Formalization of Laplace Transform Using the Multivariable Calculus Theory of HOL-Light

Syeda Hira Taqdees and Osman Hasan

School of Electrical Engineering and Computer Science (SEECS),
National University of Sciences and Technology (NUST),
Islamabad, Pakistan
{11mseestaqdees,osman.hasan}@seecs.nust.edu.pk

Abstract. Algebraic techniques based on Laplace transform are widely used for solving differential equations and evaluating transfer of signals while analyzing physical aspects of many safety-critical systems. To facilitate formal analysis of these systems, we present the formalization of Laplace transform using the multivariable calculus theories of HOL-Light. In particular, we use integral, differential, transcendental and topological theories of multivariable calculus to formally define Laplace transform in higher-order logic and reason about the correctness of Laplace transform properties, such as existence, linearity, frequency shifting and differentiation and integration in time domain. In order to demonstrate the practical effectiveness of this formalization, we use it to formally verify the transfer function of Linear Transfer Converter (LTC) circuit, which is a commonly used electrical circuit.

1 Introduction

Laplace transform [12] is an integral transform method that is used to convert the time varying functions to their corresponding s-domain representations, where s represents the angular frequency [1]. This transformation provides a very compact representation of the overall behavior of the given time varying function and is frequently used for analyzing systems that exhibit a deterministic relationship between continuously changing quantities and their rates of change. Laplace transform theory allows us to solve linear Ordinary Differential Equations (ODEs) [19] using simple algebraic techniques since the transformation allows us to convert the integration and differentiation functions from the time-domain to multiplication and division functions in the s-domain. Moreover, the s-domain representations of ODEs are also used for transfer function analysis of the corresponding systems. Due to these unique features, Laplace transform theory has been an integral part of engineering and physical system analysis and is widely used in the design and analysis of electrical networks, control systems, communication systems, optical systems, analogue filters and mechanical networks.

K. McMillan, A. Middeldorp, and A. Voronkov (Eds.): LPAR-19, LNCS 8312, pp. 744–758, 2013.

Mathematically, Laplace transform is a complex function defined for a function f, which can be either real or complex-valued, as follows

$$F(s) = \int_0^\infty f(t)e^{-st}dt,\ s \in \mathbb{C} \tag{1}$$

The first step in analyzing differential equations using Laplace transform is to take the Laplace transform of the given equation on both sides. Next, the corresponding s-domain equation is simplified using various properties of Laplace transform, such as existence, linearity, Laplace of a differential and Laplace of an integral. The objective is to either solve the differential equation to obtain values for the variable s or obtain the transfer function of the system corresponding to the given differential equation.

Traditionally, the above mentioned Laplace transform based analysis is performed using computer based numerical techniques or symbolic methods. However, both of these techniques cannot guarantee accurate analysis. Numerical methods cannot ascertain an accurate value of the improper integral of Equation (1) as there is always a limited number of iterations allowed depending on the available memory and computation resources. The round-off errors due to the usage of computer arithmetics also introduce some inaccuracies in the results. Symbolic methods, provided by Symbolic Math Toolbox of Matlab and other computer algebra systems like Maple and Mathematica, are based on algorithms that consider the improper integral of Equation (1) as the continuous analog of the power series, i.e., the integral is discretized to summation and the complex exponentials are sampled. Moreover, the presence of huge symbolic manipulation algorithms, which are usually unverified, in the core of computer algebra systems also makes the accuracy of their analysis results questionable. For-instance, a couple of examples for using Matlab or Maple for control and electrical engineering systems can be found in [3,16]. However, the results of these analyses cannot be termed as 100% accurate. Therefore, these traditional techniques should not be relied upon for the analysis of systems using the Laplace transform method, especially when they are used in safety-critical areas, such as medicine and transportation, where inaccuracies in the analysis could result in system design bugs that in turn may even lead to the loss of human lives in worst cases.

To overcome the above mentioned inaccuracy limitations, we propose to perform the Laplace transform based analysis using a higher-order-logic theorem prover. The main idea is to leverage upon the high expressiveness of higher-order logic to formalize Equation (1) and use it to verify the classical properties of Laplace transform within a theorem prover. These foundations can be built upon to reason about the exact solution of a differential equation or its transfer function within the sound core of a theorem prover. In particular, the paper presents the formal verification of existence, linearity and scaling properties of Laplace transform. It also presents the formal verification of the Laplace transforms of an arbitrary order differential and integral functions. The main advantage of these results is that they greatly minimize the user intervention for formal reasoning about the correctness of many properties of physical systems. In order to illustrate the practical effectiveness and utilization of this formalization, we use it to verify the transfer function of a Linear Transfer Converter (LTC) circuit, which is commonly used analog circuit. Formal verification of analog circuits is of utmost importance [8]. However, to the best of our knowledge, all the existing formal verification approaches work with abstracted discretized models of analog circuits (e.g., [4],[2]). This is mainly because of the inability to model and analyze the properties of differential equations in their true continuous form by the existing formal methods. The formalization of Laplace transform, presented in this paper, overcomes this limitation and we have been able to formally verify the transfer function of the LTC circuit using its differential equation.

The work described in this paper is done using the HOL-Light theorem prover [6], which supports formal reasoning about higher-order logic. The main motivation behind this choice is the availability of reasoning support about multivariable integral, differential, transcendental and topological theories [7], which are the foremost foundations required for the formalization of Laplace transform theory.

The rest of the paper is organized as follows: We provide a brief introduction about the multivariable calculus theories of HOL-Light in Section 2. The formalization of the Laplace transform function is provided in Section 3. We utilize this formalization to formally verify the classical properties of Laplace transform in Section 4. The formal verification of the LTC circuit is given in Section 5. Finally, Section 6 concludes the paper.

2 Multivariable Calculus Theories in HOL-Light

HOL-Light is a higher-order-logic theorem prover that belongs to the HOL family of theorem provers. Its unique features include an efficient set of inference rules and the usage of Objective CAML (OCaml) language [6], which is a variant of the strongly-typed functional programming language ML [11], for its development and interaction. HOL-Light provides formal reasoning support for many mathematical theories, including sets, natural numbers, real analysis, complex analysis and vector calculus, and has been particularly successful in verifying many challenging mathematical theorems. The main motivation behind choosing HOL-Light for the formalization of Laplace transform theory in this paper is the availability of a rich set of formalized multivariable calculus theories on the Euclidean space [7].

In HOL-Light, a n-dimensional vector is represented as a $\mathbb{R}^n$ column matrix with individual elements as real numbers. All of the vector operations are then handled as matrix manipulations. This way, complex numbers can be represented by the data-type $\mathbb{R}^2$, i.e, a column matrix having two elements. Similarly, pure real numbers can be represented by two different data-types, i.e., by a 1-dimensional vector $\mathbb{R}^1$ or a number on the real line $\mathbb{R}$. All the vector algebraic theorems have been formally verified using HOL-Light for arbitrary functions with a flexible data-type $\mathbb{R}^n \rightarrow \mathbb{R}^m$. For the formalization of Laplace transform, we have utilized several vector algebraic theorems for complex functions ($\mathbb{R}^2 \rightarrow \mathbb{R}^2$) and complex-valued functions ($\mathbb{R}^1 \rightarrow \mathbb{R}^2$).

In order to facilitate the understanding of the rest of the paper, some of the frequently used functions of the HOL-Light Multivariable calculus libraries [7] are described below:

Definition 1: *Cx*
⊢ ∀ a. Cx a = complex(a,&0)

The function `Cx` accepts a real number and return its corresponding complex number with the imaginary part as zero. It uses the function `complex`, which accepts a pair of real numbers and returns the corresponding complex number such that the real part of the complex number is equal to the first element of the given pair and the imaginary part of the complex number is the second element of the given pair. The operator `&` maps a natural number to its corresponding real number.

Definition 2: *Re and Im*
⊢ ∀ z. Re z = z$1
⊢ ∀ z. Im z = z$2

The functions `Re` and `Im` accept a complex number and return its real and imaginary parts, respectively. The notation `z$n` represents the n^{th} component of a vector `z`.

Definition 3: *drop and lift*
⊢ ∀ x. drop x = x$1
⊢ ∀ x. lift x = (lambda i. x)

The function `drop` accepts a 1-dimensional vector and returns its single component as a real number. The function `lift` maps a real number to a 1-dimensional vector with its single component equal to the given real number.

Definition 4: *Exponential Functions*
⊢ ∀ x. exp x = Re(cexp (Cx x))

The functions `exp` and `cexp` represent the real and complex exponential functions in HOL-Light with data-types $\mathbb{R} \to \mathbb{R}$ and $\mathbb{R}^2 \to \mathbb{R}^2$, respectively.

Definition 5: *Limit of a function*
⊢ ∀ f net. lim net f = (@l. (f→l) net)

The function `lim` is defined using the Hilbert choice operator @ in the functional form. It accepts a *net* with elements of arbitrary data-type A and a function f, of data-type $A \to \mathbb{R}^m$, and returns $l : \mathbb{R}^m$, i.e., the value to which f converges at the given *net*. To formalize the improper integral of Equation (1), we will use the `at_posinfinity`, which models positive infinity, as our *net*,

Definition 6: *Integral*
⊢ ∀ f i. integral i f = (@y.(f has_integral y) i)
⊢ ∀ f i. real_integral i f = (@y.(f has_real_integral y) i)

The function `integral` accepts an integrand function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ and a vector-space $i : \mathbb{R}^n \rightarrow \mathbb{B}$, which defines the region of integration. Here, $\mathbb{B}$ represents boolean data-type. It returns a vector of data-type $\mathbb{R}^m$, which represents the integral of f over i. The function `has_integral` defines the same relationship in the relational form. In a similar way, the function `real_integral` represents the integral of a function $f : \mathbb{R} \rightarrow \mathbb{R}$, over a set of real numbers $i : \mathbb{R} \rightarrow \mathbb{B}$. The regions of integration, for both of the above integrals, can be defined to be bounded by a vector interval $[a, b]$ or real interval $[a, b]$ using the HOL-Light functions `interval [a,b]` and `real_interval [a,b]`, respectively.

Definition 7: *Derivative*

```
⊢ ∀ f net. vector_derivative f net =
  (@f'.(f has_vector_derivative f') net)
```

The function `vector_derivative` accepts a function $f : \mathbb{R}^1 \rightarrow \mathbb{R}^m$, which needs to be differentiated, and a *net* of data-type $\mathbb{R}^1 \rightarrow \mathbb{B}$, that defines the point at which f has to be differentiated. It returns a vector of data-type $\mathbb{R}^m$, which represents the differential of f at *net*. The function `has_vector_derivative` defines the same relationship in the relational form.

We will build upon the above mentioned foundational definitions to formalize the Laplace transform function in the next section.

3 Formalization of Laplace Transform

Based on the theory of improper integrals [18], Equation (1) can be alternatively expressed as follows:

$$F(s) = \lim_{b \to \infty} \int_0^b f(t) e^{-st} dt \tag{2}$$

This definition holds under the conditions that the integral

$$f(b) = \int_0^b f(t) e^{-st} dt \tag{3}$$

exists for every $b > 0$ and the limit also exists as b approaches positive infinity.

Now, the Laplace transform function can be formalized in HOL-Light as follows:

Definition 8: *Laplace Transform*

```
⊢ ∀ s f. laplace f s =
  lim at_posinfinity (λb. integral (interval [lift(&0),lift(b)])
    (λt. cexp (-(s * Cx(drop t))) * f t))
```

The function `laplace` accepts a complex number s and a complex-valued function $f : \mathbb{R}^1 \rightarrow \mathbb{R}^2$. It returns a complex number that represents the laplace transform of f according to Equation (2). The complex exponential function cexp: $\mathbb{R}^2 \to \mathbb{R}^2$ is used in this definition because the data-type for $f(t)$ is $\mathbb{R}^2$. Similarly, in order to multiply variable $t : \mathbb{R}^1$ with the complex number s, it is first converted to $\mathbb{R}$ by using the function `drop` and then converted to data-type $\mathbb{R}^2$ by using `Cx`. Then, we use the vector integration function `integral` to integrate the expression $f(t)e^{-st}$ over the interval $[0, b]$ since the return type of this expression is $\mathbb{R}^2$. The limit of the upper interval b of this integral is then taken at positive infinity using the `lim` function with the `at_posinfinity` net. Based on the definition of `at_posinfinity`, the variable b must have a data-type $\mathbb{R}$. However, the region of integration of the vector integral function must be a vector space. Therefore, for data-type consistency, we lift the value 0 and variable b in the interval of the integral to the data-type $\mathbb{R}^1$ using the function `lift`.

The Laplace transform of a function f exists, i.e., the integral of Equation (3) is integrable and the limit of Equation (2) is convergent, if f is piecewise smooth and of exponential order on the positive real axis [1]. A function is said to be piecewise smooth on an interval if it is piecewise differentiable on that interval. Similarly, a causal function $f : \mathbb{R} \to \mathbb{C}$ is of exponential order if there exist constants $\alpha \in \mathbb{R}$ and $M{>}0$ such that $|f(t)| \leq Me^{\alpha t}$ for all $t \geq 0$. We formalize the Laplace transform existence conditions in HOL-Light as follows:

Definition 9: *Laplace Exists*
```
⊢ ∀ s f. laplace_exists f s ⇔
(∀ b. f piecewise_differentiable_on interval [lift (&0),lift b] )
  ∧ (∃ M a. Re s > drop a ∧ exp_order f M a)
```

The first conjunct in the above predicate ensures that f is piecewise differentiable on the positive real axis. The second conjunct expresses the exponential order condition of f for $\alpha < Re\ s$ using the following predicate:

Definition 10: *Exponential Order Function*
```
⊢ ∀ f M a. exp_order f M a ⇔ &0 < M ∧
(∀ t. &0 ≤ t ⇒ norm (f (lift t)) ≤ M * exp (drop a * t))
```

The function `exp_order` accepts a function $f : \mathbb{R}^1 \to \mathbb{R}^2$, a real number M and a complex number s and returns a $True$ if M is positive and f is bounded by Me^{at} for all $0 < t$.

4 Formal Verification of Laplace Transform Properties

In this section, we use Definition 8 to verify some of the classical properties of Laplace transform in HOL-Light. The formal verification of these properties not only ensures the correctness of our definition but also plays a vital role in minimizing the user intervention in reasoning about Laplace transform based analysis of systems, as will be depicted in Section 5 of this paper.

4.1 Limit Existence of the Improper Integral

According to the limit existence of the improper integral of Laplace transform property, if the given function $f : \mathbb{R} \to \mathbb{C}$ fulfills the conditions for the existence of its Laplace transform, i.e., it is of exponential order and piecewise smooth, then there will certainly exists a complex number l, to which the complex-valued integral of Equation (3) converges at positive infinity [1]. This property can be formalized based on Definitions 8 and 9 as follows:

Theorem 1: *Limit Existence of Integral of Laplace Transform*

```
⊢ ∀ f s. laplace_exists f s ⇒
  (∃l. ((λb. integral (interval [lift (&0),lift b])
    (λt. cexp (-(s * Cx (drop t))) * f t)) → l) at_posinfinity)
```

We proceed with the verification of the above theorem by first splitting the complex-valued integrand, i.e., $f(t)e^{-st}$, into its corresponding real and imaginary parts. Now using the linearity property of integral, the conclusion of the theorem can be expressed in terms of two integrals as follows:

```
∃l.( (λb. integral (interval [lift (&0),lift b])
      (λt. Cx (Re (cexp (-(s * Cx (drop t))) * f t))) +
  ii * integral (interval [lift (&0),lift b])
      (λt. Cx (Im (cexp (-(s * Cx (drop t))) * f t)))) → l)
        at_posinfinity
```

where, `ii` represents the constant value $\sqrt{-1}$ that is multiplied with the imaginary part of a complex number. Next, we verified the following two lemmas that allow us to break the above subgoal into two subgoals involving the limit existence of two real-valued integrals.

Lemma 1: *Relationship between the Real and Complex Integral*

```
⊢ ∀ f s t l. (f has_real_integral l) (real_interval [&0,t]) ⇒
  ((λt. Cx (f (drop t))) has_integral Cx l)
    (interval [lift (&0),lift t])
```

Lemma 2: *Limit of a Complex-Valued Function*

```
⊢ ∀ f L1 L2.
  ((λt. Re (f t)) ⇒ L1) at_posinfinity ∧
  ((λt. Im (f t)) ⇒ L2) at_posinfinity ⇒
    (f → complex (L1,L2)) at_posinfinity
```

The subgoal for the limit existence of the first real-valued integral is as follows:

```
laplace_exists f s ⇒
  ∃k. ((λb. real_integral (real_interval [&0,b])
    (λx. abs (Re (cexp (-s * Cx (x)) * f(lift x))))) → k)
      at_posinfinity
```

The proof of the above subgoal is primarily based on the Comparison Test for Improper Integrals [18], which has been formally verified as part of our development as follows:

Lemma 3: *Comparison Test for Improper Integrals*

```
⊢ ∀ f g a. (&0 ≤ a) ∧ (∀x. a ≤ x ⇒ &0 ≤ f x ∧ f x ≤ g x) ∧
  (∀ b. g real_integrable_on real_interval [a,b]) ∧
  (∀ b. f real_integrable_on real_interval [a,b]) ∧
  (∃ k.((λb. real_integral (real_interval [a,b]) g)⇒ k)
    at_posinfinity) ⇒
      (∃ k.((λb. real_integral (real_interval [a,b]) f) ⇒ k)
        at_posinfinity)
```

The `laplace_exists f s` assumption of Theorem 1 ensures that the integrand fe^{-st}, of our subgoal, is upper bounded by $Me^{-(Re(s)-\alpha)t}$, which in turn can also be verified to be integrable and having a convergent integral for $Re\ s > \alpha$ as the upper limit of integration approaches positive infinity. Moreover, the piecewise differentiability condition in the predicate `laplace_exists f s` ensures the integrability of f. These results allow us to fulfill the assumptions of Lemma 3 and thus conclude the limit existence subgoal for the real-valued integral of the real part. The proof of the subgoal for the limit existence of the real-valued integral corresponding to the imaginary part is very similar and its verification concludes the proof of Theorem 1.

4.2 Linearity

The linearity of Laplace transform can be expressed mathematically for two functions f and g and two complex numbers α and β as follows [1]:

$$\Big(\ \mathcal{L}\ \alpha f(x) + \beta g(x)\ \Big)(s) = \alpha(\mathcal{L}f)(s) + \beta(\mathcal{L}g)(s) \tag{4}$$

We verified this property as the following theorem:

Theorem 2: *Linearity of Laplace Transform*

```
⊢ ∀ f g s a b. laplace_exists f s ∧ laplace_exists g s ⇒
  laplace (λx. a * f x + b * g x) s =
    a * laplace f s + b * laplace g s
```

The proof is based on Theorem 1 and the linearity properties of integration and limit.

4.3 Frequency Shifting

The Frequency shifting property of Laplace transform deals with the case when the Laplace transform of the composition of a function f with the exponential function is required [1].

$$\Big(\mathcal{L}\ e^{bt}f(t)\Big)(s) = (\mathcal{L}f)(s-b) \tag{5}$$

These type of functions, called the *damping functions*, frequently occur in the analysis of many natural systems like harmonic oscillators. Frequency shifting property is used to analyze and measure the damping effects on the systems in the corresponding s-domain [17]. We verified the property as the following theorem:

Theorem 3: *Frequency Shifting*

```
⊢ ∀ f s b. laplace_exists f s ⇒
  laplace (λt. cexp (b * Cx (drop t)) * f t) s = laplace f (s - b)
```

4.4 Integration in Time Domain

The Laplace transform of an integral of a continuous function can be evaluated using the integration in time domain property

$$\Big(\mathcal{L}\int_0^t f(\tau)d\tau\Big)(s) = \frac{1}{s}(\mathcal{L}f)(s) \tag{6}$$

where $Re\ s > 0$ [1]. Such type of functions extensively occur in control and electrical systems and their s-domain analysis is greatly simplified by using the above relation [10]. This property has been verified in HOL-Light as follows:

Theorem 4: *Integration in Time Domain*

```
⊢ ∀ f s. (&0 < Re s) ∧ laplace_exists f s ∧
  laplace_exists (λx. integral (interval [lift (&0),x]) f) s ∧
  (∀x. f continuous_on interval [lift (&0),x]) ⇒
    laplace (λx. integral (interval [lift (&0),x]) f) s =
      inv(s) * laplace f s
```

where the function `inv` represents the reciprocal of a given vector. The proof of the above theorem is primarily based on the Integration-by-parts property, which was verified as part of the reported development as follows:

Lemma 4: *Integration by Parts*

```
⊢ ∀ f g f' g' a b. (drop a ≤ drop b) ∧
  (∀ x. (f has_vector_derivative f' x)
    (at x within interval [a,b])) ∧
  (∀ x. (g has_vector_derivative g' x)
    (at x within interval [a,b])) ∧
  (λx. f' x * g x) integrable_on interval [a,b] ∧
  (λx. f x * g' x) integrable_on interval [a,b] ⇒
    integral (interval [a,b]) (λx. f x * g' x) =
      f b * g b - f a * g a - integral (interval [a,b])
        (λx. f' x * g x)
```

where the function `integrable_on` formally represents the integrability of a vector function on a vector space. The integrand of Theorem 4, which is the product of a complex exponential and the function $\int_0^t f(\tau)\ d\tau$, can be simplified using Lemma 4 to obtain the following subgoal:

```
(&0 < Re s) ⇒
  lim at_posinfinity (λb. integral (interval [lift &0,lift b]) f *
   -inv s * cexp (-(s * Cx (drop (lift b))))) -
  lim at_posinfinity (λb. integral (interval [lift &0,lift b])
   (λx. f x * -inv s * cexp (-(s * Cx (drop x))))) =
  inv s * lim at_posinfinity (λb. integral
   (interval[lift &0,lift b])(λt. cexp (-(s * Cx(drop t))) * f t))
```

The first term on the left-hand-side of the above subgoal can be verified to approach zero at positive infinity since, based on the existence of Laplace transform condition, $f(t)$ grows more slowly than an exponential. The remaining two terms can then verified to be equivalent based on simple arithmetic reasoning.

4.5 First Order Differentiation in Time Domain

The Laplace of a differential of a continuous function f is given as follows [1]:

$$\left(\mathcal{L}\frac{df}{dx}\right)(s) = s(\mathcal{L}f)(s) - f(0) \tag{7}$$

We verified it as the following theorem:

Theorem 5: *First Order Differentiation in Time Domain*

```
⊢ ∀ f s. laplace_exists f s ∧
  laplace_exists (λx. vector_derivative f (at x)) s ∧
  (∀ x. f differentiable at x) ⇒
    laplace (λx. vector_derivative f (at x)) s =
      s * laplace f s - f (lift (&0))
```

using Theorem 1, Lemma 4 and the fact that $f(t)e^{-st}|_0^{\infty} = [0 - f(0)]$.

4.6 Higher Order Differentiation in Time Domain

The Laplace of a n-times continuously differentiable function f is given as the following mathematical relation [1]:

$$\left(\mathcal{L}\frac{d^n f}{dx^n}\right)(s) = s^n(\mathcal{L}f)(s) - \sum_{k=1}^{n} s^{k-1}\frac{d^{n-k}f(0)}{dx^{n-k}} \tag{8}$$

This property forms the foremost foundation for analyzing higher-order differential equations based on Laplace transform and is verified as follows:

Theorem 6: *Higher Order Differentiation in Time Domain*

```
⊢ ∀ f s n. laplace_exists_higher_derivative n f s ∧
  (∀x. higher_derivative_differentiable n f x) ⇒
  laplace (λx. higher_order_derivative n f x) s =
    s pow n * laplace f s - vsum (1..n) (λx. s pow (x-1) *
    higher_order_derivative (n-x) f (lift (&0)))
```

The first assumption ensures the Laplace existence of f and its first n higher-order derivatives. Similarly, the second assumption ensures the differentiability of f and its first n higher-order derivatives on $x \in \mathbb{R}$. The expressions `higher_order_derivative n f x` and `vsum (1..n) f` recursively model the n^{th} order derivative of f with respect to x and the vector summation of the n terms from 1 to n of function f, respectively. The proof of Theorem 6 is based on induction on variable n. The proof of the base case is based on simple arithmetic reasoning and the step case is discharged using Theorem 5 and summation properties along with some arithmetic reasoning.

The formalization, presented in this section, had to be done in an interactive way due to the undecidable nature of higher-order logic and took around 5000 lines of HOL-Light code and approximately 800 man-hours. One of the major challenges faced during this formalization is the non-availability of detailed proof steps for Laplace transform properties in the literature. The mathematical texts on Laplace transform properties provide very abstract proof steps and often ignore the subtle reasoning details. For instance, all the mathematical texts that we came across (e.g. [1,14]) provide the exponential order condition as the only condition for the limit existence of the improper integral of Laplace transform. However, as described in Section 4.1, the actual formal proof is based on splitting the complex-valued integrand into the corresponding real and imaginary parts and using the Integral comparison test and we had to find this reasoning on our own. Similarly, in verifying the integration in time property (Theorem 4), the exact reasoning about the convergence of the term $e^{-st}\int_0^t f(\tau)\, d\tau$ to zero, which was the main bottleneck in the proof, could not be found in any mathematical text on Laplace transform.

Other time-consuming factors, associated with our formalization, include the formal verification many multivariable calculus related theorems, which were required in our formalization but were not available in the current HOL-Light distribution. These generic results can be very useful for other similar formalizations and some of the ones of common interest are given below and others can be found in our proof script [15].

Lemma 5: *Upper Bound of Monotonically Increasing and Convergent f*
```
⊢ ∀ f n k. (&0 ≤ n) ∧ (∀n m. n ≤ m ⇒ f n ≤ f m) ∧
  ((f → k) at_posinfinity) ⇒ f n ≤ k
```
Lemma 6: *Limit at Positive Infinity of f implies Limit of abs(f)*
```
⊢ ∀ f l. (f → l) at_posinfinity ⇔
  ((λi. f (abs i)) → l ) at_posinfinity
```
Lemma 7: *Relationship between Real and Vector Derivative*
```
⊢ ∀ f f' x s. ((f has_real_derivative f') (atreal x within s)) ⇒
  ((Cx o f o drop has_vector_derivative Cx f')
  (at (lift x) within IMAGE lift s) )
```
Lemma 8: *Chain Rule of Differentiation for Complex-valued Functions*
```
⊢ ∀ f g f' g' x s.((f has_vector_derivative f') (at x within s)) ∧
  ((g has_complex_derivative g') (at (f x) within IMAGE f s) ) ⇔
    ((g o f has_vector_derivative f' * g') (at x within s) )
```

The main advantage of the formal verification of Laplace transform properties is that our proof script, available for download at [15], can be built upon to facilitate formal reasoning about the Laplace transform based analysis of safety-critical systems, as depicted in the next section.

5 Application: Linear Transfer Converter (LTC) circuit

As an illustrative example of our work, we formally verify the transfer function of a Linear Transfer Converter (LTC) circuit, depicted in Figure (1), which is widely used for converting the voltage and current levels in power electronics systems [13]. The functional correctness of power systems mainly depends on the design and stability of LTCs and thus the accuracy of LTC analysis is of dire need. Standard design techniques of LTCs are based on the transfer function analysis, i.e., the differential equation of a LTC circuit is first converted into its corresponding s-domain equivalent, and then depending upon the required stability requirements, the values of circuit components, like resistors and inductors are calculated [9]. We perform this analysis using our formalization of Laplace transform within the sound core of HOL-Light theorem prover in this paper. The behavior of the LTC circuit, with input complex voltage $u(t)$ across

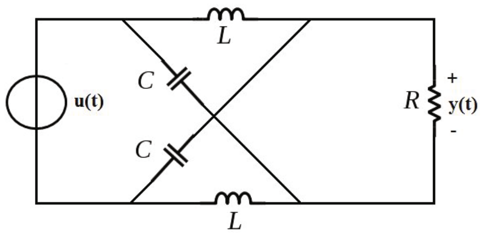

Fig. 1. Linear Transfer Converter Circuit

the voltage generator, and the output complex voltage $y(t)$, across the resistor R, can be expressed using the following differential equation [1]:

$$\frac{d^2y}{dt^2} - \frac{2}{RC}\frac{dy}{dt} + \frac{1}{LC}y = \frac{d^2u}{dt^2} - \frac{1}{LC}u \tag{9}$$

The corresponding transfer function of this given circuit is as follows [1]:

$$\frac{Y(s)}{U(s)} = \frac{s^2 - \frac{1}{LC}}{s^2 - \frac{2s}{RC} + \frac{1}{LC}} \tag{10}$$

The objective of this section is to verify this transfer function using Equation (9). In order to be able to formally express Equation (9), we formalized the following function to model an n-order differential equation in HOL-Light:

Definition 11: *Differential Equation*

```
⊢ ∀ n A f x. diff_eq n A f x ⇔
  vsum (0..n) (λt. EL t L x * higher_order_derivative t f x)
```

The function diff_eq accepts the order of the differential equation n, a list of coefficients A, differentiable function f and the differentiation variable x. It utilizes the functions vsum n f and EL m L, which return the vector summation ($\sum_{i=0}^{n} f_i$) and the m^{th} element of a list L, respectively, to generate the differential equation corresponding to the given parameters. Now, Equation (9) can be formalized as follows:

Definition 12: *Differential Equation of LTC*

```
⊢ ∀ y u x L C R. diff_eq_LTC y u x L C R ⇔
diff_eq 2 [ Cx (&1 / L * C); --Cx (&2 / R * C); Cx (&1)] y x =
diff_eq 2 [ --Cx (&1 / L * C ); Cx (&0); Cx (&1)] u x
```

The function diff_eq_LTC accepts the output voltage function $y : \mathbb{R}^1 \to \mathbb{R}^2$, the input voltage function $u : \mathbb{R}^1 \to \mathbb{R}^2$, the resistance $R : \mathbb{R}$, the inductance $L : \mathbb{R}$ and the capacitance $C : \mathbb{R}$ being the capacitance and $x : \mathbb{R}^1$ being time. It then returns Equation (9) in the summation form.

Now, the transfer function of the given LTC circuit, given in Equation (10), can be verified as the following theorem in HOL-Light.

Theorem 7: *Transfer function of LTC*

```
⊢ ∀ y u s R L C. (&0 < R) ∧ (&0 < L) ∧ (&0 < C) ∧
  (zero_initial_conditions 1 u) ∧ ( zero_initial_conditions 1 y) ∧
  (∀x. higher_derivative_differentiable 2 y x) ∧
  (∀x. higher_derivative_differentiable 2 u x) ∧
  (higher_derivative_laplace_exists 2 y s) ∧
  (higher_derivative_laplace_exists 2 u s) ∧
  (∀t. diff_eq_LTC y u t L C R) ∧ ∼(laplace u s = Cx(&0)) ∧
  ∼((Cx(&1/(L*C)) - Cx(&2/(R*C))*s) + s pow 2 = Cx(&0) ) ⇒
   (laplace y s / laplace u s =
    (s pow 2 - Cx(&1/(L*C))) / ((Cx(&1/(L*C)) -
      Cx(&2/(R*C))*s) + s pow 2))
```

The first three assumptions ensure the positive values for resistor, inductor and capacitor, respectively. The predicate zero_initial_conditions is used to define the initial conditions, i.e., to assign a value 0 to the given function and its n derivatives at time equal to zero. In our case, we need zero initial conditions for the functions u and y up to the first-order derivative, which are modeled using the fourth and fifth assumptions. The next four assumptions ensure that the functions y and u are differentiable up to the second-order and the Laplace transform exists up to the second order derivatives of these functions. The next assumption represents the formalization of Equation (9), the next two assumptions provide some interesting design related relationships, which must hold for constructing a reliable LTC, and the conclusion of the theorem represents Equation (10). The reasoning about the correctness of Theorem 7 is very straightforward and is primarily based on Definition 8 and Theorem 6 and some simple arithmetic reasoning. The proof script consists of approximately 650 lines of HOL-Light code [15] and the proof process took just a couple of hours, which clearly indicates the usefulness of our work in conducting the formal analysis of real-world applications using the Laplace transform method.

6 Conclusion

This paper advocates the usage of higher-order-logic theorem proving for conducting Laplace transform based analysis, which is an essential design step for almost all physical systems. Due to the high expressiveness of the underlying logic, we can formally model the differential equation depicting the behaviour of the given physical system in its true form, i.e., without compromising on the precision of the model. The Laplace transform method can then be used in a theorem prover to deduce interesting design parameters from this equation. The inherent soundness of theorem proving guarantees correctness of this analysis and ensures the availability of all pre-conditions of the analysis as assumptions of the formally verified theorems. To the best of our knowledge, these features are not shared by any other existing computerized Laplace transform based analysis technique and thus the proposed approach can be very useful for the analysis of physical systems used in safety-critical domains.

The main challenge in the proposed approach is the enormous amount of user intervention required due to the undecidable nature of the higher-order logic. We propose to overcome this limitation by formalizing Laplace transform theory in higher-order logic and thus minimizing the user guidance in the reasoning process by building upon the already available results. As a first step towards this direction, this paper presents the formalization of Laplace transform and the formal verification of some of its classical properties, such as existence, linearity, frequency shifting and differentiation and integration in time domain, using the multivariable calculus theories of HOL-Light. Based on this work, we are able to conduct the formal analysis of a Linear Transfer Converter (LTC) circuit, which is commonly used electronic circuit in a very straightforward way.

This paper opens the doors towards a novel and promising usage of theorem proving. The formalization of Laplace transform foundations, presented in this paper, can be directly used to reason about the transfer functions of many systems used in the domains of control engineering and analog and mixed signal (AMS) circuits, where the usage of formal verification is a dire need given their safety-critical nature. Our formalization can also be built upon to formalize the inverse Laplace transform function and its associated properties, which can be very useful in analyzing the behavior of engineering systems in the time-domain [1]. Our formalization can also be used to formalize other mathematical transforms. For instance, Fourier transform [5], which is a foundational mathematical theory for analyzing digital signal processing applications, can be easily formalized by restricting the variable s of the Laplace transform definition to acquire pure imaginary values only.

Acknowledgements. This work was supported by the National Research Program for Universities grant (number 1543) of Higher Education Commission (HEC), Pakistan.

References

1. Beerends, R.J., Morsche, H.G., Van den Berg, J.C., Van de Vrie, E.M.: Fourier and Laplace Transforms. Cambridge University Press, Cambridge (2003)
2. Denman, W., Akbarpour, B., Tahar, S., Zaki, M., Paulson, L.C.: Formal Verification of Analog Designs using MetiTarski. In: Formal Methods in Computer Aided Design, pp. 93–100. IEEE (2009)
3. Dorcak, L., Petras, I., Gonzalez, E., Valsa, J., Terpak, J., Zecova, M.: Application of PID Retuning Method for Laboratory Feedback Control System Incorporating FO Dynamics. In: International Carpathian Control Conference (ICCC), pp. 38–43. IEEE (2013)
4. Frehse, G., Le Guernic, C., Donzé, A., Cotton, S., Ray, R., Lebeltel, O., Ripado, R., Girard, A., Dang, T., Maler, O.: Spaceex: Scalable Verification of Hybrid Systems. In: Gopalakrishnan, G., Qadeer, S. (eds.) CAV 2011. LNCS, vol. 6806, pp. 379–395. Springer, Heidelberg (2011)
5. Gaydecki, P.: Foundations of Digital Signal Processing: Theory, Algorithms and Hardware Design. IET (2004)
6. Harrison, J.: HOL Light: An overview. In: Berghofer, S., Nipkow, T., Urban, C., Wenzel, M. (eds.) TPHOLs 2009. LNCS, vol. 5674, pp. 60–66. Springer, Heidelberg (2009)
7. Harrison, J.: The HOL Light Theory of Euclidean Space. Automated Reasoning 50(2), 173–190 (2013)
8. Zaki, M.H., Tahar, S., Boisr, G.: Formal Verification of Analog and Mixed Signal Designs: A survey. Microelectronics Journal 39, 1395–1404 (2008)
9. Ioinovici, A.: Power Electronics and Energy Conversion Systems, Fundamentals and Hard-switching Converters. John Wiley & Sons (2013)
10. Paul, B.: Industrial Electronics and Control. PHI Learning Pvt. Ltd. (2004)
11. Paulson, L.C.: ML for the Working Programmer. Cambridge University Press, Cambridge (1996)
12. Podlubny, I.: The Laplace Transform Method for Linear Differential Equations of the Fractional Order. Technical report, Slovak Acad. Sci., Kosice (1994)
13. Rashid, M.: Power Electronics Handbook. Elsevier (2011)
14. Schiff, J.L.: The Laplace Transform: Theory and Applications. Springer (1999)
15. Taqdees, S.H.: Formalization of Laplace Transform using the Multivariable Calculus Theory of HOL-Light (2013), `http://save.seecs.nust.edu.pk/shtaqdees/laplace.html`
16. Ucar, A., Cetin, E., Kale, I.: A Continuous-Time Delta-Sigma Modulator for RF Subsampling Receivers. In: IEEE Transactions on Circuits and Systems, pp. 272–276. IEEE (2012)
17. Westra, J.R., Verhoeven, C.J.M., van Roermund, A.H.M.: Oscillators and Oscillator Systems: Classification, Analysis and Synthesis. Springer (1999)
18. Xiao, J.: Integral and Functional Analysis. Nova Publishers (2008)
19. Yang, X.: Mathematical Modeling with Multidisciplinary Applications. John Wiley & Sons (2013)