Journal of Computer and System Sciences 80 (2014) 323–345

Contents lists available at SciVerse ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

An approach for lifetime reliability analysis using theorem proving

Naeem Abbasi *, Osman Hasan, Sofiène Tahar

Dept. of Electrical & Computer Engineering, Concordia University, 1455 de Maisonneuve West, Montreal, Quebec, H3G 1M8, Canada

ARTICLE INFO

Article history:
Received 1 November 2010
Received in revised form 20 February 2012
Accepted 4 April 2013
Available online 7 June 2013

Keywords:
Reliability analysis
Lifetime analysis
Failure rate
Hazard function
Fractile function
Statistical properties
Random variables
Formal methods
Theorem proving
HOL

ABSTRACT

Recently proposed formal reliability analysis techniques have overcome the inaccuracies of traditional simulation based techniques but can only handle problems involving discrete random variables. In this paper, we extend the capabilities of existing theorem proving based reliability analysis by formalizing several important statistical properties of continuous random variables like the second moment and the variance. We also formalize commonly used concepts about the reliability theory such as survival, hazard, cumulative hazard and fractile functions. With these extensions, it is now possible to formally reason about important measures of reliability (the probabilities of failure, the failure risks and the mean-time-to failure) associated with the life of a system that operates in an uncertain and harsh environment and is usually continuous in nature. We illustrate the modeling and verification process with the help of examples involving the reliability analysis of essential electronic and electrical system components.

1. Introduction

Tragedies such as the industrial accident in the union carbide pesticide plant in Bhopal, India [1], the space shuttle Columbia and Challenger accidents [2], and the high-speed train accident near the village of Eschede in Lower Saxony in Germany [3] all 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 specified period of time under the specified environmental conditions [4]. The two most popular representations of the distribution of the lifetime of a system are the survival function and the hazard function [4]. The survival function describes the probability that a system is functioning at any time t, and the hazard function describes the failure risk at a time t.

Traditionally, reliability analysis has been done using either paper-and-pencil or simulation based approaches. In engineering applications, the paper-and-pencil approach very quickly becomes impractical because of the amount of detail involved. Simulation based reliability analysis is popular because of the availability of a number of automated tools. Unfortunately, the simulation based analysis is neither accurate nor can it truly model random behavior. Computer simulations rely on floating-point numbers based representation of system parameters which can lead to errors in reliability analysis and thus can have costly consequences. For example, the floating point bug in Intel Pentium 5 was related to a few missing entries in the lookup table used by the digital divide operation algorithm. This resulted in rare round-off errors. Intel eventually had to recall the flawed chips at a cost of over 475 million dollars [5]. Moreover, simulation based techniques use

[*] Corresponding author.
E-mail addresses: n_ab@ece.concordia.ca (N. Abbasi), o_hasan@ece.concordia.ca (O. Hasan), tahar@ece.concordia.ca (S. Tahar).

0022-0000/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jcss.2013.05.002

pseudo random number generators for simulating the random behavior and require a large number of computing resources. Another problem with the simulation based analysis is the time needed to compile and interpret simulation results. Some simulation based methods [6] utilize computation tools, such as MATLAB [7], which supports arbitrarily large base sizes for number representation and helps in controlling computational errors. This, however, comes at the cost of significant increase in simulation times. For some applications, such as communication networks, the simulation softwares often make overly simplified assumptions which are not realistic [8] or use different levels of details [9] and lead to results that do not match real world measurements. Formal method-based techniques are 100% accurate and allow the modeling and analysis of true random behavior and thus provide an alternative approach for reliability analysis of the critical parts of a system.

Formal techniques that analyze system reliability using probabilistic models, such as probabilistic model checking, are accurate; however, they cannot effectively handle properties that summarize the statistical behavior of a lifetime distribution, such as its moments and variance. Moreover, similar to traditional model checking techniques, probabilistic model checking techniques also suffer from the state space explosion problem, and, therefore, only a small set of reliability analysis problems can be handled using these techniques. With techniques based on theorem proving, it is possible to accurately deal with complexity and reason about reliability analysis related probabilistic and statistical properties for large sized engineering problems. These techniques, however, are very often interactive and require a formalized infrastructure for reasoning.

The state of the art in theorem proving based probabilistic analysis consists of a formalization of measure and probability theories [10], discrete and continuous random variables and their probabilistic [11] and expectation properties [11,12]. Some of these foundations have been utilized to asses reliability aspects involving discrete random variables [13] and expectation properties of continuous random variables [12]. Despite these efforts, there are many reliability aspects that cannot be reasoned about in a mechanical theorem prover, namely, the higher-order moments, variance and the concepts of survival function, hazard function, cumulative hazard function and fractile function. In this paper, we formalize these reliability fundamentals by building upon the existing probability [10–12] and reliability [14] theory foundations. Our first contribution is to formally verify a general expression that facilitates reasoning about the second moment of bounded continuous random variables that ranges over the interval $[a, b]$.

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

where E is the expectation operator, X is the bounded random variable, and $\mathbb{P}$ is the probability measure. $E[X^2]$ represents the expectation of X squared with respect to $\mathbb{P}$. The initial verification effort involved in proving the correctness of this general result in an interactive theorem proving environment is quite significant. However, it makes the interactive verification of statistical properties of specific random distributions less tedious to handle. This is mainly because the reasoning involved in the verification of statistical properties now involves the concepts of summation of sequences and their limits rather than relatively more involved concepts from set, measure and Lebesgue integration theories.

The second main contribution of this paper is that we utilize the general expression of Eq. (1), along with a similar expression for unbounded random variables, given in [14], to verify several important statistical properties of random variables that are commonly used in reliability analysis. For example, the second moment and variance relations for the Uniform, Triangular, and Exponential random variables are verified. When short term lifetime behavior of a system is of interest uniform distribution is preferred. When very little information about the lifetime behavior of a system is known (such as the rough estimates of the minimum and maximum life of a system, as is sometimes the case in the initial planning and design stages), reliability engineers prefer triangular random distribution. And finally, exponential distribution accurately models constant failure rate behavior, which is the most commonly used distribution for lifetime modeling of electronic and electrical components of a system.

Different lifetime distribution representations have been used in the past depending upon the specific needs of the problem of analyzing lifetime. For example, sometimes the probability of failure is of interest at a certain time (survival function), whereas, in another 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 [15]. Two commonly used important reliability properties of survival function and hazard function have already been formalized in [14]. We add to these two more equally important lifetime distribution representations of cumulative hazard function and the fractile function. Cumulative hazard function gives the amount of risk associated with a system up to a given time while the fractile functions allow reasoning about times for a given probability of failure [4]. The survival function $S_X(x)$ is defined as:

$$S_X(t) = 1 - F_X(t) \tag{2}$$

where $F_X(x)$ is the cumulative distribution function of the random variable X. The hazard function, $h_X(t)$, is defined as:

$$h_X(t) = -\frac{\frac{dS_X(t)}{dt}}{S_X(t)} = \lim_{h\to 0}\frac{S_X(t) - S_X(t+h)}{hS_X(t)} \tag{3}$$

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

$$H_X(t) = \int_0^t h_X(\tau)\,d\tau \tag{4}$$

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

$$t_X(p) = F_X^{-1}(p) \tag{5}$$

This paper's contributions lie in higher-order-logic formalization of the reliability concepts and proof of the important properties of the reliability theory using theorem proving. However, it does not contribute any semantic innovation to the underlying logic.

Finally, to illustrate the practical effectiveness of our reliability theory formalization, we present two examples of applications: the lifetime reliability analysis of an electronic system component (a capacitor) and the lifetime analysis of insulated power transmission cable. Both are critically important components of electrical power systems; and, to the best of our knowledge, the reliability modeling and analysis of such system components were, until now, only possible using inaccurate simulation based techniques. We utilize the method described in [13] to conduct this reliability analysis. The method allows modeling of functional, performance and lifetime behavior using discrete and continuous random variables with appropriate distributions. The analysis is then mechanically and interactively done in the sound environment of the HOL theorem prover [16].

The rest of the paper is divided into eight sections. Section 2 reviews related work. Section 3 describes higher-order-logic formalizations of measure, probability, continuous random variables and Lebesgue integration theories along with some notations referred to in the rest of the paper. Section 4 presents the formalization and verification of statistical properties of continuous random variables. In Section 5, using the verified second moment results of Section 4, the second moment and variance properties of Uniform, Triangular and Exponential random variables are verified. Section 6 describes the formalization of reliability theory concepts of survival, hazard, accumulated hazard, and fractile functions. For illustration purposes, Section 7 presents the reliability analyses of a capacitor and of an insulated cable used in electrical power transmission and distribution systems. Finally, Section 8 concludes the paper.

2. Related work

A system is considered dependable if it is reliable, available, safe and secure [17]. Reliability refers to continuity of service and is an important component of dependability. Availability relates to readiness for use; safety deals with avoiding catastrophic consequences on the environment; and security means preservation of confidentiality. The process for modeling and analysis of dependability starts with a mathematical description of faults and failure mechanisms. The analysis involves use of random variables with appropriate probability distributions and verifies the dependability requirements of the system. In this section, we focus on the work related to one of the most important attributes of dependability: reliability.

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 [19].

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 [20]. 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 [21], FIDES [22], and IEEE 1332 [23] 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 nondeterminism 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. In these cases, model checking and simulation based techniques have an advantage over theorem proving based techniques. For these and other reasons, simulation is often chosen as the reasonable alternative to formal techniques. The price paid, of course, is the compromise made with accuracy, computation time and computation resources. Simulation based analysis cannot be termed 100% accurate and free from computational inaccuracies because of the use of fixed and floating point arithmetic and the use of pseudo random numbers instead of true random numbers. Table 1 lists a few examples of simulation based tools for analyzing reliability and their applications.

Formal methods for performance analysis include run time verification [34], model checking [35] and theorem proving [17]. These techniques have been extended to analyze reliability of systems during the last two decades. Run time

Table 1
Simulation based reliability analysis tools [15].

Reliability analysis tool	Description and application
CARE [24,25], ARP [15], SHARE [15], SURF [26], AIRES [15]	Fault Tolerant Computer Architectures
RELIANT [27], SysRel [28], ERNI [29]	Integrated Circuit conductor reliability and failure analysis, predict reliability and hazards due electro-migration
MARK1 [30]	Markov Modeling Package
METASAN [31]	Michigan Evaluation Tool for the Analysis of Stochastic Activity Networks
SAVE [32]	System AVailability Estimation
BERT [33]	BErkely Reliability Tool

verification checks properties of the system during execution. In this technique, a formal specification language is used to describe the system properties, while simulation is used to check the compliance of the functional, the performance and the reliability requirements. Other expressive formalisms such as stochastic Petri nets [36] and process algebras [37] along with various probabilistic [38] and stochastic temporal logics [39], and compositional and guarded command notations [40] have been used in modeling, specification and analysis of complex engineering [41] and applied science problems [42].

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 [43,44]. Probabilistic model checkers, for example PRISM [45], 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, 100% 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 paper, 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 involve discrete random variables in a theorem proving environment. Hurd [10] formalized a probability theory along with discrete random variables in the HOL theorem prover [16]. Building upon Hurd's work [10], Hasan [11] formalized statistical properties of single and multiple discrete random variables. Hasan [11] also formalized a class of continuous random variables for which the inverse CDF functions can be expressed in a closed form. Hasan et al. [13] 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. In [12], Hasan et al. formalized expectation for both bounded and unbounded continuous random variables in the HOL theorem prover. An expression of second moment of unbounded random variables was verified by Abbasi et. al [14]. Both of these works utilized the Lebesgue integration theory for the verification of statistical properties of continuous random variables developed in [46] and [47].

Despite the general nature of the Lebesgue integral and the fact that it can handle a larger class of functions than the Riemann integral, the underlying mathematical complexity of the verification of expectation and other statistical properties, using interactive higher-order-logic theorem proving, makes this approach very tedious. An ingenious solution to this problem that is ideally suited to interactive theorem proving environments is presented in [12], where the authors first verified general expressions for the expectation of both bounded and unbounded continuous random variables. The initial, one time effort in the verification of these general expressions was significant. But these general expressions only consist of summations and limit of sequences. The authors of this work convincingly demonstrate the usefulness of such results in the verification of expectation property of arbitrary continuous random variables.

This paper is an extended version of the work presented in [14]. We build upon the higher-order-logic formalization of [13] and follow an approach similar to that first proposed by Hasan et al. [12], utilizing the Lebesgue integration theories developed in [46] and [47]; and in doing so we verify an additional general expression for the second moment of bounded continuous random variables. Thus we avoid having to deal with complex reasoning and, at the same time, benefit from the general nature of the Lebesgue integral. We have formalized two more important concepts commonly used in reliability analysis, that is the cumulative hazard function and the fractile function. This paper also includes the verification of some of the classical properties associated with these concepts along with an additional case study.

Table 2
Continuous random variables in HOL.

Distribution	CDF	Formalized random variable
Uniform(a, b)	0 if $x \leqslant a$; $\frac{x-a}{b-a}$ if $a < x \leqslant b$; 1 if $b < x$.	$\vdash \forall$s a b . uniform_rv a b s = (b − a)(std_unif_rv s) + a
Triangular$(0, b)$	0 if $x \leqslant 0$; $(\frac{2}{b}(x - \frac{x^2}{2b}))$ if $0 < x < b$; 1 if $b \leqslant x$.	$\vdash \forall$s b . triangular_rv b s = b(1 − $\sqrt{1 - \texttt{std\_unif\_rv s}}$)
Exponential(m)	0 if $x \leqslant 0$; $1 - e^{-mx}$ if $0 < x$.	$\vdash \forall$s m . exp_rv m s = $-\frac{1}{\mathtt{m}}$ln (1 − std_unif_rv s)

3. Preliminaries

In this section, we provide an overview of the higher-order-logic formalizations of probability theory, continuous random variables and Lebesgue integration theory. Main ideas and some notation is also introduced that is used later in this paper.

3.1. 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 these subsets are usually referred to as *measurable sets*, and μ is a *measure* with domain Σ [48]. A *probability space* is a measure space $(\Omega, \Sigma, \mathbb{P})$ where Ω is the sample space, Σ is the set of events, and $\mathbb{P}$ is the probability measure. Measure theory in HOL, formalized by Hurd [10], defines a measure space as a pair (Σ, μ). The sample space, on which this pair is defined, is implicitly assumed to be equal to the universal set of the appropriate data-type. The probability space in HOL is defined as 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 in HOL is modeled in higher-order logic as a deterministic function, which accepts the infinite Boolean sequence as an argument. This function makes random choices based on popping as many random bits as needed for the computation. When this function terminates, it returns 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 $\mathcal{F}$.

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

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 follows

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

It accepts an infinite Boolean sequence, where shd and stl are the sequence equivalents of the list operation *'head'* and *'tail'*. The formalized $\mathbb{P}$ and $\mathcal{E}$ have been used to verify the basic laws of probability and the probabilistic properties of random variables in the HOL theorem prover.

The above approach has been successfully used to formalize and verify most of the commonly used discrete random variables [10].

3.2. Formalization of continuous random variables in HOL

An approach for the formalization of continuous random variables, based on the work of [10], was presented in [11]. It uses the Inverse Transform Method (ITM) [49] to formalize continuous random variables for which an expression for inverse CDF function of the random variable can be determined. For example, for a random variable X with continuous cumulative distribution function (CDF) F, is formalized as $X = F^{-1}(U)$, where F^{-1} is the inverse function of F, and U represents the Standard Uniform random variable. Based on this approach, the CDFs and higher-order-logic definitions of three continuous random variables are given in Table 2. The Uniform, the Triangular and the Exponential random variables were formalized in [11].

In this paper, we formalize and verify the CDF properties of the Weibull random variable, which is one of the most commonly used continuous random variable in the reliability analysis literature. It has two parameters, a shape and a scale parameter and using these parameters it can be used to suit many reliability analysis needs. For example, it can be used to model increasing, constant and decreasing failure rate behavior by making its shape parameter less than, equal to, or greater than one, respectively. In fact, exponential life time distribution presented in [14] is a special case of the Weibull random variable when the shape parameter is set equal to 1.

Table 3
HOL formalization of Weibull random variable.

Property description	Formalization in HOL
Definition $X = \frac{1}{m}(-ln(1-U))^{\frac{1}{a}}$	⊢ ∀a m s. weibull_rv a m s = (1 / m) real_pow (−ln (1 − std_unif_cont s)) ($\frac{1}{a}$)
Cumulative density function $F_X(x) = 1 - e^{-(mx)^a}$	⊢ ∀x a m. (0 < a) ∧ (0 < m) ⇒ (prob bern {s | weibull_rv a m s ⩽ x} = (if x ⩽ 0 then 0 else 1 − exp (−real_pow (mx) a)))
Inverse cumulative distribution function $F_X^{-1}(x) = \frac{1}{m}(-ln(1-(x)))^{\frac{1}{a}}$	⊢ ∀x a m. (0 < a) ∧ (0 < m) ⇒ INV_CDF_FN (λx. (1 / m) real_pow (−ln (1 − x)) ($\frac{1}{a}$)) (λx. (if x ⩽ 0 then 0 else (1 − exp (−real_pow (mx) a))))
CDF at negative infinity $\lim_{n\to-\infty} F_X(x) = 0$	⊢ ∀x a m.(0 < a) ∧ (0 < m) ⇒ (λn. (λx. (if x ⩽ 0 then 0 else (1 − exp (−real_pow (mx) a)))) ((λn. & n) n)) → 0
CDF at positive infinity $\lim_{n\to+\infty} F_X(x) = 1$	⊢ ∀x a m. (0 < a) ∧ (0 < m) ⇒ (λn. (λx. (if x ⩽ 0 then 0 else (1 − exp (−real_pow (mx) a)))) ((λn. & n) n)) → 1
CDF monotonic non-decreasing *if* $(c \leqslant d)$ *then* $F_X(c) \leqslant F_X(d)$	⊢ ∀x a m. (0 < a) ∧ (0 < m) ⇒ ∀c d. (c < d) ⇒ (λx. (if x ⩽ 0 then 0 else (1 − exp (−real_pow (mx) a)))) c ⩽ (λx. (if x ⩽ 0 then 0 else (1 − exp (−real_pow (mx) a)))) d
CDF bounded $0 \leqslant F_X(x) \leqslant 1$	⊢ ∀x a m. (0 < a) ∧ (0 < m) ⇒ ((prob bern {s | weibull_rv a m s ⩽ x} ⩽ 1) ∧ (0 ⩽ prob bern { s | weibull_rv a m s ⩽ x }))

In Table 3, we summarize formalization of Weibull random variable. Only a few selected results are included here due to space limitations. They include the definition of Weibull random variable, as it is formalized in HOL, using the inverse transform method [50], and important properties of its CDF function. The first column of the table includes a brief description of the property along with its mathematical representation. For example, X represents the random variable, F_X represents the CDF function of X and U represents the standard Uniform random variable. The variables and notation used in this table is as follows: a and m are the shape and scale parameters of the Weibull random variable. s is a variable of type num → bool. `real_pow` takes two real arguments and returns a real value such that the result is first argument raised to the power second argument of the function. `exp` is the exponential function. `std_unif` represents the standard Uniform random variable. `weibull_rv` is the Weibull random variable, and `INV_CDF_FN` is a predicate that takes two function arguments. & is an operator that takes an argument of type num and returns a real. ⇒ is the logical implication operator and → is a convenient abbreviation for tends-to or approaches a certain value on the right hand side of this operator.

We will see the four reliability theory properties of Weibull random variable and its application to a critical engineering application later in this paper.

3.3. 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* [48].

In HOL Lebesgue integration theory [47], 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, described in this paper are such well-behaved functions. We utilize the following convergence of a non-negative integrable function f property in this paper to verify the second moment relation given in Eq. (1).

Theorem. *If f is any non-negative integrable function, there exists a sequence of positive simple functions (f_n) such that $\forall n\, x.\ f_n(x) \leqslant f_{n+1}(x) \leqslant f(x)$ and $\forall x.\ f_n(x) \to f(x)$, and*

$$\int_\Omega f\,d\mu = \lim_n \int_\Omega f_n\,d\mu \tag{6}$$

In the next section, we utilize this property of Lebesgue integral to verify a general expression for the second moment of the continuous random variables.

Table 4
Statistical properties and their HOL formalizations.

Property	Definition	HOL formalization
Expec. $h(X)$	$E[h(X)] = \int_{\mathcal{U}} h(X)\,d\mathbb{P}$	`⊢ ∀m h rv. fun_rv m h rv = expec m (λx. h (rv x))`
First moment	$\mu = E[X] = \int_{\mathcal{U}} X\,d\mathbb{P}$	`⊢ ∀m rv. first_moment m rv = expec m (λx. rv x)`
Second moment	$\mu_2 = E[X^2] = \int_{\mathcal{U}} X^2\,d\mathbb{P}$	`⊢ ∀m rv. second_moment m rv = expec m (λx. (rv x) pow 2)`
N-th moment	$\mu_N = E[X^N] = \int_{\mathcal{U}} X^N\,d\mathbb{P}$	`⊢ ∀m rv N. nth_moment m rv N = expec m (λx. (rv x) pow N)`
Variance	$\sigma^2 = E[(X-\mu)^2]$	`⊢ ∀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	$E[\lvert X-\mu\rvert]$	`⊢ ∀m rv. m_abs_dev m rv = expec m (λx. abs((rv x) - expec m rv))`

Coef. of skewness	$\alpha_3 = E[(\frac{X-\mu}{\sigma})^3]$	`⊢ ∀m rv. skew m rv = expec m (λx. ((rv x) - expec m rv) pow 3)`
		`/((std_dev m rv) pow 3)`

Coef. of kurtosis	$\alpha_4 = E[(\frac{X-\mu}{\sigma})^4]$	`⊢ ∀m rv. kurt m rv = expec m (λx. ((rv x) - expec m rv) pow 4)`
		`/((std_dev m rv) pow 4)`

4. Statistical properties of lifetime distributions

In this section, we present the formalization of the definitions of several important statistical properties of random variables in HOL. These statistical properties summarize some of the most important aspects of the probability distribution of a random variable. For example, the coefficient of skewness is a measure of symmetry of the probability distribution of a random variable. Other formalized definitions include the expectation of a function of a random variable, first, second and n-th moments, variance, standard deviation, mean absolute deviation, and coefficients of variation and kurtosis of a random variable, as summarized in Table 4. 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 second moment and variance relations for the bounded and unbounded random variables begins with the definition of the second moment given in the third row of Table 2. The function `second_moment` accepts a probability space, $(\mathcal{U}, \mathcal{E}, \mathbb{P})$, and a random variable `rv` that maps infinite Boolean sequences to real numbers.

It is important to note that by using Hurd's formalization of the probability space $(\mathcal{U}, \mathcal{E}, \mathbb{P})$, where $\mathcal{U}$ represents the universal set of all Boolean sequences, as outlined in [11], we utilize the above definition to reason about second moment of random variables formalized in [10,11].

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

Theorem 1 *(Second moment of bounded random variables).*

$$
\begin{aligned}
&\vdash \forall \mathtt{a}\ \mathtt{b}\ \mathtt{rv}.\ (0 \leqslant \mathtt{a}) \wedge (\mathtt{a} < \mathtt{b}) \wedge (\forall \mathtt{s}.\ \mathtt{a} \leqslant \mathtt{rv}\ \mathtt{s} \leqslant \mathtt{b}) \wedge \\
&\quad (\forall \mathtt{x}\ \mathtt{y}.\ \mathtt{x} < \mathtt{y} \Rightarrow \{\mathtt{s} \mid \mathtt{x} \leqslant \mathtt{rv}\ \mathtt{s} < \mathtt{y}\} \in \mathcal{E}) \Rightarrow \\
&\quad (\mathtt{second\_moment}\ (\mathcal{U}, \mathcal{E}, \mathbb{P})\ \mathtt{rv} = \\
&\quad \lim_{n \to \infty}[\textstyle\sum_{i=0}^{2^n-1}(a + \frac{i}{2^n}(b-a))^2 \mathbb{P}\{s \mid a + \frac{i}{2^n}(b-a) \leqslant \mathtt{rv}\ \ s < a + \frac{i+1}{2^n}(b-a)\}])
\end{aligned}
$$

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:

$$
\mathrm{rv_n(x)} = \sum_{i=0}^{2^n-1}\left(a + \frac{i}{2^n}(b-a)\right)\mathbb{I}_{\{s \mid a + \frac{i}{2^n}(b-a) \leqslant \mathrm{rv}\ s < a + \frac{i+1}{2^n}(b-a)\}}(x)
$$

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 [46] under the given assumptions.

The convergence of a positive measurable function to the Lebesgue integral property [46] and the Modus Ponens (MP) rule are then used to split the proof goal of Theorem 1 into the following seven subgoals. They correspond to the monotonicity and positive simple-function requirement on rv_n and five other assumptions described below [46]:

$$\mathtt{mono\_increasing}\left[\sum_{\mathtt{i}=0}^{2^{\mathtt{n}}-1}\left(\mathtt{a}+\frac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\right)^2 \mathbb{I}_{\{\mathtt{s}\mid \mathtt{a}+\frac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\leqslant \mathtt{rv\ s}<\mathtt{a}+\frac{\mathtt{i}+1}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\}}(\mathtt{x})\right] \tag{7}$$

$$\left(\forall \mathtt{i}.\left(\mathtt{i}<2^{\mathtt{n}}\right)\Rightarrow\left\{\mathtt{s}\;\middle|\;\mathtt{a}+\frac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\leqslant \mathtt{rv\ s}<\mathtt{a}+\frac{\mathtt{i}+1}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\right\}\in\mathcal{E}\right) \tag{8}$$

$$\left(\forall \mathtt{i}.0\leqslant \mathtt{a}+\frac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\right) \tag{9}$$

$$\left(\mathtt{FINITE}\left\{\mathtt{i}\;\middle|\;\mathtt{i}<2^{\mathtt{n}}\right\}\right) \tag{10}$$

$$\left[\sum_{\mathtt{i}=0}^{2^{\mathtt{n}}-1}\left(\mathtt{a}+\frac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\right)^2 \mathbb{I}_{\{\mathtt{s}\mid \mathtt{a}+\frac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\leqslant \mathtt{rv\ s}<\mathtt{a}+\frac{\mathtt{i}+1}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\}}(\mathtt{x})\right]\leqslant \mathtt{rv}(\mathtt{x}) \tag{11}$$

$$\lim_{\mathtt{n}\to\infty}\left[\sum_{\mathtt{i}=0}^{2^{\mathtt{n}}-1}\left(\mathtt{a}+\frac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\right)^2 \mathbb{I}_{\{\mathtt{s}\mid \mathtt{a}+\frac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\leqslant \mathtt{rv\ s}<\mathtt{a}+\frac{\mathtt{i}+1}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\}}(\mathtt{x})\right]=\mathtt{rv}(\mathtt{x}) \tag{12}$$

$$\exists \mathtt{y}.\lim_{\mathtt{n}\to\infty}\left[\sum_{\mathtt{i}=0}^{2^{\mathtt{n}}-1}\left(\mathtt{a}+\frac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\right)^2 \mathbb{P}\left\{\mathtt{s}\;\middle|\;\mathtt{a}+\frac{\mathtt{i}}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\leqslant \mathtt{rvs}<\mathtt{a}+\frac{\mathtt{i}+1}{2^{\mathtt{n}}}(\mathtt{b}-\mathtt{a})\right\}\right]=\mathtt{y} \tag{13}$$

The monotonically increasing property in the first subgoal (Eq. (7)) 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 (Eqs. (8), (9) and (10)) 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 1, arithmetic reasoning and set theory principles, respectively. The fifth subgoal (Eq. (11)) 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 (Eq. (12)) 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 (Eq. (13)) 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 1.

The verification of the second moment relation for an unbounded continuous random variable, given in [14] is as follows:

Theorem 2 *(Second moment of an unbounded random variable).*

$$\vdash \forall \mathtt{rv.}\ \ (\forall \mathtt{s.}\ \ 0\ \leqslant\ \mathtt{rv\ \ s})\ \wedge\ (\forall \mathtt{x.}\ \ \{\mathtt{s}\ \mid\ \mathtt{rv\ \ s}\ \geqslant\ \mathtt{x}\}\ \in\ \mathcal{E})$$
$$(\forall \mathtt{x\ \ y.}\ \ \mathtt{x}\ <\ \mathtt{y}\ \Rightarrow\ \{\mathtt{s}\ \mid\ \mathtt{x}\ \leqslant\ \mathtt{rv\ \ s}\ <\ \mathtt{y}\}\ \in\ \mathcal{E})\ \Rightarrow$$
$$(\mathtt{second\_moment}\ \ (\mathcal{U},\mathcal{E},\mathbb{P})\ \ \mathtt{rv}\ =$$
$$\lim_{\mathtt{n}\to\infty}[\textstyle\sum_{\mathtt{i}=0}^{\mathtt{n}2^{\mathtt{n}}-1}(\frac{\mathtt{i}}{2^{\mathtt{n}}})^2\mathbb{P}\{\mathtt{s}\mid\frac{\mathtt{i}}{2^{\mathtt{n}}}\leqslant\mathtt{rv\ \ s}<\frac{\mathtt{i}+1}{2^{\mathtt{n}}}\}+\mathtt{n}\mathbb{P}\{\mathtt{s}\mid\mathtt{rv\ \ s}\geqslant\mathtt{n}\}])$$

As in Theorem 1, the function `second_moment` accepts a probability space, $(\mathcal{U},\mathcal{E},\mathbb{P})$, and a random variable rv that maps infinite Boolean sequences to real numbers [11]. A detailed description of the proof can be found in [14].

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, etc. This allows us to formally reason about the statistical properties of random variables commonly used in reliability analysis while at the same time gain the benefits of the original Lebesgue based definition.

5. Moments and variance of lifetime distributions

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. On the other hand, statistical properties such as the variance, which is also known as the second central moment, is a measure of dispersion of the lifetime distribution of a system. Similarly standard deviation is another measure of dispersion of the distribution. Both variance and standard deviation depend on the scale of the measurement. The coefficient of variation, defined as the ratio standard deviation and the expectation of a random variable, which is a dimensionless number, is thus some times used to overcome this scale problem. The coefficient of skewness is a measure of the skewness and the coefficient of kurtosis is a measure of peakedness of the lifetime distribution of a system [4].

Our formalization of the statistical properties of several continuous random variables including the Exponential random variable allows us to verify these important statistical properties of the life time distribution of electronic system components.

We now utilize the two second moment theorems (Theorems 1 and 2) for the verification of the statistical properties of the Uniform, the Triangular and the Exponential random variables.

5.1. Uniform random variable

Uniform distribution is a simple two parameter distribution and is mainly used in reliability analysis for modeling the life time of a system over relatively short intervals of time. Its parameters are a and b, where $a \leqslant x < b$. It is also used in the formalization of random variables using methods such as the inverse transform method and the acceptance–rejection method [49]. The second moment for the continuous Uniform random variable bounded in the interval $[a, b]$ is formalized as follows:

Theorem 3 *(Second moment of the Uniform(a, b) random variable).*

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

We start the proof process by rewriting the left hand side of the proof goal of Theorem 3 using the general second moment theorem for bounded random variables (Theorem 1).

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

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

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

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

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

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.

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

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

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

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

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

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

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

Theorem 4 *(Variance of the Uniform(a, b) random variable).*

$$\vdash \forall \mathtt{a}\ \mathtt{b}.\ (0 \leqslant \mathtt{a}) \wedge (\mathtt{a} < \mathtt{b}) \Rightarrow (\mathtt{variance}\ (\mathcal{U}, \mathcal{E}, \mathbb{P})\ (\mathtt{uniform\_rv}\ \mathtt{a}\ \mathtt{b}) = \tfrac{(\mathtt{b}-\mathtt{a})^2}{12})$$

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 [12] and the second moment of the Uniform random variable (Theorem 3). This reduced the left hand side to:

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

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

5.2. Triangular random variable

In reliability theory, Triangle distribution is found to be very useful in cases where there is limited amount of information available regarding the relationship between various factors that affect the life time of a system. For example, if only the most likely, minimum and maximum lifetimes estimates are available, the parameter of the Triangle distribution can then be used to model the lifetime behavior of the system [51].

The second moment for the continuous Triangular random variable bounded in the interval $[0, b]$ is formalized as follows:

Theorem 5 *(Second moment of the Triangular(b) random variable).*

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

The proof process begins rewriting the left hand side using the second moment theorem for bounded random variables (Theorem 1).

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

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

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

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

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

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.

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

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

$$\lim_{n\to\infty}\sum_{i=0}^{2^n-1}(-2\mathtt{i}\mathtt{b}^2)\frac{\mathtt{i}^3}{2^{4n}} = \frac{-\mathtt{b}^2}{2}, \qquad \lim_{n\to\infty}\sum_{i=0}^{2^n-1}(-\mathtt{b}^2)\frac{\mathtt{i}^2}{2^{4n}} = 0, \quad \text{and}$$

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

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 6 *(Variance of the Triangular*(b) *random variable).*

$$\vdash \forall \mathtt{b}.\ (0 < \mathtt{b}) \Rightarrow (\mathtt{variance}\ (\mathcal{U}, \mathcal{E}, \mathbb{P})\ (\mathtt{triangular\_rv}\ \mathtt{b}) = \tfrac{\mathtt{b}^2}{18})$$

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:

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

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.

5.3. Exponential random variable

In this section, we utilize Theorem 2 for the verification of the second moment and variance properties of the Exponential random variable. The second moment for the continuous Exponential random variable, is formalized as follows:

Theorem 7 *(Second moment of the Exponential*(m) *random variable).*

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

We start the proof process by rewriting the left hand side using the general second moment theorem for the unbounded random variables (Theorem 2).

$$\lim_{n\to\infty} \sum_{i=0}^{n2^n-1} \left(\frac{i}{2^n}\right)^2 \mathbb{P}\left\{s \,\middle|\, \frac{i}{2^n} \leqslant (\mathrm{exp\_rv}\, m)\ s < \frac{i+1}{2^n}\right\} + \mathbb{P}\{s \mid n \leqslant (\mathrm{exp\_rv}\, m)\ s\} = \frac{2}{m^2}$$

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

$$\mathbb{P}\left\{s \,\middle|\, \frac{i}{2^n} \leqslant (\mathrm{exp\_rv}\, m)\ s < \frac{i+1}{2^n}\right\} + n\mathbb{P}\{s \mid n \leqslant (\mathrm{exp\_rv}\, m)\ s\} = \left[\left(e^{-m\frac{i}{2^n}}\right)\left(1 - e^{-\frac{m}{2^n}}\right) + ne^{-mn}\right]$$

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

$$\lim_{n\to\infty} \left[\sum_{i=0}^{n2^n-1} \left(\frac{i}{2^n}\right)^2 \left(e^{-m\frac{i}{2^n}}\right)\left(1 - e^{-\frac{m}{2^n}}\right) + ne^{-mn}\right] = \frac{2}{m^2}$$

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

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

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

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

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

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

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.

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

Then we specialize the above two results for the case when $x=\frac{1}{2^n}$ and show that

$$\lim_{n\to\infty}\left[\frac{e^{\frac{-m}{2^n}}}{2^n(1-e^{\frac{-m}{2^n}})}\right]=\frac{1}{m}\quad\text{and}\quad \lim_{n\to\infty}\left[\frac{1}{2^n(1-e^{\frac{-m}{2^n}})}\right]=\frac{1}{m}$$

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

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

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

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 8 *(Variance of the Exponential(m) random variable).*

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

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.

6. Reliability theory formalization

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.

6.1. 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 1 *(Survival function).*

```
⊢ ∀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 → bool) → real) → real → real).

Theorem 9 *(Survival function, Exponential(m) random variable).*

$$\vdash \forall \texttt{m t}.\ (0 < \texttt{m}) \wedge (0 \leqslant \texttt{t}) \Rightarrow (\texttt{survival\_function}\ (\lambda \texttt{s. exp\_rv m s})\ \texttt{t} = e^{-\texttt{mt}})$$

Theorem 9 was verified using the definitions of survival function and CDF of 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 9, we can now formally reason about probabilities of failure events at any time t i.e., $\mathtt{P}\{T \leqslant t\}$, or between any two times t_1 and t_2, i.e., $\mathtt{P}\{t_1 \leqslant T \leqslant t_2\}$.

Besides Theorem 9, we also formally verified three important existence properties of the survival function in HOL:

Property 1. Survival function at time 0 is equal to 1

```
⊢ ∀rv. (∀x. CDF_in_events_bern rv x) ⇒ (survival_function rv 0 = 1)
```

Here the assumption of Property 1 ensures that events of the type $\{s \mid rv\ s \leqslant x\}$, which define the CDF, are in the sample space.

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

Property 2. Survival function approaches 0 for very large values of times

```
⊢ ∀rv. (∀x. CDF_in_events_bern rv x) ⇒ (λn. survival_function rv &n ) → 0
```

The proof of Property 2 involved rewriting with the definition of survival function, real analysis and CDF properties of the random variable rv.

Property 3. Survival function is a non-increasing function

```
⊢ ∀rv a b. (a < b) ∧ (∀x. CDF_in_events_bern rv x) ⇒
   (survival_function rv b ⩽ survival_function rv a)
```

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

6.2. 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 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. Using Definition 2, we formally verified the following important property of the hazard function in HOL.

Property 4. 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 (Property 3).

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 (Table 6). 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 10.

Theorem 10 *(Hazard function, Exponential(m) random variable).*

```
⊢ ∀m t. (0 < m) ∧ (0 ⩽ t) ⇒ (hazard_function (λs. exp_rv m s) t = m)
```

Table 5
Formally verified survival function relations for commonly used life time distributions.

Distribution	Survival function, $S(t)$
Uniform	⊢ ∀a b t. (0 ⩽ a) ∧ (a < b) ∧ (0 ⩽ t) ⇒ survival_function (λs. uniform_rv a b s) t = $(\frac{b-t}{b-a})$
Triangular	⊢ ∀b t. (0 < b) ∧ (0 ⩽ t) ⇒ survival_function (λs. triangle_rv b s) t = $1-\frac{2}{b}(t-\frac{t^2}{2b})$
Exponential	⊢ ∀m t. (0 < m) ∧ (0 ⩽ t) ⇒ survival_function (λs. exp_rv m s) t = e^{-mt}
Weibull	⊢ ∀a m t. (0 < a) ∧ (0 < m) ∧ (0 ⩽ t) ⇒ survival_function (λs. weibull_rv a m s) t = $e^{-(mt)^a}$

Table 6
Formally verified hazard function relations for commonly used life time distributions.

Distribution	Hazard function, $h(t)$
Uniform	⊢ ∀a b t. (0 ⩽ a) ∧ (a < b) ∧ (0 ⩽ t) ⇒ hazard_function (λs. uniform_rv a b s) t = $\frac{1}{b-t}$
Triangular	⊢ ∀b t. (0 < b) ∧ (0 ⩽ t) ⇒ 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	⊢ ∀m t. (0 < m) ∧ (0 ⩽ t) ⇒ hazard_function (λs. exp_rv m s) t = m
Weibull	⊢ ∀a b t. (0 < a) ∧ (0 < m) ∧ (0 ⩽ t) ⇒ hazard_function (λs. weibull_rv a m s) t = $am^a t^{a-1}$

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 10, we can now formally reason about the amount of failure risks 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 6 summarizes the hazard function relations for the Uniform, Triangle, Exponential, and Weibull random variables.

6.3. *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:

$$H_X(t) = \int_0^t h_X(\tau)\, d\tau \tag{14}$$

Its HOL formalization is given in Definition 3:

Definition 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) the accumulated hazard function at time zero is zero, which is mathematically expressed as:

$$H_X(0) = 0 \tag{15}$$

HOL formalization of this property is given in Property 5.

Property 5. 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 Property 5 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 3.

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

$$0 \leqslant H_X(t) \tag{16}$$

the HOL formalization is given in Property 6.

Table 7
Formally verified cumulative hazard function relations for commonly used life time distributions.

Distribution	Cumulative hazard function, $H(t)$
Uniform	⊢ ∀a b t. (0 ⩽ a) ∧ (a < b) ∧ (0 ⩽ t) ⇒ cumu_haz_function (λs. uniform_rv a b s) t = ln($\frac{b-a}{b-t}$)
Triangular	⊢ ∀b t. (0 < b) ∧ (0 ⩽ t) ⇒ cumu_haz_function (λs. triangle_rv b s) t = 2ln($\frac{b}{b-t}$)
Exponential	⊢ ∀m t. (0 < m) ∧ (0 ⩽ t) ⇒ cumu_haz_function (λs. exp_rv m s) t = mt
Weibull	⊢ ∀a m t. (0 < a) ∧ (0 < m) ∧ (0 ⩽ t) ⇒ cumu_haz_function (λs. weibull_rv a m s) t = $(\mathtt{m\ t})^{a}$

Property 6. 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 Property 6 involved rewriting with the definition of accumulated function and Properties 4 and 5.

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

$$t_1 \leqslant t_2 \Rightarrow H_X(t_1) \leqslant H_X(t_2) \tag{17}$$

The HOL formalization of this property is given in Property 7.

Property 7. 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 Property 7 involved reasoning from Properties 5 and 6, and the fact that for $t_1 \leqslant t_2$ 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 have 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 [52,16].

Table 7 summarizes the cumulative hazard function relations that we formally verified using Definition 3 and Properties 5, 6 and 7.

6.4. *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 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 *(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 8 lists the p-th fractile functions that we formally verified in HOL for the Uniform, Triangle, Exponential, and Weibull random variables.

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

Table 8
Formally verified p-th fractile relations for commonly used life time distributions.

Distribution	p-th fractile
Uniform	$\vdash \forall$a b p t. (0 $\leqslant$ 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 + $\sqrt{1-\mathrm{p}^2}$)
Exponential	$\vdash \forall$m p t. (0 $<$ m) $\wedge$ (0 $<$ p) $\wedge$ (p $<$ 1) $\Rightarrow$ fractile (λs. exp_rv m s) p = $-\frac{1}{\mathrm{m}}\ln(1-\mathrm{p})$
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 = $\frac{1}{\mathrm{m}}(-\ln(1-\mathrm{p}))^{\frac{1}{\mathrm{a}}}$

The lifetime distributions can be defined in other ways, including the Mellin transform [53], the moment generating function [54], the probability density function [4], or the mean residual life function [4]. Formalization of these concepts is possible using our proposed approach and the existing theories used in the HOL theorem prover and the ones we have developed and described in this paper and in our previous work [14,12]. We plan to work on these formalizations in the future to enhance the proposed approach into a complete framework that can then be utilized for accurate formal analysis of reliability problems in engineering, biostatistics and other applied sciences.

7. Reliability analysis examples

7.1. Reliability analysis of a capacitor

Capacitors are essential component of many electrical systems ranging from basic electronics used in medical devices to avionics used in space shuttles. Uninterruptable power supplies and inverters commonly used in renewable energy power systems contain capacitors for filtering and smoothing 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 the correct behavior of electronics used in critical safety systems and in the 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 memoryless 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 [4]. 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. Environmental and qualitative 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 6 gives the base failure rate for a capacitor [20].

Definition 6 *(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 [20]), 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 [20]). 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 the second argument of the function (i.e., real_pow A b $= \mathrm{A}^{\mathrm{b}}$). 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 environmental and qualitative 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 stress for an electronic component arises from the environment in which it operates, including its operating temperature, applied voltage, current and power levels.

The two factors are given in [20] and are formalized in HOL as follows.

Definition 7 *(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 8 *(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 = 5 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 9.

Definition 9 *(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)
```

7.1.1. Capacitor lifetime model

The lifetime of a capacitor 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 10 *(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)
```

7.1.2. Verification of reliability properties

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

7.1.2.1. Survival and hazard functions: Theorems 11 and 12 formally prove the survival and hazard function properties of the capacitor.

Theorem 11 *(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 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 12 *(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 7 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.

7.1.2.2. Statistical properties: We formally verified several statistical properties of the capacitor's lifetime using the proposed reliability analysis method in the HOL theorem prover; three of these are presented below, namely, the mean, the second moment, and the variance of Time-to-Failure of the capacitor.

Theorem 13 *(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 14 *(Second moment of Time-to-Failure, 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) ⇒
    second_moment (𝒰,ℰ,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
```

Similarly other statistical properties such as the coefficient of variance, standard deviation and reliability properties such as the cumulative hazard function and p-th fractiles can be formally verified for electronic system components.

Theorem 15 *(Variance of Time-to-Failure, 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) ⇒
    variance (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)^2
```

The proofs of the above statistical properties were greatly facilitated by the statistical properties of the Exponential random variables, described in Section 4.

In the next section, we present modeling and verification of the end-of-life time of cables used in electrical power systems.

7.2. Reliability analysis of insulated cables

Insulated cables are an important component of electrical power systems that operate in harsh environments and are frequently subjected to one or more types of stresses throughout 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's insulation. All of these stresses progressively deteriorate the ability of the cable's 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 [55,56].

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 [57]. Modeling based on formal methods 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 [57,58]. 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 the Weibull distribution described by the following equation:

$$P\{X \leqslant t\} = F_X(t) = 1 - e^{-(mt)^a} = 1 - S_x(t) \tag{18}$$

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:

$$m = \frac{sinh(\frac{\epsilon_0 \epsilon_r \Delta V E^2}{2kT})}{\frac{h}{2\pi f kT} e^{\frac{\Delta G}{kT}}} \tag{19}$$

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 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:

$$\Delta G = \Delta H - T \Delta S \tag{20}$$

In [57] 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 general expressions for the probability that the cable insulation will fail at a time t. We also verify the instantaneous and accumulated risk associated with the useful lifetime of the cable.

The HOL formalization of the scale parameter or factor m for the Weibull distribution is given in Definition 11.

Definition 11 *(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 11. Our formalization of hyperbolic functions includes the 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 ($cosh^2(x) - sinh^2(x) = 1$) and so forth. 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 the HOL theorem prover; details of the hyperbolic function theory can be found elsewhere [59].

7.2.1. *Cable insulation lifetime model*

The higher-order-logic life time model of an insulated cable is given in Definition 12. 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 12 *(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)
```

7.2.1.1. Verification of reliability properties: Theorems 16, 17, 18, and 19 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 16.

Theorem 16 *(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 the 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 [4].

The amount of failure risk associated with the insulated cable at any time *t* is verified in Theorem 17.

Theorem 17 *(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 general parameters in this theorem completely describe the failure risk associated with the insulated cable as a function of time. The shape of the hazard function gives an indication of how the insulated cable ages. A larger value of hazard function means that the insulated cable is under greater risk of failure and a smaller value of this function indicates that the insulated cable is under less risk. The shape of this function can be an increasing, constant, decreasing or bath-tub shaped, representing different aging types and lifetime failure behaviors. With proper selection of the insulated cable parameters and the Weibull distribution parameters, an increasing, a constant, a decreasing or a bath-tub shaped hazard function can be modeled.

The total amount of failure risk up to time *t* associated with the insulated cable is verified in Theorem 18.

Theorem 18 *(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 19. A special case of this property, when $p = 0.5$, is referred to as the median lifetime of the insulated cable.

Theorem 19 *(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, 6, 7 and 8. 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 an 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.

8. Conclusions

In this paper, 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. 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 formalizations of several important statistical properties of random variables and the formal proof of general expressions for the second moment of bounded and unbounded continuous random variable using probability, measure and Lebesgue integration theories. We then used these expressions to prove the second moment and the variance relations for the Uniform, the Triangular, and the Exponential random variables. The usefulness of the proposed reliability analysis method was demonstrated with the help of two examples. The first example dealt with the reliability analysis of a capacitor, an essential building block in electrical and electronic systems. In the second example, we modeled the lifetime behavior of insulated power transmission cables using Weibull random variables and formally verified the survival properties including risks associated throughout the useful life of the insulated cables. The HOL formalization and proof effort described in this paper took approximately 250 man-hours and consists of around 6000 lines of HOL code.

The work presented in this paper 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 and 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.

We are currently working on the formalization of other lifetime probability distributions such as Gamma and Gaussian distributions to further enhance the proposed reliability analysis approach. As a first step we are formalizing and verifying methods such as the acceptance–rejection method. This will allow us to formally verify an even larger class of random variables in the HOL theorem prover. One of the objectives of our research is to enhance the proposed approach through formalization of other random variables and lifetime distribution representations so that a complete framework for reliability analysis can be developed and be capable of handling engineering reliability analysis problems in an intuitive and systematic manner. This presents our first significant contribution in this direction.

References

[1] E. Broughton, The Bhopal disaster and its aftermath: a review, Environ. Health 4 (6) (2005) 1–6, http://dx.doi.org/10.1186/1476-069X-4-6.

[2] Rogers Commission report, Report of the Presidential Commission on the Space Shuttle Challenger Accident, vol. 1, Chapter 4, p. 72; http://history.nasa.gov/rogersrep/v1ch4.htm, 1986.

[3] Investigative documentary on National Geographic Channel, Derailment at Eschede (High Speed Train Wreck), Seconds From Disaster, 2007.

[4] L.M. Leemis, Reliability: Probabilistic Models and Statistical Methods, Ascended Ideas, 2009.

[5] B. Cipra, How number theory got the best of the pentium chip, Science (N. S.) 267 (5195) (1995) 175.

[6] Radim Bris, Exact reliability quantification of highly reliable systems with maintenance, Reliab. Eng. Syst. Saf. 95 (12) (2010) 1286–1292.

[7] Mathworks Inc., Matlab, 2011.

[8] D. Kotz, C. Newport, R.S. Gray, J. Liu, Y. Yuan, C. Elliott, Experimental evaluation of wireless simulation assumptions, in: Proceedings of the ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, 2004, pp. 78–82.

[9] D. Cavin, Y. Sasson, A. Schiper, On the accuracy of manet simulators, in: Proceedings of the ACM International Workshop on Principles of Mobile Computing, 2002, pp. 38–43.

[10] J. Hurd, Formal verification of probabilistic algorithms, PhD thesis, University of Cambridge, Cambridge, UK, 2002.

[11] O. Hasan, Formal probabilistic analysis using theorem proving, PhD thesis, Concordia University, Montreal, QC, Canada, 2008.

[12] O. Hasan, N. Abbasi, B. Akbarpour, S. Tahar, R. Akbarpour, Formal reasoning about expectation properties for continuous random variables, in: Formal Methods, in: Lecture Notes in Comput. Sci., vol. 5850, 2009, pp. 435–450.

[13] O. Hasan, S. Tahar, N. Abbasi, Formal reliability analysis using theorem proving, IEEE Trans. Comput. 59 (5) (2010) 579–592.

[14] N. Abbasi, O. Hasan, S. Tahar, Formal lifetime reliability analysis using continuous random variables, in: Logic, Language, Information and Computation, in: Lecture Notes in Comput. Sci., vol. 6188, Springer, 2010, pp. 84–97.

[15] A.M. Johnson, M. Malek, Survey of software tools for evaluating reliability availability and suviceability, ACM Comput. Surv. 20 (4) (1998) 227–269.

[16] M.J.C. Gordon, T.F. Melham, Introduction to HOL: A Theorem Proving Environment for Higher-Order Logic, Cambridge University Press, 1993.

[17] T. Kropf, Introduction to Formal Hardware Verification, Springer, 1999.

[18] S. Dean, Considerations involved in making system investments for improved service reliability, EEI Bulletin 6 (1938) 491–496.

[19] R.H. Myers, L.W. Ball, Reliability Engineering for Electronic Systems, J. Wiley, 1964.

[20] US Department of Defence, Reliability prediction of electronic equipment, Military handbook, MIL-HDBK-217B, 1974.

[21] US Department of Defense, Reliability-Centered Maintenance (RCM) requirements for naval aircraft, weapon systems, and support equipment, MIL-HDBK-2173, 1998.

[22] FIDES, Reliability Methodology for Electronic Systems, 2009.

[23] Institute of Electrical and Electronics Engineers, IEEE standard reliability program for the development and production of electronic systems and equipment, IEEE 1332 (1998).

[24] J.J. Stiffler, L.A. Bryant, L. Guccione, CARE III final report phase I, vols. I and II, Technical Report NASA Contractor Rep. 159122 and 159123, SRI International, November 1979.

[25] P.M. Nagel, Software reliability: Repetitive run experimentation and modeling, Technical Report NASA CR-165836, Boeing Computer Services Co., 1982.

[26] A. Costes, J.E. Doucet, C. Landrault, J.C. Laprie, SURF: A program for dependability evaluation of complex fault-tolerant computing systems, in: Digest of the IEEE Annual Symposium on Fault-Tolerant Computing, 1981, pp. 72–78.

[27] D.F. Frost, K.F. Poole, D.A. Haeussler, RELIANT: A reliability analysis tool for VLSI interconnects, in: Proceedings of the IEEE Custom Integrated Circuits Conference, 1998, pp. 27.8/1–27.8/4.

[28] S.M. Alam, G.C. Lip, C.V. Thompson, D.E. Troxel, Circuit level reliability analysis of Cu interconnects, in: Proceedings of the International Symposium on Quality Electronic Design, 2004, pp. 238–243.

[29] Y. Chery, S. Hau-Riege, S. Alam, D.E. Troxel, C.V. Thompson, A tool for technology-generic circuit-level reliability projections, in: Interconnect Focus Center Annual Review, 1999.

[30] J.H. Lala, Mark1 - Markov Modeling Package, The Charles Stark Draper Laboratory, Cambridge, MA, 1983.

[31] W.H. Sanders, J.F. Meyer, METASAN: A performability evaluation tool based on stochastic activity networks, in: Proceedings of the Fall Joint Computer Conference, 1986, pp. 807–816.

[32] A. Goyal, W.C. Carter, D.E. Silva, E. Lavenberg, K.S. Trivedi, The system availability estimator, in: Digest of the IEEE Annual Symposium on Fault-Tolerant Computing, 1986, pp. 84–89.

[33] R.H. Tu, E. Rosenbaum, W.Y. Chan, C.C. Li, E. Minami, K. Quader, P.K. Ko, C. Hu, Berkeley reliability tools-bert, IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 12 (10) (1993) 1524–1534.

[34] M. Leucker, C. Schallhart, A brief account of runtime verification, J. Log. Algebr. Program. 78 (5) (2009) 293–303.

[35] E. Clarke, O. Grumberg, D. Peled, Model Checking, MIT Press, 2000.

[36] S. Donatelli, J. Sproston, CSL model checking for the GreatSPN tool, in: Computer and Information Sciences, in: Lecture Notes in Comput. Sci., vol. 3280, Springer, 2004, pp. 543–552.

[37] J. Hillston, A Compositional Approach to Performance Modelling, Cambridge University Press, New York, NY, USA, 1996.

[38] H. Hansson, B. Jonsson, A logic for reasoning about time and reliability, Form. Asp. Comput. 6 (1994) 102–111.

[39] C. Baier, B.R. Haverkort, H. Hermanns, J.-P. Katoen, Model-checking algorithms for continuous-time Markov chains, IEEE Trans. Softw. Eng. 29 (6) (2003) 524–541.

[40] J. Hurd, A. McIver, C. Morgan, Probabilistic guarded commands mechanized in HOL, in: Proceedings of the Workshop on Quantitative Aspects of Programming Languages, Electron. Notes Theor. Comput. Sci. 112 (2005) 95–111.

[41] M. Duflot, M. Kwiatkowska, G. Norman, D. Parker, S. Peyronnet, C. Picaronny, J. Sproston, Practical applications of probabilistic model checking to communication protocols, in: FMICS Handbook on Industrial Critical Systems, IEEE Computer Society Press, 2010.

[42] P. Lecca, C. Priami, Cell cycle control in eukaryotes: a biospi model, in: Proceedings of the Workshop on Concurrent Models in Molecular Biology, Electron. Notes Theor. Comput. Sci. 180 (3) (2007) 51–63.

[43] C. Baier, B. Haverkort, H. Hermanns, J. Katoen, Model checking algorithms for continuous time Markov chains, IEEE Trans. Softw. Eng. 29 (4) (2003) 524–541.

[44] J. Rutten, M. Kwiatkowska, G. Norman, D. Parker, Mathematical Techniques for Analyzing Concurrent and Probabilisitc Systems, CRM Monogr. Ser., vol. 23, American Mathematical Society, 2004.

[45] M. Kwiatkowska, G. Norman, D. Parker, Quantitative analysis with the probabilistic model checker PRISM, Electron. Notes Theor. Comput. Sci. 153 (2) (2005) 5–31.

[46] A. Coble, Anonymity, information and machine-assisted proof, PhD thesis, University of Cambridge, Cambridge, UK, 2009.

[47] T. Mhamdi, O. Hasan, S. Tahar, On the formalization of the Lebesgue integration theory in HOL, in: Interactive Theorem Proving, in: Lecture Notes in Comput. Sci., vol. 6172, Springer, 2010, pp. 387–402.

[48] J. Galambos, Advanced Probability Theory, Marcel Dekker, 1995.

[49] A. Papouli, S.U. Pillai, Probability, Random Variables and Stochastic Processes, McGraw–Hill, 2002.
[50] O. Hasan, S. Tahar, Formalization of the continuous probability distributions, in: Automated Deduction, in: Lecture Notes in Comput. Sci., vol. 4603, Springer, 2007, pp. 3–18.
[51] M. Evans, N. Hastings, B. Peacock, Triangular distribution, in: Statistical Distributions, Wiley, New York, NY, USA, 2000, pp. 187–188, Chapter 40.
[52] J. Harrison, Theorem Proving with the Real Numbers, Springer, 1998.
[53] P.G. Moschopoulos, A general procedure for deriving distributions, Commun. Statist. Theoret. Meth. 12 (17) (1983) 2005–2015.
[54] R.E. Hogg, J.W. McKean, A.T. Craig, Introduction to Mathematical Statistics, Prentice Hall, Englewood Cliffs, NJ, 2005.
[55] G. Montanari, L. Simoni, Aging phenomenology and modeling, IEEE Trans. Electr. Insul. 28 (5) (1993) 755–776.
[56] L. Simoni, Fundamentals of Endurance of Electrical Insulating Materials, CLUEB, Bologna, Italy, 1983.
[57] P. Vovos, Economic system operation considering the cost of wear of cables, IEEE Trans. Power Syst. 26 (2) (2011) 642–652.
[58] J.P. Crine, J.L. Parpal, G. Lessard, A model of aging of dielectric extruded cables, in: Proceedings of the International Conference on Conduction and Breakdown in Solid Dielectrics, 1989, pp. 347–351.
[59] N. Abbasi, O. Hasan, S. Tahar, Formalization of Weibull random variable in HOL, Technical report, Department of Electrical and Computer Engineering, Concordia University, Montreal, QC, Canada, October 2010.