used in safety critical systems and in efficient operation of electrical power systems.

Failures in electronic components most commonly occur at the beginning and towards the end of their lifetime. Throughout their useful lifetime, the electronic system components, such as capacitors, exhibit a memory less lifetime behavior. That is, a used capacitor that is functioning has the same lifetime distribution as a new capacitor. Exponential distribution is a continuous distribution that is memoryless and has a constant hazard function. That is, the risk of failure associated with such a device stays constant throughout its useful lifetime. Thus exponential distribution is the most appropriate distribution for modeling the reliability behavior of a capacitor [43]. The computation of the exponential distribution parameter or the failure rate starts with a component base failure rate value corresponding to standard operating environment and stress levels. Environment and quality factors are then used to account for the changes in the base failure rate of a component due to the variations in the environment, the operating stresses and the quality of components used in the design. Definition 8 gives the base failure rate for a capacitor [51].

Definition 6.1: *Base Failure Rate, Capacitor*

```
⊢ ∀ A B VRop Ns Top NT G H.
    cap_failure_rate_base A B VRop Ns Top NT G H =
    (A) (real_pow (real_pow (VRop / Ns) H + 1) B)
    (exp (real_pow ((Top + 273) / NT) G))
```

where A is the adjustment and B is the shaping factor (specified in [51]), VRop is the electrical stress ratio and is defined as the ratio of the operating to rated power. Ns is a stress constant, Top is the operating temperature, NT is the temperature constant, and G and H are called the acceleration constants (specified in [51]). The HOL function real_pow takes two real numbers as input and returns a real number. The returned number is equal to the first argument raised to the power of second argument of the function (i.e., real_pow A b = A^b). exp represents the exponential function. In the part failure method, each electronic system component is assigned a base failure rate corresponding to standard operating environment and stress levels. The quality and environment stress factors are used to adjust the base failure rate of a component according to the operating environment and expected stress levels. A major source of electronic component stress is its operating environment such as its operating temperature, its applied voltage, current and power levels.

The definitions of these two factors are given in [51] and are formalized in HOL as follows.

Definition 6.2: *Quality Stress Factor*

```
⊢ ∀ quality.
     cap_stress_factor_quality quality =
     (if quality = 0 then 15 / 10 else
     (if quality = 1 then 1 else
     (if quality = 2 then 3 / 10 else
     (if quality = 3 then 1 / 10 else 3 / 100))))
```

Definition 6.3: *Environment Stress Factor*

```
⊢ ∀ environment.
     cap_stress_factor_environment environment =
     (if environment = 0 then 1 else
     (if environment = 1 then 1 else
     (if environment = 2 then 2 else
     (if environment = 3 then 4 else
     (if environment = 4 then 5 else
     (if environment = 6 then 7 else
     (if environment = 6 then 15 / 2 else
     (if environment = 7 then 8 else 15)))))))))
```

The HOL formalization of these stress factors accepts a natural number as input. Each natural number represents a range of environmental parameters and returns a real number that represents the stress value. The formalization of the capacitor part failure rate, operating in a certain environment under certain electrical stress levels, is given in Definition 11.

Definition 6.4: *Part Failure Rate, Capacitor*

```
⊢ ∀ A B VRop Ns Top NT G H n m.
   cap_failure_rate_part A B VRop Ns Top NT G H n m =
   (cap_failure_rate_base A B VRop Ns Top NT G H )
   (cap_stress_factor_environment n) (cap_stress_factor_quality m)
```

6.1.1 Capacitor Lifetime Model

The capacitor life time in HOL is modeled using a function that takes as input the capacitor failure rate and returns a function of Exponential random variable of type

((num→bool)→real).

Definition 6.5: *Capacitor Lifetime Model*

```
⊢ ∀ A B VRop Ns Top NT G H n m.  cap_lifetime_model A B VRop Ns Top NT
G H n m = (λs.  exp_rv (cap_failure_rate_part A B VRop Ns Top NT G H n
m) s)
```

6.1.2 Verification of Reliability Properties of a Capacitor

The survival and hazard functions and three important statistical properties of capacitor life time are presented in this section.

6.1.2.1 Survival and Hazard Functions

Theorems 6.1 and 6.2 formally prove the survival and hazard function properties of the capacitor.

Theorem 6.1: *Survival Function, Exponential Random Variable*

```
⊢ ∀ A B VRop Ns Top NT G H n m t.
    (0 < t) ∧ (0 < A) ∧ (0 ≤ B) ∧ (0 ≤ G) ∧ (0 ≤ H) ∧
    (0 < Ns) ∧ (0 < NT) ∧ (0 ≤ VRop) ∧ (VRop ≤ 1) ∧
    (0 ≤ n) ∧ (0 ≤ m) ⇒
   (survival_function (cap_lifetime_model A B VRop Ns Top NT G H n m) t
   = exp(-(cap_failure_rate_part A B VRop Ns Top NT G H n m) t))
```

All assumptions in Theorem 6.1 except for (`0 < t`) ensure that the capacitor part failure rate (`cap_failure_rate_part A B VRop Ns Top NT G H n m`) is a positive real number.

Theorem 6.2: *Hazard Rate, Exponential Random Variable*

```
⊢ ∀ A B VRop Ns Top NT G H n m t.
    (0 < t) ∧ (0 < A) ∧ (0 ≤ B) ∧ (0 ≤ G) ∧ (0 ≤ H) ∧
    (0 < Ns) ∧ (0 < NT) ∧ (0 ≤ VRop) ∧ (VRop ≤ 1) ∧
    (0 ≤ n) ∧ (0 ≤ m) ⇒
    (hazard_function (cap_lifetime_model A B VRop Ns Top NT G H n m) t
    = cap_failure_rate_part A B VRop Ns Top NT G H n m)
```

The proof of Theorem 6.2 involved rewriting with the definitions of survival and hazard functions, part failure rate and the CDF of the Exponential random variable. The limit term is simplified using L'hopital's rule.

6.1.2.2 Statistical Properties

We formally verified several statistical properties of the capacitor lifetime using the proposed reliability analysis method in the HOL theorem prover. Three of which are presented below, namely, the mean, the second moment, and the variance of Time-to-Failure of the capacitor.

Theorem 6.3: *Mean Time-to-Failure (MTTF), Exponential(m)*

```
⊢ ∀ A B VRop Ns Top NT G H n m t.
    (0 < t) ∧ (0 < A) ∧ (0 ≤ B) ∧ (0 ≤ G) ∧ (0 ≤ H) ∧
    (0 < Ns) ∧ (0 < NT) ∧ (0 ≤ VRop) ∧ (VRop ≤ 1) ∧
    (0 ≤ n) ∧ (0 ≤ m) ⇒
    mttf (𝒰, ℰ, ℙ) (cap_lifetime_model A B VRop Ns Top NT G H n m)
    =(1)/(cap_failure_rate_part A B VRop Ns Top NT G H n m)
```

Theorem 6.4: *Second Moment of Time-to-Failure, Exponential(m)*

$\vdash \forall$ A B VRop Ns Top NT G H n m t.

(0 $<$ t) $\wedge$ (0 $<$ A) $\wedge$ (0 $\leq$ B) $\wedge$ (0 $\leq$ G) $\wedge$ (0 $\leq$ H) $\wedge$

(0 $<$ Ns) $\wedge$ (0 $<$ NT) $\wedge$ (0 $\leq$ VRop) $\wedge$ (VRop $\leq$ 1) $\wedge$

(0 $\leq$ n) $\wedge$ (0 $\leq$ m) $\Rightarrow$

second_moment $(\mathcal{U}, \mathcal{E}, \mathbb{P})$ (cap_lifetime_model A B VRop Ns Top NT G H n m)

= (2)/(cap_failure_rate_part A B VRop Ns Top NT G H n m)^2

Theorem 6.5: *Variance of Time-to-Failure, Exponential(m)*

$\vdash \forall$ A B VRop Ns Top NT G H n m t.

(0 $<$ t) $\wedge$ (0 $<$ A) $\wedge$ (0 $\leq$ B) $\wedge$ (0 $\leq$ G) $\wedge$ (0 $\leq$ H) $\wedge$

(0 $<$ Ns) $\wedge$ (0 $<$ NT) $\wedge$ (0 $\leq$ VRop) $\wedge$ (VRop $\leq$ 1) $\wedge$

(0 $\leq$ n) $\wedge$ (0 $\leq$ m) $\Rightarrow$

variance $(\mathcal{U}, \mathcal{E}, \mathbb{P})$ (cap_lifetime_model A B VRop Ns Top NT G H n m)

= (1)/(cap_failure_rate_part A B VRop Ns Top NT G H n m)^2

The proofs of the above statistical properties were greatly facilitated by the corresponding Exponential random variable statistical properties, described in Section 3.4.3. These verified statistical properties summarize the reliability behavior of the capacitor. Other statistical properties such as the standard deviation and the coefficient of variance can be similarly verified. Moreover, other probabilistic reliability properties such as the cumulative hazard function and the fractile functions can be formally proved for electronic system components using the properties we have verified in Chapters 3 and 5 of this thesis.

The proofs of the probabilistic and statistical reliability properties described in this section are accurate and general, and together with our proposed reliability analysis method provide an accurate alternative to traditional computer simulations

based reliability analysis method.

6.2 Insulated Power Cables

Insulated cables are an important component of electrical power systems that operate in harsh environment and are frequently subjected to one or more types of stresses through out their useful life. These stresses can be electrical, mechanical or environmental in nature. For example, changes in transmission voltages and presence of harmonics produce varying electric fields that stress the cable insulation material. Mechanical stresses, such as bending and vibration, and environmental stresses, such as temperature variations, pollution and humidity also have an effect on the cable insulation. All of these stresses progressively deteriorate the ability of the cable insulation material to prevent conduction. This process is sometimes called aging and is also commonly referred to as the wear of the insulation in power system literature. A cable is said to have failed or reached its end-of-life once it is no longer able to prevent conduction as a result of these applied stresses [47, 59].

Modeling of the cable aging process is an active area of research. Accurate modeling, analysis and prediction of the times when cable insulation will stop complying with its specifications plays an important role in planning, design and reliable operation of power systems. Inaccurate aging models and inaccurate analysis and prediction of the time and probability of failures can result in serious and expensive consequences for power system operators [62]. Formal methods based modeling and analysis techniques, such as the one proposed in this paper, have the potential to alleviate these limitations of the traditional inaccurate and error-prone approaches such as simulation and paper-and-pencil based approaches, respectively.

In this section, we consider an end-of-life model described in [62, 16]. This

thermodynamic model assumes that the cable aging process is triggered by the supply of heat. The model states the probability of insulation failure at time t using Weibull distribution described by the following equation.

$$P\{X \leq t\} = F_X(t) = 1 - e^{-(mt)^a} = 1 - S_x(t) \tag{6.1}$$

where a is the Weibull shape parameter. The parameter m or the scale parameter depends on several physical parameters of cable insulation material and its operating environment and is given by the following equation.

$$m = \frac{sinh(\frac{\epsilon_0 \epsilon_r \Delta V E^2}{2kT})}{\frac{h}{2\pi fkT} e^{\frac{\Delta G}{kT}}} \tag{6.2}$$

where $sinh$ is the sine hyperbolic function, ΔS is the entropy, T is the temperature, ΔH is the enthalpy, ΔV is the activation volume of the insulation material, k is the Boltzmann's constant, h is Planck's constant, f is the alternating signal frequency, ϵ_0 and ϵ_r are the absolute permittivity of free space and the relative permittivity of the insulation material, respectively, E is intensity of the electric field, and ΔG is the energy required to trigger the aging chemical reaction in the cable insulation and is given by:

$$\Delta G = \Delta H - T\Delta S \tag{6.3}$$

In [62] the author verifies the capability of this model to estimate the end-of-life time under various conditions and estimates parameters of the model for various types of cables with different insulation materials and operating voltages. In our formalization of this problem, we model the wear behavior in higher-order-logic, and verify expressions for the probability that the cable insulation will fail at a time t, as

general expressions. We also verify the instantaneous and accumulated risk associated during the useful lifetime of the cable.

The HOL formalization of the scale parameter or factor m for the Weibull distribution is given in Definition 6.6.

Definition 6.6: *Wear factor, scale factor (m) for Weibull distribution*

```
⊢ ∀ h k Tc f dV E e0 er dH dS.
     scale_fact h k Tc f dV E e0 er dH dS =
     sinh (e0 er dV E pow 2 / (2 k Tc)) /
     (h / (2 pi f k Tc) exp (dG dH Tc dS / (k Tc)))
```

In this definition *sinh* represents the sine hyperbolic function. We needed this function for modeling the wear behavior of the insulated cable as shown in Definition 13. Our formalization of hyperbolic functions includes basic definitions of the sine, cosine, tangent, cosecant, secant, and cotangent hyperbolic functions. In this formalization, we also prove commonly used hyperbolic function identities, such as $(cosh^2(x) - sinh^2(x) = 1)$ etc. We have also verified several important results related to the derivatives of hyperbolic functions and some related to the definite integral of hyperbolic functions. This formalization was greatly helped by the real number and transcendental function theories in HOL theorem prover, details of the hyperbolic function theory can be found elsewhere [3].

6.2.1 Cable Insulation Lifetime Model

The higher-order-logic life time model of an insulated cable is given in Definition 14. The insulated cable lifetime is modeled using a higher order logic function *insu_cable_lifetime_model*, which takes as input various physical parameters and returns a Weibull random variable of type (num→bool)→real

Definition 6.7: *Cable insulation lifetime model*

```
⊢ ∀ shape_fact h k Tc f dV E e0 er dH dS.
insu_cable_lifetime_model shape_fact h k Tc f dV E e0 er dH dS =
(λs. weibull_rv shape_fact (scale_fact h k Tc f dV E e0 er dH dS) s)
```

6.2.2 Verification of Reliability Properties

Theorems 6.6, 6.7, 6.8, and 6.9 prove important lifetime properties of the insulated power transmission cable. The probability that the insulated power transmission cable is functioning at a time t (survival function) is verified in Theorem 6.6.

Theorem 6.6: *Survival Function, Weibull Random Variable*

```
⊢ ∀ h k Tc f dV E e0 er dH dS shape_fact.
   (0 < shape_fact) ∧ (0 < Tc) ∧ (0 < dV) ∧ (0 < f) ∧ (0 < t)
   ⇒ (survival_function
   (insu_cable_lifetime_model shape_fact h k Tc f dV E e0 er dH dS) t =
   exp(-real_pow ((scale_fact h k Tc f dV E e0 er dH dS)
(t)) shape_fact)
```

The HOL function `real_pow` in Theorem 16 takes two real numbers as input and returns a real number. The returned number is equal to the first argument raised to the power of second argument of the function (i.e., `real_pow A b` $= A^b$).

All assumptions except for (`0 < t`) and (`0 < shape_fact`)ensure that the (`scale_fact h k Tc f dV E e0 er dH dS`) is a positive real number.

The lifetime distribution of a system can be determined from the individual lifetime distributions. Sometimes a single survival function is used to model or represent the lifetime behavior of the entire population when a large population of items has identically distributed lifetimes. In this interpretation, the survival functions of two

populations can be used to compare the survival patterns of the two populations of items [43].

The amount of failure risk associated with the insulated cable at any time t is verified in Theorem 6.7.

Theorem 6.7: *Hazard Rate, Weibull Random Variable*

```
⊢ ∀ h k Tc f dV E e0 er dH dS shape_fact.
   (0 < shape_fact) ∧ (0 < Tc) ∧ (0 < dV) ∧ (0 < f) ∧ (0 < t)
   ⇒ (hazard_function
   (insu_cable_lifetime_model shape_fact h k Tc f dV E e0 er dH dS) t =
   shape_fact (real_pow t (shape_fact - 1))
   (real_pow (scale_fact h k Tc f dV E e0 er dH dS) shape_fact ) )
```

Hazard rate represents an expression for failure risk as a function of time. The verified expression in Theorem 6.7 is completely general. The parameters in this theorem when provided specific values for the insulated cable represent the failure risk for the insulated cable as a function of time. The shape of the hazard function gives an indication of how an electronic system component ages. For example, in this case it describes how the insulated cable ages. A larger value of hazard function means that the insulated cable is under a greater risk of failure and a smaller value of this function indicates that the insulated cable is under less risk.

Moreover, with proper selection of insulated cable and weilbull distribution parameters, a decreasing, a constant, or an increasing hazard function can be modeled. The decreasing, constant, and increasing hazard functions represent risks an insulated cable experiences during its infancy, its useful lifetime, and close to its end of life, respectively.

The total amount of failure risk up to time t associated with the insulated cable is verified in Theorem 6.8.

Theorem 6.8: *Cumulative Hazard Function, Weibull Random Variable*

```
⊢ ∀ h k Tc f dV E e0 er dH dS shape_fact.
   (0 < shape_fact) ∧ (0 < Tc) ∧ (0 < dV) ∧ (0 < f) ∧ (0 < t)
   ⇒ (cumu_haz_function
  (insu_cable_lifetime_model shape_fact h k Tc f dV E e0 er dH dS) t =
  real_pow ( ((scale_fact h k Tc f dV E e0 er dH dS)(t)) shape_fact ) )
```

The p-th fractile property for the insulated cable is verified in Theorem 6.9. A special case of this property, when p=0.5, is some times is also referred to as the median lifetime of the insulated cable.

Theorem 6.9: *P-th Fractile Function, Weibull Random Variable*

```
⊢ ∀ h k Tc f dV E e0 er dH dS shape_fact p.
   (0 < shape_fact) ∧ (0 < Tc) ∧ (0 < dV) ∧ (0 < f) ∧ (0 < t) ∧
   (0 < p) ∧ (p < 1) ⇒ (fractile
   (insu_cable_lifetime_model shape_fact h k Tc f dV E e0 er dH dS) p =
   (1/(scale_fact h k Tc f dV E e0 er dH dS))
   (real_pow (-ln(1-p)) (1/shape_fact)) )
```

The proofs of the above lifetime properties were completed with the help of Weibull random variable theorems listed in Tables 5.1, 5.2, 5.3 and 5.4. It is important to note that the reliability analysis results proved in this section are completely generic expressions rather than numerical values as is the case in simulation based techniques. Moreover these results are 100% accurate as we are dealing with real numbers rather than floating point numbers as is the case in simulation based techniques. Such

analysis was not previously possible in a theorem proving environment and we believe it to be a major step forward in the direction of the formal reliability analysis of engineering systems.

6.3 Reliability Analysis of an Automobile Transmission

One of the objectives of reliability analysis is to identify and to predict the failure behavior of a system as early as possible in the design process. This allows discovery of weak points of the design and assists in their elimination in the early stages of design. In this chapter, we present the formal reliability analysis of a single stage transmission of an automobile. This example illustrates the details of the transmission system, the determination of the reliability of each system component and the calculation of the overall system reliability.

6.3.1 Automobile Transmission

The mechanical drawing of a single stage transmission is shown in Figure 6.1. The transmission transfers mechanical power from the input shaft to the output shaft using a pair of gears. The power is transmitted from a larger gear on the input shaft to a smaller gear on the output shaft.

A detailed list of all the components is given in Table 6.3.1. Some of these components are reliability relevant and some have no effect on the reliability of the transmission and are termed as reliability neutral components.

Even though this example is simple, it is practical and at the same time clearly illustrates the steps involved in the formal reliability analysis using theorem proving.

Table 6.1: Components of an automotive transmission

housing	locking washer 1	bearing cover sealing 2
housing cover	locking washer 2	bearing cover sealing 3
housing bolts	spacer ring	bearing cover sealing 4
housing cover sealing	bearing cover 1	shaft seal 1
input shaft	bearing cover 2	shaft seal 2
output shaft	bearing cover 3	roll bearing 1
gear wheel 1	bearing cover 4	roll bearing 2
gear wheel 2	hex bolt 1-12	roll bearing 3
fitting key connection	bearing cover sealing 1	roll bearing 4

The developed higher-order-logic infrastructure is capable of handling much larger problems with ease.

Figure 6.2 shows the reliability functional block diagram of the system. The rectangular blocks, in Figure 6.2 represent various components of the automotive mechanical power transmission system. The circles represent various interfaces between the components. The two and three character alpha-numeric codes inside circular symbols abbreviate the interface names and their descriptions.

The method for the determination of system reliability is outlined in Figure 6.3. It consists of three main steps. The first step is to identify the reliability relevant components determine their reliability. The second step is to determine the reliability structure of the system. Finally, based on the reliability structure of the system, calculate the overall reliability of the system. These three steps are described in detail in the rest of this section.

6.3.1.1 Reliability Relevant Components

ABC and FMEA analysis are qualitative analysis methods commonly used in the classification of system components into groups of components that are prone to risk and

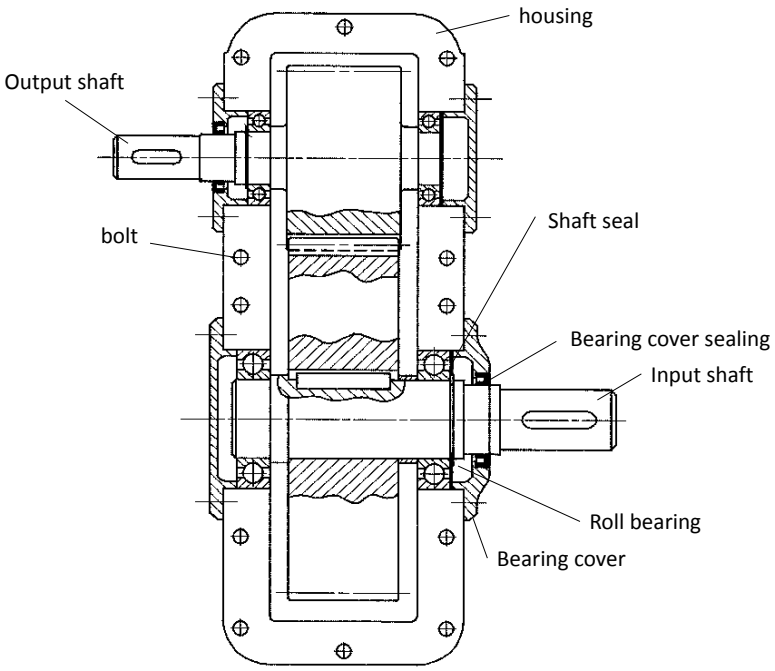

Figure 6.1: Mechanical drawing of the transmission.

those that are not. The components that are prone to failure risk are some times also called the reliability relevant components. All other components are considered reliability neutral components. ABC analysis looks at the loads and stresses experienced by each component of the system and classifies them into three categories called the A, the B and the C categories. The components belonging to groups A and B are prone to risks while components in category C are reliability neutral. The category A components are components that are loaded by defined static stresses and are involved in power transmission. Their failure behavior is determined using Wholer curves. These curves provide information needed to determine the distribution parameters of the random variables used for reliability modeling. Weibull and exponential random variables are two most commonly used random variables in the lifetime analysis of mechanical systems. The components in category B experience friction, abrasion, extreme temperatures and corrosion. For this category, the distribution parameters

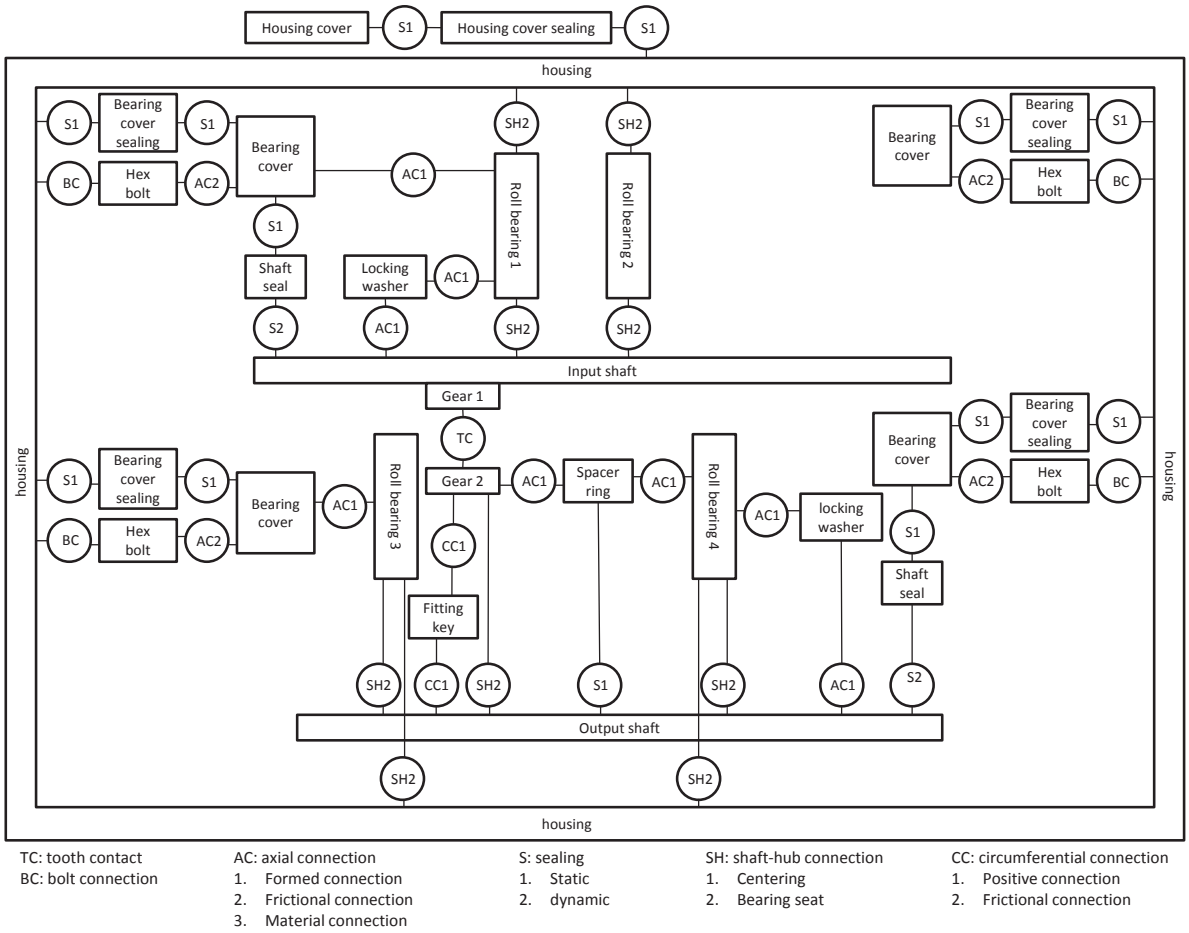

Figure 6.2: Reliability block diagram of the transmission.

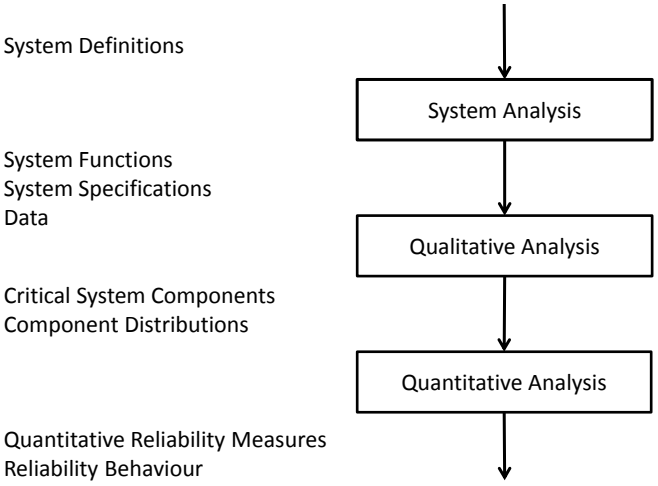

Figure 6.3: Reliability analysis method

of the random variables are determined through experiments. The category C components are randomly loaded by impacts, friction and abrasion etcetera. They are neutral to risk and usually not considered in the reliability analysis. In the ABC analysis, both the physical components and the interfaces between the components are considered in the reliability analysis. Failure Mode Effect Analysis (FMEA) is a similar qualitative analysis method that is usually applied to more complex systems. The end result in both types of analysis is the classification of components of the system in to categories depending on their risk of failure.

Using the ABC analysis, the 27 parts in the automotive transmission can be categorized into the A, B and C categories as shown in Table 6.3.1. This analysis allows us to identify the twelve reliability relevant components of the system. These components include the shafts, the bearings, the gears, the fitting keys and the seals.

Table 6.2: Reliability relevant components based on ABC analysis

Category A	Category B	Category C
input shaft	shaft seal 1	housing, housing cover, bolts and sealing
output shaft	shaft seal 2	locking washer 1 and 2
gear 1 breakage		spacer ring
gear 2 breakage		bearing cover 1-4
gear 1/2 pitting		bearing cover sealing 1-4
fitting key connection		hex bolt 1-12
roll bearing 1-4		

6.3.1.2 Automotive Transmission Reliability Structure

After the classification of the system components, the next step in the reliability analysis is to determine the reliability structure of the system. In this process, the functional block diagram and the power flow schematics are used. Both of these types of diagrams show how the mechanical power is transferred from input to output

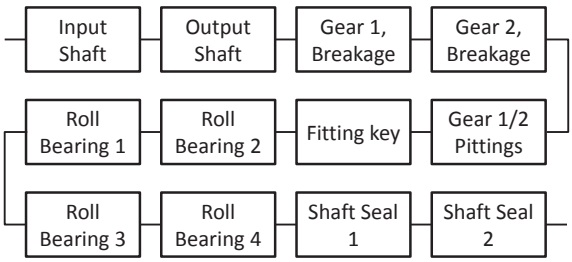

Figure 6.4: Reliability structure.

and how the system components are stressed. They also show how failure of one component affects the rest of the system. For example, from the functional block diagram of the transmission in Figure 6.2, we see that there are twelve reliability relevant components in the system, and that all of these elements of the system have to be working correctly for the system to be correct. The reliability block diagram thus has a pure serial structure as shown in Figure 6.4.

The serial block diagram and system equations represent the system reliability in terms of relevant components and their functional dependencies.

The system reliability R_{TRAN} is given by the product of the reliability of the individual components.

$$R_{TRAN} = R_{IS}.R_{OS}.R_{G1B}.R_{G2B}.R_{RB1}.R_{RB2}.R_{FK}.R_{G12P}.R_{RB3}.R_{RB4}.R_{SS1}.R_{SS2} \quad (6.4)$$

6.3.1.3 Determination of System Reliability

In real life operation of systems, it is often the case that the failure behavior of a component is not influenced by the failure behavior of other components in the system. This fact in analysis requires that the random variables used in the analysis are independent random variables. Our formalization of multiple continuous random variables enables modeling of true random and independent behavior. Simulation based techniques which have traditionally been used in computer based reliability analysis

cannot achieve true random or independent behavior. This is one of the strengths of the proposed reliability analysis approach using theorem proving technique.

6.3.2 Formal Reliability Description of the Automotive Transmission

In this analysis, we assume Weibull random variable is used to model the reliability behavior of various components of the automotive transmission. Weibull distribution is a commonly used in such analysis. We use the two parameter version of the Weibull distribution in this analysis.

The transmission components are modeled using higher-order logic functions. First a list of N independent Weibull random variables is constructed as given in Definition 6.8.

Definition 6.8: *Automotive Transmission Reliability Model*

```
⊢ ∀a b N s.  auto_rv_list a b N s =
   rv_val_indep (WB_RV_LIST a b) (s_split (PRE N) N s)
```

In Definition 6.8, `a` and `b` are lists that contains shape and scale parameters of the Weibull random variables in the `WB_RV_LIST`. `x` is a real list, `N` represents the number of components on the series reliability structure and t is a positive real value. Each element of this list represents the lifetime of a component of the transmission. Table 6.3 shows the formal models of each of the transmission components. We use these models to verify several important reliability properties of the individual components of the transmission.

Definition 6.9 formally states the reliability model of the automotive transmission. The series reliability structure is modeled using the series reliability structure definition (`N_series_survival_function`) from Chapter 5.

Definition 6.9: *Automotive Transmission Reliability Model*

```
⊢ ∀a b x N t.  auto_trans_rel_model_N a b x N t =

   N_series_survival_function (WB_RV_LIST a b) x N t
```

	Component	Formal Model
1	Input Shaft (IS)	⊢ ∀ a b t. IS_model a b x = (λs. EL 0 (auto_rv_list a b 12 s))
2	Output Shaft (OS)	⊢ ∀ a m t. OS_model a b x = (λs. EL 1 (auto_rv_list a b 12 s))
3	Gear 1, Breakage (G1B)	⊢ ∀ a m t. G1B_model a b x = (λs. EL 2 (auto_rv_list a b 12 s))
4	Gear 2, Breakage (G2B)	⊢ ∀ a m t. G2B_model a b x = (λs. EL 3 (auto_rv_list a b 12 s))
5	Roll Bearing 1 (RB1)	⊢ ∀ a m t. RB1_model a b x = (λs. EL 4 (auto_rv_list a b 12 s))
6	Roll Bearing 2 (RB2)	⊢ ∀ a m t. RB2_model a b x = (λs. EL 5 (auto_rv_list a b 12 s))
7	Roll Bearing 3 (RB3)	⊢ ∀ a m t. RB3_model a b x = (λs. EL 6 (auto_rv_list a b 12 s))
8	Roll Bearing 4 (RB4)	⊢ ∀ a m t. RB4_model a b x = (λs. EL 7 (auto_rv_list a b 12 s))
9	fitting Key (FK)	⊢ ∀ a m t. FK_model a b x = (λs. EL 8 (auto_rv_list a b 12 s))
10	Gear 1,2 Pitting (G12P)	⊢ ∀ a m t. G12P_model a b x = (λs. EL 9 (auto_rv_list a b 12 s))
11	Shaft Seal 1 (SS1)	⊢ ∀ a m t. SS1_model a b x = (λs. EL 10 (auto_rv_list a b 12 s))
12	Shaft Seal 2 (SS2)	⊢ ∀ a m t. SS2_model a b x = (λs. EL 11 (auto_rv_list a b 12 s))

Table 6.3: Formal reliability models

6.3.3 Lifetime Reliability Analysis in HOL

6.3.3.1 Reliability Analysis of Transmission Components

Using the transmission component models give in Table 6.3, we have proved the survival function, the hazard function, the cumulative hazard function and the fractile

function relations for the various components of the transmission. B1 and B10 are commonly used measures of reliability in mechanical engineering systems. They represent the 1 and the 10 percent fractiles of the lifetime random variable distribution. As an example, we list the reliability properties of the input shaft in Table 6.4. These properties were proved using the general reliability properties we verified in Chapter 5 of this thesis for the Weibull random variable. These already verified properties of the Weibull random variable reduced the interactive effort to relatively small number of steps. This shows the strength of our work in reducing the interactive analysis effort and making it less time consuming and at the same time making sure that the analysis is one hundred percent correct.

Name	**Verified Input Shaft Reliability Properties**
Survival Function	$\vdash \forall$ a b t. $(0 \leq$ EL 0 a$) \wedge (0 <$ EL 0 b$) \wedge (0 \leq$ t$) \Rightarrow$ survival_function (IS_model a b x) t $= e^{-((EL\ 0\ b)t)^{(EL\ 0\ a)}}$
Hazard Function	$\vdash \forall$ a b t. $(0 \leq$ EL 0 a$) \wedge (0 <$ EL 0 b$) \wedge (0 \leq$ t$) \Rightarrow$ hazard_function (IS_model a b x) t $= (EL\ 0\ a)(EL\ 0\ b)^{(EL\ 0\ a)}t^{(EL\ 0\ a)-1}$
Cum. Hazard Function	$\vdash \forall$ a b t. $(0 \leq$ EL 0 a$) \wedge (0 <$ EL 0 b$) \wedge (0 \leq$ t$) \Rightarrow$ cum_haz_function (IS_model a b x) t $= ((EL\ 0\ b)t)^{(EL\ 0\ a)}$
B1	$\vdash \forall$ a b t. $(0 \leq$ EL 0 a$) \wedge (0 <$ EL 0 b$) \wedge (0 \leq$ t$) \Rightarrow$ fractile (IS_model a b x) $(1/100) = \frac{1}{(EL\ 0\ b)}\,(-ln(99/100))^{\frac{1}{(EL\ 0\ a)}}$
B10	$\vdash \forall$ a b t. $(0 \leq$ EL 0 a$) \wedge (0 <$ EL 0 b$) \wedge (0 \leq$ t$) \Rightarrow$ fractile (IS_model a b x) $(1/10) = \frac{1}{(EL\ 0\ b)}\,(-ln(9/10))^{\frac{1}{(EL\ 0\ a)}}$

Table 6.4: Reliability properties of the input shaft

6.3.3.2 Reliability Analysis of the Automotive Transmission

The automotive transmission has a series reliability structure. We determined this structure as well as the reliability relevant components using the qualitative analysis

method described in section 6.3.1.

Theorem 6.10: *Automotive Transmission System Reliability*

$\vdash$ ∀a b t.(∀a b t. indep_rv_list (WB_RV_LIST a b) (FILL_LIST_R x t)) ∧
(∀i. 0 < (EL i a)) ∧ (∀i. 0 < (EL i b)) ∧ (0 ≤ t) ∧
(LENGTH (WB_RV_LIST a b) = 12) ⇒
(auto_trans_rel_model_N a b x 12 t =
prod1 (0,12) (λi. survival_function (EL i (WB_RV_LIST a b)) t))

Theorem 6.10 formally states that for an automotive transmission, consisting of 12 critical reliability relevant components, given in Table 6.3, the over all system reliability is given by the product of reliability of its individual components, provided the components of the transmission fail independent of each other.

The proof of Theorem 6.10 required rewriting with Definition 6.9 and reasoning from Theorem 5.12 for the series connected system. Theorem 6.10 provides a formal proof of correctness of the reliability specification of an automotive transmission. The expression provides a general result and is applicable to many situations. Such an analysis was not possible in theorem proving environment and is enabled because of the formalized reliability theory described in this thesis. The proofs of Theorems 6.1 through 6.10 required an order of magnitude less effort in terms of lines of HOL code and the number of man-hours required. This was mainly due to the fact that several of the general results needed for reasoning in the proofs of these theorems were available to us which we had already verified in Chapters 4 and 5. This fact shows the strength of our proposed higher-order logic framework for formal reliability analysis of engineering systems. Such analysis has traditionally been done using computer simulations which have inherent accuracy limitations. Moreover, it is not possible to create operating conditions in computer simulations that are truly random in nature

because of the use of pseudo random number generators. Computer simulations usually require hundreds of thousands of samples and sometimes even millions of samples to achieve reliability numbers with high enough confidence. With the availability of our developed framework for reliability analysis, it now possible to perform many such analyses in the sound core of the HOL theorem prover and get reliability analysis results simply by specializing the general results for specific distributions and system parameter values.

6.4 Summary

In this chapter, we presented three applications. In the first two applications, we formally analyzed the lifetime behavior of electronic system components and the complex aging behavior of insulated power transmission and distribution cables, respectively. In the third application, we utilized formalized multiple continuous random variables to perform formal reliability analysis of an automobile transmission. We described how the system, qualitative and quantitative analysis steps are performed. During modeling and analysis we showed how the proposed reliability analysis infrastructure developed in this thesis facilitated the formal analysis of the automotive transmission. It reduced the interactive effort significantly, provided formal proofs of correctness of properties and formal proofs of the analysis. Such analysis was only possible using simulation based techniques before this research. Even though this example is simple, it does highlight all the basic steps in formal reliability analysis. The infrastructure developed is general and can facilitate performance and reliability analysis. It does not have theoretical limitations as far as the number of system components and the complexity of structure is concerned.

Chapter 7

Conclusions and Future Work

7.1 Conclusions

Reliability engineering is an important area of research. Formal methods based techniques are more accurate and are better able to deal with the problem of book keeping in complex reliability problems. They provide an alternative to the traditional computer simulations and the paper-and-pencil based reliability analysis approaches. In this thesis, we presented a higher-order logic theorem proving based approach to engineering reliability analysis. We have developed an infrastructure that can be used to perform formal reliability analysis of engineering problems in the sound environment of the HOL theorem prover. Reliability models can be constructed using multiple continuous random variables and an analysis can be performed that is free from approximations. The expressive power of higher-order logic makes it possible to deal with a wide range of reliability problems, including but not limited to, commercial and industrial safety critical hardware and software systems, and large mechanical, civil and aerospace engineering systems.

The primary focus of the thesis research was on using higher-order logic theorem proving for reliability analyses of engineering systems. The basic infrastructure developed can now facilitate more complex analysis at higher levels of abstraction, where the results presented in this thesis can be used as basic primitive results. Formal modeling and analysis is a complex and time consuming task. While conducting proofs, several times clever choices have to be made to simplify reasoning in order to complete the proofs. In some cases, we proved results with slightly longer proof scripts in a shorter period of time because we reduced the reasoning from set theory to real numbers. We encountered many such situation during the proofs presented in this thesis where we had to resort to such tactics to reduce interactive effort required for the proofs. The time and effort spent in developing the basic infrastructure paid off later when we applied these results to the formalization of reliability theory. The thesis makes the following main contributions towards the development of a formal reliability analysis framework in HOL.

- Building on existing HOL theories of probability and lebesgue integration, it provides formalized statistical properties of continuous random variables. Continuous random variables and their probabilistic and statistical properties are a measures of reliability of the lifetime of the components of a system.

- It provides formalized multiple continuous random variables. In many real world engineering applications, the failure mechanisms and behaviors of components of a system are random and independent of each other. Formalized independent random variables with different distributions enable realistic modeling and analysis of practical engineering systems.

- It describes formalization of various measures of reliability and how reliability engineering problems can be modeled and analyzed in the sound core of a

theorem prover. The reliability analysis notions of the cumulative distribution function, the survival function, the hazard function, the cumulative hazard function and the fractile function are presented. Various useful properties of these measures are also verified. These theorems facilitate reasoning when constructing formal reliability proofs.

- Finally, the thesis presents several illustrative examples of applications of the work in both electrical and mechanical engineering.

We used the HOL theorem prover in this work because it had basic mathematical support already formalized in higher-order logic, that is, measure, probability, lebesgue integration, real, list and boolean theories. The task of formalization was very tedious and time consuming. Knowledge of both mathematical concepts and the HOL Theorem prover were required. Often times the proof descriptions in textbooks were not detailed enough or were hard to find. In those cases, we had to come up with proofs using the paper-and-pencil method; we then verified them interactively in the theorem prover. The theorem proving based approach is also efficient in book keeping; once a theorem is proved, it can be re-used and accessed in a much more easy fashion than in the case of the paper-and-pencil based approach. We encountered many such cases in this thesis research where a lot of initial formalization effort went into proving many helpful lemmas and theorem which later on reduced the interactive theorem proving effort for proving main results. This makes the theorem proving based approach a useful tool for both mathematicians and engineers to accurately document mathematical knowledge and make sure that the hardware and software used in safety critical applications is correct and reliable.

7.2 Future Research Directions

The contributions of this thesis can be used as a basis to enhance the reliability analysis framework presented which will allow engineers to tackle many more interesting reliability analysis problems.

- A random process is a sequence of random variables defined over a probability space. Random processes are used in the modeling and analysis of many engineering and applied-science problems. For example, the analysis of performance of a communication system operating in an uncertain environment and the study of behavior of biological processes. The infrastructure presented in this thesis formally defines the notion of a list of a random variable and verifies some of its properties. It would be interesting to extend this work and investigate the avenue of formalization of random processes and their properties. Mechanically, the process can begin with a formal definition of a random process based on a standard advanced probability textbook. This should be followed by verification of basic properties of stochastic processes to verify the logical and mathematical correctness of such a definition. This may require development of support infrastructure related to real sequences. Finally, detailed proofs should be constructed with reasoning as detailed as possible using the paper and pencil based technique. The formalization can then begin using the backward proof method. The proof steps can be continued until the proof goals are reduced to a form that are either trivial or simple enough to be discharged. Such subgoals can be added as assumptions to the main goals. Once the verification of main goals has been completed, then as many of the assumptions can be discharged as possible to make the results more general, powerful and less constrained, ideally equivalent to their mathematical statements. Finally, such results can be specialized

to create corollaries and a set of helpful lemmas and theorems that can facilitate analysis of engineering systems requiring formalized stochastic processes.

- Many engineering problems require that the multiple random variables have some correlation between the random variables to model and analyze a behaviour that is close to real world conditions. The proposed infrastructure can be used to generate correlated random variables with ease. The process would begin with the generation of correlated standard uniform random variables using techniques such as the one described in [50]. Then, using inverse transform method random variables with the desired probability distributions can be formalized [29].

- Another contribution that can be made to extend this work is to formalize methods such as the Box-Muller method [10] and the Acceptance-Rejection method for the formalization of other continuous random variables that are used in reliability analysis such as the Gaussian and the Gamma random variables.

- Lifetime distributions can also be defined using the Mellin transform [48], the moment generating function [33], the laplace and fourier transforms, the total time to test transform [6, 17], the probability density function [43], the mean residual life functions [43], the reversed hazard rate [9], and the density quartile functions [54]. Most of the needed mathematic infrastructure exists in the HOL theorem proving environment and the formalization of these concepts using our proposed approach is possible. This would further enhance the formal reliability analysis framework.

- Modern engineering systems such as, nuclear power plants and state-of-the art aircrafts consist of thousands of sub systems and millions of components working together. Such safety critical systems can be formally analyzed by using

the infrastructure presented in this thesis. There is a possibility of developing a formal automated tool that can map functional descriptions of engineering systems to predicates involving random variables, probabilities and other measures of reliability. Such a tool shall also rely on the infrastructure presented in this thesis and on some of the formal proofs we provide for modeling of complex multi component systems.

- There is a need to develop domain-specific theories in HOL to further reduce the interactive effort and facilitate the process of reasoning for formal verification engineers. One of the reasons that formal methods based approaches for analysis have not become main stream is that domain specific problem modeling and analysis is still too tedious and time consuming for an engineer or an applied scientist. A simple solution to this problem is to create domain-specific theories. For example, the two-port network theory was developed in the late 1950s to reduce the paper-and-pencil analysis required when analyzing electrical networks. Many standard results were proven and are still used to-date in the analysis of circuits and systems. The variables used in this analysis can be random variables describing some behavior of the circuit components or their environment. Formalization of the two-port network theory in higher-order logic along with the formalization of the multiple continuous random variables we present in this thesis would open up a new avenue. It would be possible to conduct formal analysis of electrical and electronic circuits and systems. For example, the formal analysis an electrical power transmission system and the front end of an ASDL modem. Moreover, it would be possible to construct proofs of correctness of functionality, performance, and reliability for such system, something that is not possible today.

Bibliography

[1] N. Abbasi. Formalization of the Product of Sequence Theory in HOL. Technical Report, Hardware Verification Group, Concordia University, Canada, 2011, http://users.encs.concordia.ca/∼n_ab/prod_seq_theory.pdf.

[2] N. Abbasi, O. Hasan, and S. Tahar. Formal Lifetime Reliability Analysis using Continuous Random Variables. In *Workshop on Logic, Language, Information and Computation*, volume 6188 of *LNCS*, pages 84–97. Springer, 2010.

[3] N. Abbasi, O. Hasan, and S. Tahar. Formalization of Weibull random variable in HOL. Technical Report, Hardware Verification Group, Concordia University, Canada, http://users.encs.concordia.ca/∼n_ab/weibullFormTR.pdf, 2010.

[4] S. M. Alam, G. C. Lip, C. V. Thompson, and D. E. Troxel. Circuit Level Reliability Analysis of Cu Interconnects. In *Proceedings of the 5th International Symposium on Quality Electronic Design*, pages 238–243, 2004.

[5] C. Baier, B. Haverkort, H. Hermanns, and J.P. Katoen. Model Checking Algorithms for Continuous time Markov Chains. *IEEE Transactions on Software Engineering*, 29(4):524–541, 2003.

[6] R. E. Barlow. Geometry of Total Time on Test Transform. *Naval Research Logistics Quarterly*, 26(3):393–402, 1979.

[7] J. Barnat, L. Brim, and D. Safranek. High-Performance Analysis of Biological Systems Dynamics with the DiVinE model checker. *Briefings in Bioinformatics*, 11(3):301–312, 05 2010.

[8] H. S Bear. *A primer of Lebesgue integration*. Academic Press, San Diego, 2002.

[9] S. Bloch-Mercier. Monotone Markov Processes with respect to the Reversed Hazard Rate ordering: An Application to Reliability. *Journal of Applied Probability*, 38(1):195–208, 2001.

[10] G. E. P. Box and Mervin E. Muller. A note on the generation of random normal deviates. *Ann. Math. Statist.*, 29(2):610–611, 1958.

[11] E. Broughton. The Bhopal Disaster and its Aftermath: A Review. *Environmental Health*, 2005.

[12] Y. Chery, S. Hau-Riege, S.M. Alam, D. E. Troxel, and C. V. Thompson. A Tool For Technology-Generic Circuit-Level Reliability Projections. In *Interconnect Focus Center Annual Review*, 1999.

[13] F. Ciocchetta and J. Hillston. Bio-PEPA: A Framework for the Modelling and Analysis of Biological Systems. *Theoretical Computer Science*, 410(33):3065–3084, 08/21 2009.

[14] A. Coble. *Anonymity, Information and Machine-assisted Proof*. PhD thesis, University of Cambridge, Cambridge, UK, 2009.

[15] A. Costes, J. E. Doucet, C. Landrault, and J. C. Laprie. SURF: A program for Dependability Evaluation of Complex Fault-Tolerant Computing Systems. In *Digest of the 11th IEEE Annual Symposium on Fault-Tolerant Computing*, pages 72–78, 1981.

[16] J. P. Crine, J. L. Parpal, and G. Lessard. A Model of Aging of Dielectric Extruded Cables. In *Proceedings of the Third International Conference on Conduction and Breakdown in Solid Dielectrics*, pages 347–351, 1989.

[17] M. Csorgo, L.Csorgo, and L. Horvath. An Asymptotic Theory for Empirical Reliability and Concentration Processes. *Communications in Statistics Theoretical Methods*, 1986.

[18] S.M. Dean. Considerations involved in making System Investments for improved Service Reliability. *EEI Bulletin*, (6):491–496, 1938.

[19] M. DeGroot. *Probability and Statistics*. Addison-Wesley, 1989.

[20] L. Devroye. *Non-Uniform Random Variate Generation*. Springer-Verlag, 1986.

[21] O. Grumberg E. M. Clarke and D. Peled. *Model Checking*. MIT Press, 2000.

[22] FIDES. *The FIDES Methodology*. 1991.

[23] D. F. Frost, K. F. Poole, and D. A. Haeussler. RELIANT: A Reliability Analysis Tool for VLSI Interconnects. In *Proceedings of the IEEE Custom Integrated Circuits Conference*, pages 27.8/1–27.8/4, 1998.

[24] J. Galambos. *Advanced Probability Theory*. Marcel Dekker Inc., 1995.

[25] M. Gordon, R. Milner, and C. Wadsworth. Edinburgh LCF. In *Lecture Notes in Computer Science*. Springer, 1979.

[26] M.J.C. Gordon and T.F. Melham. *Introduction to HOL: A Theorem Proving Environment for Higher-Order Logic*. Cambridge University Press, 1993.

[27] A. Goyal, W. C. Carter, D. E. Silva, E. Lavenberg, and K. S. Trivedi. The System Availability Estimator. In *Digest of the 16th IEEE Annual Symposium on Fault-Tolerant Computing*, pages 84–89. IEEE, 1986.

[28] J. Harrison. *Theorem Proving with the Real Numbers*. Springer, 1998.

[29] O. Hasan. *Formal Probabilistic Analysis using Theorem Proving*. PhD Thesis, Concordia University, Montreal, QC, Canada, 2008.

[30] O. Hasan, N. Abbasi, B. Akbarpour, S. Tahar, and R. Akbarpour. Formal Reasoning about Expectation Properties for Continuous Random Variables. In *Formal Methods*, volume 5850 of *LNCS*, pages 435–450, 2009.

[31] O. Hasan and S. Tahar. Performance Analysis of ARQ Protocols using a Theorem Prover. In *Proc. International Symposium on Performance Analysis of Systems and Software*, pages 85–94. IEEE Computer Society, 2008.

[32] O. Hasan, S. Tahar, and N. Abbasi. Formal Reliability Analysis Using Theorem Proving. *IEEE Transactions on Computers*, 59(5):579–592, May 2010.

[33] R. E. Hogg, J. W. McKean, and A. T. Craig. *Introduction to Mathematical Statistics. 6th Edition.* Prentice-Hall, Englewood Cliffs, N.J., 2005.

[34] J. Hurd. *Formal Verification of Probabilistic Algorithms*. PhD Thesis, University of Cambridge, Cambridge, UK, 2002.

[35] Investigative Documentary on National Geographic Channel. Derailment at Eschede.

[36] A. McIver J. Hurd and C. Morgan. Probabilistic Guarded Commands Mechanized in HOL. *Theoretical Computer Science*, 346(1):96–112, 2005.

[37] A. M. Johnson and M. Malek. SURVEY of Software Tools for Evaluating Reliability Availability and Suviceability. *ACM Computing Surveys*, 20(4), 1998.

[38] T. Kropf. *Introduction to Formal Hardware Verification*. Springer, 1999.

[39] M. Kwiatkowska, G. Norman, and D. Parker. Quantitative Analysis with the Probabilistic Model Checker PRISM. *Electronic Notes in Theoretical Computer Science*, 153(2):5–31, 2005. Elsevier.

[40] M. Kwiatkowska, G. Norman, R. Segala, and J. Sproston. Automatic Verification of Real-Time Systems with Discrete Probability Distributions. *Theoretical Computer Science*, 282(1):101–150, 2002. Elsevier.

[41] K. Labadi, S. Saggadi, and L. Amodeo. PSA-SPN - a Parameter Sensitivity Analysis Method Using Stochastic Petri Nets: Application to a Production Line System. *AIP Conference Proceedings*, 1107(1):263–268, 03/05 2009.

[42] J. H. Lala. *Mark1 Markov Modeling Package*. The Charles Stark Draper Laboratory, Cambridge, Massachusetts, 1983.

[43] L.M. Leemis. *Reliability: Probabilistic Models and Statistical Methods*. Ascended Ideas, 2009.

[44] M. Leucker and C. Schallhart. A Brief Account of Runtime Verification. *Journal of Logic and Algebraic Programming*, 78(5):293–303, 2009.

[45] T. Mhamdi, O. Hasan, and S. Tahar. On the Formalization of the Lebesgue Integration Theory in HOL. In *Theorem Proving in Higher-Order Logics*, volume 6172 of *LNCS*, pages 387–402. Springer, 2010.

[46] M. Mitzenmacher and E. Upfal. *Probability and Computing*. Cambridge University Press, 2005.

[47] G.C. Montanari and L. Simoni. Aging Phenomenology and Modeling. *IEEE Transactions on Electrical Insulation*, 28(5):755–776, October 1993.

[48] P. G. Moschopoulos. A General Procedure for Deriving Distributions. *Communications in Statistics Theoretical Methods*, 12(17):2005–2015, 1983.

[49] P. M. Nagel. Software Reliability: Repetitive Run Experimentation and Modeling. Technical Report NASA CR-165836, Boeing Computer Services Co., 1982.

[50] L. M. Novak. Generating correlated weibull random variables for digital simulations. In *Decision and Control including the 12th Symposium on Adaptive Processes, 1973 IEEE Conference on*, volume 12, pages 156 –160, dec. 1973.

[51] US Department of Defence. *Reliability Prediction of Electronic Equipment, Military handbook, MIL-HDBK-217F*. 1991.

[52] U.S. Department of Defense. *Reliability-Centered Maintenance (RCM) Requirements for Naval Aircraft, Weapon Systems, and Support Equipment, MIL-HDBK-2173*. 1998.

[53] Institute of Electrical and Electronics Engineers. *IEEE Standard Reliability Program for the Development and Production of Electronic Systems and Equipment, IEEE 1332,*. 1998.

[54] E. Parzen. Nonparametric Statistical Data Modeling. *Journal of American Statistical Association*, 74(365):105–131, 1979.

[55] Leslie W. Ball Richard H. Myers. *Reliability Engineering for Electronic Systems*. J. Wiley, 1964.

[56] Rogers Commission report, Report of the Presidential Commission on the Space Shuttle Challenger Accident, Volume 1, chapter 4, page 72. http://history.nasa.gov/rogersrep/v1ch4.htm, 1986.

[57] J. Rutten, M. Kwaiatkowska, G. Normal, and D. Parker. *Mathematical Techniques for Analyzing Concurrent and Probabilisitc Systems*, volume 23 of *CRM Monograph Series*. American Mathematical Society, 2004.

[58] W. H. Sanders and J. F. Meyer. METASAN: A Performability Evaluation Tool based on Stochastic Activity Networks. In *Proceedings of the 1986 Fall Joint Computer Conference, AFIPS*, pages 807–816, 1986.

[59] L. Simoni. *Fundamentals of Endurance of Electrical Insulating Materials*. CLUEB: Bologna, Italy, 1983.

[60] J. J. Stiffler, L. A. Bryant, and L. Guccione. CARE III Final Report Phase I volume I and II. Technical Report NASA Contractor Rep. 159122 and 159123., SRI International, November 1979.

[61] R. H. Tu, E. Rosenbaum, W. Y. Chan, C. C. Li, E. Minami, K. Quader, P. K. Ko, and C. Hu. Berkeley reliability tools-bert. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 12(10):1524–1534, 1993.

[62] P.N. Vovos. Economic System Operation Considering the Cost of Wear of Cables. *IEEE Transactions on Power Systems*, 26(2):642 –652, May 2011.

[63] R. E. Wernikoff. Outline of Lebesgue Theory: A Heuristic Introduction. Technical Report 310, Research Laboratory of Electronics, Massachusettes Institute of Technology, Cambridge, Massachusetts, 1957.

[64] B. Widrow. Statistical Analysis of Amplitude-quantized Sampled Data Systems. *AIEE Trans. (Applications and Industry)*, 81:555–568, January 1961.

[65] D. Williams. *Probability with Martingales*. Cambridge University Press, 1991.