FORMALIZATION OF LAPLACE TRANSFORM USING THE MULTIVARIABLE CALCULUS THEORY OF HOL-LIGHT

By

SYEDA HIRA TAQDEES

2011-NUST-MS-EE(S)-017

Supervisor:

Dr. Osman Hasan

A thesis submitted in partial fulfillment of the requirements for the degree of Masters of Science in Electrical Engineering

School of Electical Engineering and Computer Science,

National University of Sciences and Technology (NUST), Islamabad,

Pakistan.

(November 2013)

to my

Ammi & Bhai

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 develop a verification scheme of analog circuits. These days, analog circuits have become an integral part of almost all embedded systems. However, the unavailability of accurate analysis methods for analog circuits, which exhibit continuous behavior, jeopardizes the usage of embedded systems in many safety-critical applications. In order to overcome this limitation, we propose to use higher-order-logic theorem proving for verifying analog circuits. Towards this direction, this thesis presents an approach to formally verify the transfer functions of continuous models of analog circuits using the Laplace transform theory. In particular, we presents a higher-order-logic formalization of the Kirchhoffs voltage and current laws and basic analog components using the HOL-Light theorem prover. To illustrate the practical effectiveness and utilization of the proposed approach, we provide the formal analysis of first and second-order Sallen-Key low-pass filters and Linear Transfer Converter (LTC) circuit, which are commonly used electrical circuit.

Table of Contents

List of Figures

Chapter 1

Introduction

Laplace transform [25] 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 [3]. 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) [35] 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.

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

$$F(s) = \int_0^{\infty} f(t)e^{-st}dt, \;\; s \in \mathbb{C} \tag{1.1}$$

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.

1.1 Problem Statement

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 (1.1) 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 (1.1) 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, in the fields of control systems and electrical engineering, techniques involving Laplace transform analysis are being proposed and tested by using the Matlab and Maple Laplace transform libraries [7, 30], that make them prone to inaccuracy approximation errors. 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.

1.2 Proposed Solution

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 (1.1) 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, we formally verify the existence, linearity and scaling properties of Laplace transform. We 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.

The main idea behind the proposed methodology is to use the HOL-Light theorem prover [16], 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 [17], which are the foremost foundations required for the formalization of Laplace transform theory.

In order to illustrate the practical effectiveness and utilization of this formalization, we use it to develop a methodology for the formal verification of transfer function of analog circuits. Formal verification of analog circuits is of utmost importance [18]. However, to the best of our knowledge, all the existing formal verification approaches work with abstracted discretized models of analog circuits (e.g., [9], [5]). 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. Our formalization of Laplace transform overcomes this limitation and we have been able to formally verify the transfer function of the low-pass Sallen-Key filters and LTC circuit using their differential equation.

1.3 Outline of the Thesis

The rest of the thesis report is organized as follows: To aid the understanding of this work, a brief overview of formal verification and HOL-Light theorem prover is provided in Chapter 2. Next, we present our formalization of Laplace transform theory and its properties in Chapter 3. Chapter 4 contains our proposed formal technique for analog circuits verification based on the formalized Laplace transform theory. Finally, Chapter 5 concludes the thesis.

Chapter 2

Preliminaries

In this chapter, we present some foundational material about basics of formal verification with focus on theorem proving and HOL-Light theorem prover to facilitate understanding of this thesis.

2.1 Formal Verification

Formal methods are the use of ideas and techniques from applied mathematics and logic to specify, analyze and reason about computing systems in order to increase design assurance and eliminate defects. In hardware and physical systems, basic aim of formal verification is to ensure the correct functionality with the highest reliably and completeness as compared to simulation based verification techniques. Because of the inherent soundness of formal verification, it has become an essential step in the design process of systems for safety-critical applications.

Formal verification is broadly classified into two types i.e. theorem proving and model checking. In theorem proving, implementation and specification of the system are described in formal logic and then their relationship is verified within the sound core of a theorem prover. Theorem prover actually builds on top of a functional programming language; hence soundness and completeness are assured for every verified theorem. Whereas in model checking, behavior of the system is checked and its properties are verified using an algorithm that determines the validity of formulae written in some temporal logic with respect to the behavioral model of the system.

Systems dealing with continuous quantities and mathematical analysis including complex and real numbers; like Laplace transform formalization; are best to be verified using theorem proving because of its ability to handle the continuous values. Theorem proving can completely capture their continuous behavior whereas model checking works with the abstracted discretized models and thus gives incomplete verification.

2.2 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 [16], which is a variant of the strongly-typed functional programming language ML [24], 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 thesis is the availability of a rich set of formalized multivariable calculus theories on the Euclidean space [17].

2.3 Multivariable Calculus Theories in HOL-Light

The formalized multivariable calculus in HOL-Light contains integral, differential, transcendental and topological theories. Their formalization is primarily based on vector-space algebra. 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 $\mathbb{R}^n \to \mathbb{R}^m$. For the formalization of Laplace transform, we have utilized several vector algebraic theorems for complex functions ($\mathbb{R}^2 \to \mathbb{R}^2$) and complex-valued functions ($\mathbb{R}^1 \to \mathbb{R}^2$).

In order to facilitate the understanding of the rest of the thesis, some of the frequently used functions of the HOL-Light Multivariable calculus libraries [17] are described below:

Definition 2.1: *Cx*

$\vdash \forall$ `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 2.2: *Re and Im*

$\vdash \forall$ `z. Re z = z$1`

$\vdash \forall$ `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 2.3: *drop and lift*

$\vdash$ ∀ x. `drop x = x$1`

$\vdash$ ∀ 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 2.4: *Exponential Functions*

$\vdash$ ∀ 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 $\mathbb{R} \rightarrow \mathbb{R}$ and $\mathbb{R}^2 \rightarrow \mathbb{R}^2$, respectively.

Definition 2.5: *Limit of a function*

$\vdash$ ∀ 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 $A \rightarrow \mathbb{R}^m$, 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 (1.1), we will use the `at_posinfinity`, which models positive infinity, as our *net*,

Definition 2.6: *Integral*

$\vdash$ ∀ f i. `integral i f = (@y.(f has_integral y) i)`

$\vdash$ ∀ 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 $f : \mathbb{R} \to \mathbb{R}$, over a set of real numbers $i : \mathbb{R} \to \mathbb{B}$. 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 2.7: *Derivative*

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

The function `vector_derivative` accepts a function $f : \mathbb{R}^1 \to \mathbb{R}^m$, which needs to be differentiated, and a *net* of data-type $\mathbb{R}^1 \to \mathbb{B}$, 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 chapter.

2.4 Summary

Formal methods employing higher-order-logic theorem proving are most suitable for the formalization of Laplace transform theory because of the ability to deal continuous complex variables and underlying soundness. We have used HOL-Light theorem prover to formalize the integral of Laplace transform and to verify its properties because of the availability of formalized multivariable calculus; including integral, differential, transcendental and topological theories; in HOL-Light. In this chapter, we have provided the basic functions of these theories to aid in understanding the definitions and theorems in rest of the thesis.

Chapter 3

Formalization of Laplace Transform

In this chapter, we provide the formalization detail of Laplace transform definition and its properties.

3.1 Formalized Laplace Transform Definition

Based on the theory of improper integrals [34], Equation (1.1) can be alternatively expressed as follows:

$$F(s) = \lim_{b \to \infty} \int_0^b f(t) e^{-st} dt \tag{3.1}$$

This definition holds under the conditions that the integral

$$f(b) = \int_0^b f(t) e^{-st} dt \tag{3.2}$$

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 3.1: *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 $f : \mathbb{R}^1 \to \mathbb{R}^2$. It returns a complex number that represents the Laplace transform of f according to Equation (3.1). 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 (3.2) is integrable and the limit of Equation (3.1) is convergent, if f is piecewise smooth and of exponential order on the positive real axis [3]. 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 3.2: *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 3.3: *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 $0 < t$.

3.2 Formal Verification of Laplace Transform Properties

In this section, we use Definition 3.1 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 Chapter 4.

3.2.1 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 (3.2) converges at positive infinity [3]. This property can be formalized based on Definitions 3.1 and 3.2 as follows:

Theorem 3.1: *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 3.1: *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 3.2: *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 [34], which has been formally verified as part of our development as follows:

Lemma 3.3: *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 3.1 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 3.3 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 3.1.

3.2.2 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 [3]:

$$\Big(\mathcal{L}\ \alpha f(x) + \beta g(x) \Big)(s) = \alpha(\mathcal{L}f)(s) + \beta(\mathcal{L}g)(s) \tag{3.3}$$

We verified this property as the following theorem:

Theorem 3.2: *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 3.1 and the linearity properties of integration and limit.

3.2.3 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 [3].

$$\Big(\mathcal{L}\ e^{bt}f(t)\Big)(s) = (\mathcal{L}f)(s-b) \tag{3.4}$$

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 [32]. We verified the property as the following theorem:

Theorem 3.3: *Frequency Shifting*

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

3.2.4 Integration in Time Domain

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

$$\left(\mathcal{L}\int_0^t f(\tau)d\tau\right)(s) = \frac{1}{s}(\mathcal{L}f)(s) \tag{3.5}$$

where $Re\ s > 0$ [3]. Such type of functions extensively occur in control and electrical systems and their s-domain analysis is greatly simplified by using the above relation [23]. This property has been verified in HOL-Light as follows:

Theorem 3.4: *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 3.4: *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 3.4, which is the product of a complex exponential and the function $\int_0^t f(\tau)\, d\tau$, can be simplified using Lemma 3.4 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.

3.2.5 First Order Differentiation in Time Domain

The Laplace of a differential of a continuous function f is given as follows [3]:

$$\left(\mathcal{L}\frac{df}{dx}\right)(s) = s(\mathcal{L}f)(s) - f(0) \tag{3.6}$$

We verified it as the following theorem:

Theorem 3.5: *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 3.1, Lemma 3.4 and the fact that $f(t)e^{-st}|_0^\infty = [0 - f(0)]$.

3.2.6 Higher Order Differentiation in Time Domain

The Laplace of a n-times continuously differentiable function f is given as the following mathematical relation [3]:

$$\left(\mathcal{L}\frac{d^n f}{dx^n}\right)(s) = s^n(\mathcal{L}f)(s) - \sum_{k=1}^{n} s^{k-1}\frac{d^{n-k}f(0)}{dx^{n-k}} \tag{3.7}$$

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

Theorem 3.6: *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 3.6 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 3.5 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. [3, 27]) 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 3.2.1, 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 3.4), 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.

Lemma 3.5: *Upper Bound of Monotonically Increasing and Convergent f*

$\vdash$ ∀ f n k. (&0 ≤ n) ∧ (∀n m. n ≤ m ⇒ f n ≤ f m) ∧

((f $\rightarrow$ k) at_posinfinity) $\Rightarrow$ f n $\leq$ k

Lemma 3.6: *Limit at Positive Infinity of f implies Limit of abs(f)*

$\vdash$ $\forall$ f l. (f $\rightarrow$ l) at_posinfinity $\Leftrightarrow$

((λi. f (abs i)) $\rightarrow$ l) at_posinfinity

Lemma 3.7: *Relationship between Real and Vector Derivative*

$\vdash$ $\forall$ f f' x s. ((f has_real_derivative f') (atreal x within s)) $\Rightarrow$

((Cx o f o drop has_vector_derivative Cx f')

(at (lift x) within IMAGE lift s))

Lemma 3.8: *Chain Rule of Differentiation for Complex-valued Functions*

$\vdash$ $\forall$ f g f' g' x s.((f has_vector_derivative f') (at x within s)) $\wedge$

((g has_complex_derivative g') (at (f x) within IMAGE f s)) $\Leftrightarrow$

((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 can be built upon to facilitate formal reasoning about the Laplace transform based analysis of safety-critical systems, as depicted in the next chapter.

3.3 Summary

We have formalized Laplace transform definition given in Equation (1.1) using the `integral` and `limit` functions of HOL-Light. We have also defined functions to formalize the basic conditions necessary for the existence of Laplace transform of a function. [3] Using these definitions and mathematical reasoning in HOL-Light, we have verified the limit existence and properties of Laplace transform. The proof details are provided in this chapter. We have also highlighted some of the important mathematical theorems that we verified in order to formalize Laplace transform properties.

Chapter 4

Applications: Analog Circuits Verification

In this chapter, we use our formalized Laplace transform theory to develop a methodology for the formal verification of transfer function of analog circuits. With the latest advancement in the integrated circuit technology, several types of analog circuits [12] are being designed to amplify, process and filter analog signals in a wide range of applications. Functional verification of these analog circuits used independently or as a part of an embedded system is of paramount importance given the safety-critical nature of hardware applications these days. The goal of the functional verification of an analog circuit is to make sure that the implementation of the circuit exhibits the desired behavior. The implementation of a given circuit is obtained from its structure and components along with the well-known circuit analysis techniques. While the desired behavior of analog circuits is usually expressed as the transfer function of output and input signals in the s-domain, where s represents the angular frequency [21]. The relationship between the implementation and the behavior is then verified by taking the Laplace transform [31] of the differential equation obtained from the implementation model.

Traditionally, analog circuits are analyzed using simulation techniques. However, simulation results cannot be termed as 100% accurate due to the approximations introduced by using computer arithmetics, such as floating or fixed point numbers, for constructing computer based models of the continuous analog circuits. Moreover, the circuits are analyzed for some specific test cases only since exhaustive simulation is not possible due to the continuous nature of inputs. Due to these limitations, more rigorous and accurate analysis techniques for analyzing analog circuits are actively sought and formal verification, i.e., a computer based mathematical analysis technique, offers a promising solution [36].

Formal verification of analog circuits is an active area of research. Various formal techniques, based on conformance and model checking, have been developed in the last decade. However, to the best of our knowledge, all the existing formal verification approaches work with abstracted discretized models of analog circuits. In [29] and [2], conformance checking techniques have been presented to show the equivalence between the specified and implemented transfer function of analog circuits. In these techniques, the verification ideas are primarily based on the discretization of the s-domain transfer functions to the z-domain using the bilinear transformation, which raises issues, like the error analysis of transfer function coefficients and the state-space explosion when the inherited discretization of the design is encoded for larger models. Model checking (e.g., [8, 13, 20]) has also been used to formally verify analog circuits but all the model checking based techniques work with the abstraction of continuous dynamics because of the inability to model and analyze continuous systems. Thus, despite the inherent soundness of formal verification methods, such analysis cannot be termed as absolutely accurate.

We propose to use higher-order-logic theorem proving in order to formally verify transfer functions of continuous models of analog circuits. Higher-order logic is a system of deduction with a precise semantics and, due to its high expressiveness, can be used to describe any mathematical relationship, including the transfer functions of continuous models of analog circuit implementations and their desired transfer function specifications. Their equivalence can then be verified within the sound core of a theorem prover. Due to the high expressibility of higher-order logic, the proposed approach is very flexible in terms of analyzing a variety of analog circuits and transfer functions.

As a first step towards the proposed direction, we present the higher-order-logic formalization of the well-known Kirchhoffs voltage and current laws (commonly known as KVL and KCL) [6] and a few basic components of analog circuits, like resistor, inductor and capacitor. These are some of the foremost foundations for analog circuit analysis. Thus, the formalization of these results along with our formalized Laplace transform theory facilitates the formal analysis of analog circuits within the sound core of a higher-order-logic theorem prover. To the best of our knowledge, this is the first time that the formal reasoning support for the above mentioned analog circuit analysis foundations is being presented. In order to demonstrate the practical effectiveness and utilization of the reported formalization, we utilize it to verify the transfer function of first and second-order Sallen-Key low-pass filters [31] in a very straight-forward manner. Besides being used in several applications, these filters are also used as the basic building blocks of other higher-order low-pass filters and thus the formal verification of their transfer functions would facilitate the verification of a wide range of higher-order-filters as well. We also verify the transfer function of Linear Transfer Converter (LTC) circuit which is a very important part of power electronic system.

4.1 Existing Analog Circuits Verification Techniques based on Theorem Proving

In an early attempt to use higher-order-logic theorem proving for analog circuit verification, the PVS theorem prover was used to formally prove the functional equivalence between behavioral specification of VHDL-AMS designs and approximated linearized models of their synthesized netlists [11]. In the similar direction, Hanna [15] proposed an approach for verifying implementations of digital systems described at the analog level of abstraction. This approach is based on specifying the behaviors of transistors by conservative approximation techniques based on piecewise-linear predicates on voltages and currents. Moreover, Hanna proposed constraint based techniques for automating the verification process [14]. These early attempts focus more on constructing the circuit component models and for verifying the specification of the observed behaviour. However, the analyses were done at a very high abstraction level and thus realistic analog circuit models using complex numbers or differential equations were not used. This way, these analyses cannot be termed as the most precise and accurate ones.

Denman et al [5] proposed a functional verification approach for analog circuits using MetiTarski [1], which is an automated theorem prover for real-valued trigonometric functions. The behavioral model of the analog circuit is transformed into its closed form solution by using the *invlaplace* function of Maple and an inequality relating the closed form solution with the required property is fed to MetiTarski, which in turn determines if the inequality holds and in this case also generates the corresponding formal proof. A similar approach is also proposed in [22] for the verification of analog circuits using MetiTarski in the presence of noise and process variation by introducing stochastic modeling. However, these techniques do not aim for the complete transfer function analysis and are not suitable for real-world analog circuits that commonly deal with the complex voltages and currents. Moreover, the usage of computer algebra algorithms, which are unverified (cf. [5] p. 3), for calculating the closed form solution of the behavioral model also compromises on the accuracy of the analysis. These formal and semi-formal techniques have also been used for verifying some basic constituent components and building blocks of analog circuits, like logic gates [15], operational amplifier (op-amp) [5,11], oscillators [5] and op-amp integrator [22]. The proposed technique is generic enough to cater for the verification of all these components and their arbitrary combinations. For illustration purpose, we present the verification of Sallen-Key low pass filters, which are quite compatible in complexity to the existing formally verified circuits.

The comprehensive survey article about the formal verification techniques for the analog part of the A&MS systems [36] concludes by stating that, to date, no technique has been successful to model the analog circuits with continuous differential equations without approximations and to analyze them using Laplace transform in the sound core of a theorem prover. In this thesis, we overcome these limitations and have have been able to exactly model the true differential equation based models of analog circuits and to verify their transfer functions by using the formalized Laplace transform theory.

4.2 Methodology

The proposed methodology for the formal verification of transfer functions of analog circuits is shown in Figure 4.1. The inputs required for the proposed verification methodology are (i) a structural view of the given analog circuit representing the connections of its sub-components, (ii) the modeling differential equation of the given circuit relating its input and output quantities in the time domain and (iii) the transfer function representing the required behavior in the s-domain. The first step in the proposed methodology is to translate the structural representation of the given circuit to its corresponding higher-order-logic function using the definitions available in the formalized analog library. This provides us with our implementation model as shown in the Figure 4.1. The next step in the proposed methodology is to formalize the given modeling differential equation and the transfer function in higher-order logic to get the formal differential equation based specification and the

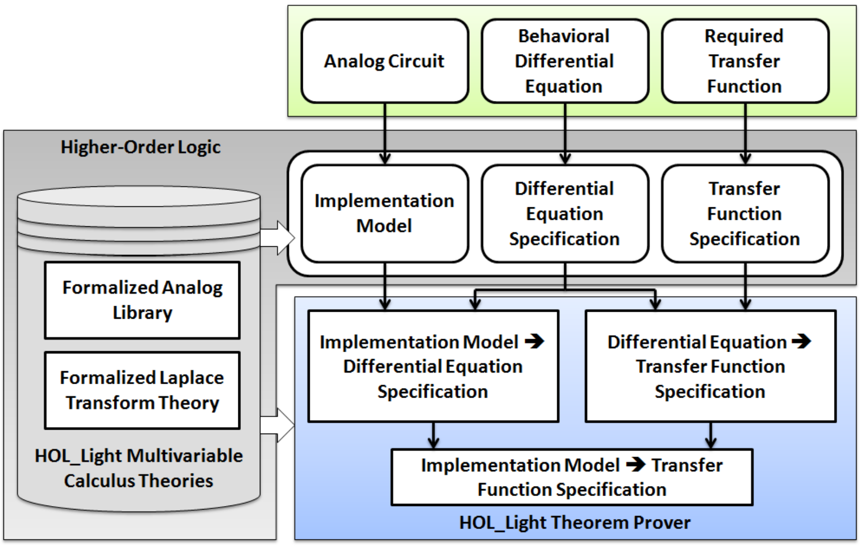

Figure 4.1: Proposed Methodology for the Formal Verification of Analog Circuits

formal transfer function based specification, respectively. These translations can be done based on the available multivariable calculus formalizations in HOL-Light [17]. The next step is to formally verify the implication between the implementation model and the formal differential equation based specification of the given circuit. This verification can be done in a very straightforward way based on the formalized analog library functions and some simple arithmetic reasoning. The next step in the proposed methodology is to verify that the differential equation specification of the given circuit implies the given transfer function specification using the formalized Laplace transform theory and arithmetic reasoning. The two implications verified in the last two steps also imply that the given structural view of the circuit implies the given transfer function based specification, which concludes the formal verification of the desired result within the sound core of the theorem prover.

The distinguishing features of this methodology include the higher confidence in the verification results due to the usage of pure complex and real number data-types for modeling the given circuit and the usage of theorem proving for the verification.

It is important to note that, just like any other verification approach, the proposed methodology requires the circuit and its desired behavior to be known apriori and it just allows us to formally verify that they correspond to one another.

4.3 Formalization of Analog Library

In this section, we explain our formalization of the various analog components and circuit simplification rules. To facilitate the understanding of definitions and theorems, HOL-Light definitions and functions in this chapter are described using a mixed-form notation, i.e., mathematical symbols are used for arithmetic operators, like integration, differentiation and summation.

We begin by formalizing the voltage and current expressions for a resistor, capacitor and inductor, which are the most commonly used analog circuit components, as the following higher-order-logic functions:

Definition 4.1: *Resistor, Inductor and Capacitor*

$\vdash$ ∀ R i.res_vol R i = (λt.i t * R)

$\vdash$ ∀ R v.res_cur R v = (λt.v t / R)

$\vdash$ ∀ L i.ind_vol L i = (λt.L * $\frac{di}{dt}$)

$\vdash$ ∀ L v Io.ind_cur L v Io =

(λt.Io + 1/L * $\int_0^t v(t)\ dt$)

$\vdash$ ∀ C i Vo.cap_vol C i Vo =

(λt.Vo + 1/C * $\int_0^t i(t)\ dt$)

$\vdash$ ∀ C v. cap_cur = (λt.C * $\frac{dv}{dt}$)

where (λx. f(x)) represents the lambda abstraction function f which accepts a variable x and returns $f(x)$. The variables i and v represents the time-dependant current and voltage variables, respectively, of complex data type. While the variables

R, L and C represent the constant resistance, inductance and the capacitance of their respective components, respectively. The variables Io and Vo are used in the definitions of inductance and capacitance to model the initial current in the inductor and the initial voltage across the capacitor [6], respectively. All these functions return a complex-valued type function that models the corresponding time dependant voltage or current.

Kirchhoff's voltage law (KVL) and Kirchhoff's current law (KCL) [6] form the most foundational circuit analysis and simplification laws. The KVL and KCL state that the directed sum of all the voltage drops around any closed network (loop) of an electrical circuit and the directed sum of all the branch currents leaving an electrical node is zero, respectively. Mathematically:

$$\sum_{k=1}^{n} V_k = 0, \sum_{k=1}^{n} I_k = 0 \tag{4.1}$$

where V_k and I_k represent the voltage drops across the k^{th} component in a loop and the current leaving the k^{th} branch in a node, respectively. Their formalization is as follows:

Definition 4.2: *Kirchhoff's Voltage and Current Law*

$\vdash \forall$ `V t. kvl V t =`

  $(\sum_{k=0}^{LENGTH\ \ V-1}$ `(`λ`n.EL n V t) = 0)`

$\vdash \forall$ `V t. kcl I t =`

  $(\sum_{k=0}^{LENGTH\ \ I-1}$ `(`λ`n.EL n I t) = 0)`

The function `kvl` accepts a list V of functions of type (`real` $\rightarrow$ `complex`), which represents the behavior of time-dependant voltages in the given circuit and a time variable t as a *real* number. It returns the predicate that guarantees that the sum of all the voltages in the loop is zero. Similarly, the function `kcl` accepts a list I, which represents the behavior of time-dependant currents and a time variable t and returns the predicate that guarantees that the sum of all the currents leaving the node is zero. Here, `EL` is a HOL-Light function, which takes a list and a number n and returns the n^{th} element of the list. Similarly, `LENGTH` takes a list as the input and return a number representing the total number of elements in the list.

4.4 Verified Circuits

The proposed methodology can be applied to formally verify the s-domain transfer functions for a wide range of analog circuits. In order to illustrate the practical effectiveness and utilization of the proposed methodology for verifying real-world analog circuits, we present the verification of first and second-order Sallen-Key low-pass filters [31] and Linear Transfer Converter (LTC) circuit in this section.

4.4.1 Sallen-Key Low Pass Filters

Sallen-Key is one of the most widely used filter topologies [33] and Sallen-Key low pass filters are extensively being used in numerous applications, such as analog-to-digital converters, radio transmitters, audio crossover and telephone lines [12].

4.4.2 First-Order Sallen-Key Low Pass Filter

First-order Sallen-Key low-pass filter is shown in Figure (4.2). Its modeling differential equation and transfer function are as follows: [4]

$$R_1 C_1 \frac{dv_{out}(t)}{dt} + v_{out}(t) = v_{in}(t) \tag{4.2}$$

$$\frac{V_{out}(s)}{V_{in}(s)} = \frac{1}{R_1 C_1 s + 1} \tag{4.3}$$

By using our formal analog library definitions, the implementation model for

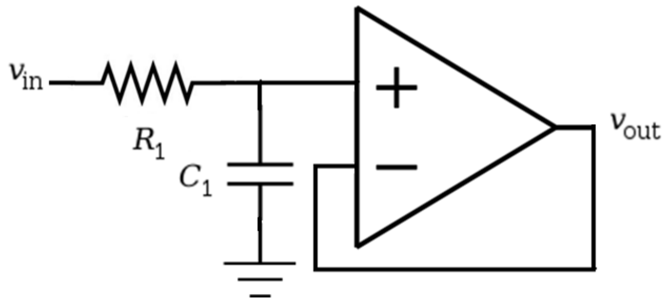

Figure 4.2: First-Order Sallen-Key Low-Pass Filter

the first-order low-pass filter is obtained as follows:

Definition 4.3: *Implementation of* 1^{st}*-order LP Filter*

```
⊢ ∀ R1 C1 Vin Vout Va.
  LP_imp R1 C1 Vin Vout Va =
   (∀t.  0 < t ⇒
    kcl [res_cur R1 (λt.  Vin t - Va t);
    cap_cur C1 (λt.  -Va t)] t) ∧
    (λt.  0 < t ⇒ Va t = Vout t)
```

where `Va` represents the voltage at non-inverting input of the op-amp in Figure 4.2. The first conjunct represents the node at the non-inverting input of the op-amp. In the given circuit, the op-amp is being used in the negative-feedback configuration. The second conjunct in the above definition represents this negative-feedback configured op-amp, which ensures that the voltage at the inverting input of op-amp is equal to the output voltage [28].

According to the proposed methodology, the next step is to formalize the differential equation and the required transfer function of the given first-order low-pass filter as follows:

Definition 4.4: *Differential Eq. Spec. of* 1^{st}*-order LP Filter*

```
⊢ ∀ R1 C1 Vin Vout y.
  LP_behav R1 C1 Vin Vout y =
   (diff_eq_lhs [λt.1; λt.R1 * C1] Vout 2 y =
      Vin y)
```

Definition 4.5: *Transfer Function Spec. of* 1^{st}*-order LP Filter*

```
⊢ ∀ R1 C1 Vin Vout s.
  first_order_tran_fun_spec R1 C1 Vin Vout s =
```

$$\left(\frac{laplace\ \ Vout\ \ s}{laplace\ \ Vin\ \ s} = \frac{1}{R1*C1*s+1} \right)$$

where the function `diff_eq_lhs` is used to formalize the left-hand-side (LHS) of a differential equation. It accepts a list corresponding to the coefficients of terms of differential equation, the differentiable function and the differentiation variable and returns the LHS of the equation in the summation form having individual terms as the product of coefficients and derivatives of the differentiable function with respect to the differentiation variable. Then, the following theorem representing the implication between the implementation and the formal differential equation specification can be verified:

Theorem 4.1: *Relationship between Implementation and Differential Eq. Spec.*

```
⊢ ∀ R1 C1 Vin Va Vout.(0 < R1) ∧ (0 < C1) ∧
  (∀t.  differentiable 1 Vout (at t)) ∧
  (∀t.  differentiable 1 Vin (at t)) ∧
  (LP_imp R1 C1 Vin Vout Va) ⇒
    (∀t.(0 < t) ⇒ LP_behav R1 C1 Vin Vout t)
```

In the above theorem, the first two assumptions ensure that the resistors and capacitors values in the given circuit must be greater than zero, which is the necessary condition for the circuits to exhibit the behavior of Equation 4.2. In the next two assumptions, the `differentiable` function is used to ensure the differentiability of the input, output and the nodal voltage of the circuit which is also a necessary condition. Note that we have not put the differentiability condition for `Va` as it is equal to the `Vout` according to the implementation. Finally, the last assumption represents the implementation model of the given circuit. The proof of Theorem 4.1 is based on the function definitions along with some multivariable arithmetic reasoning and is thus very straightforward.

Once, the modeling differential equation is formally verified, the following theorem is verified indicating the implication between differential equation and transfer function specification using formalized Laplace Transform Theory.

Theorem 4.2: *Relationship between Diff. Eq. and Transfer Function Spec.*

⊢ ∀ R1 C1 Vin Vout t s.(0 < R1) ∧ (0 < C1) ∧
  (∀t. differentiable 1 Vout (at t)) ∧
  (∀t. differentiable 1 Vin (at t)) ∧
  (laplace_exists_higher_deriv 1 Vout s) ∧
  (laplace_exists_higher_deriv 1 Vin s) ∧
  ($s \neq \frac{-1}{R1*C1}$) ∧ (laplace Vin s ≠ 0) ∧
  (∀t.(0 < t ⇒ LP_behav R1 C1 Vin Vout t) ∧
    ((t = 0) ⇒ Vin = 0 ∧ Vout = 0)) ⇒
  tf_spec R1 C1 Vin Vout s

Besides the assumptions, used in Theorem 4.1, the predicate `laplace_exists_higher_deriv` is used to ensure the Laplace transform existence of `Vin` and `Vout` and their first two derivatives as well for `s`, which indicates the frequency domain variable in our analysis. These conditions are necessary for the translation of Equation 4.2 to the s-domain [31]. The next assumption is used to avoid singularities in the transfer function and is also indicating the pole of the transfer function. Similarly, the next assumption represents the non-zero condition of the Laplace transform of the input voltage `Vin` [31]. Finally, the last assumption represents the differential equation of the given circuit. The above theorem is proved by using the functions and theorems of the formalized Laplace transform theory and multivariable calculus reasoning. This concludes the formal verification of the transfer function of the first-order Sallen-Key low-pass filter.

4.4.3 Second-Order Sallen-Key Low Pass Filter

Now, we will explain the verification of second-order Sallen-Key low-pass filter in detail. Second-order Sallen-Key low-pass filter is shown in Figure (4.3). The

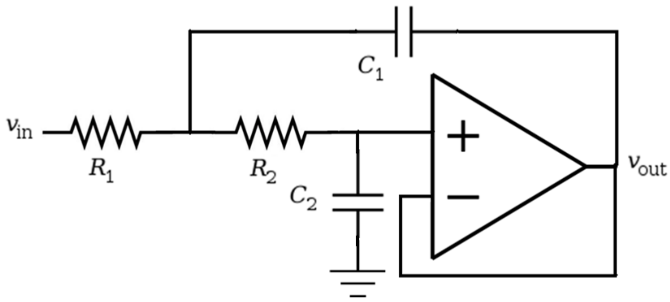

Figure 4.3: Second-Order Sallen-Key Low-Pass Filter

modeling differential equation and transfer function of the second-order low-pass filter are as follows: [31]

$$R_1C_1R_2C_2\frac{d^2v_{out}(t)}{dt^2} + C_2(R_1+R_2)\frac{dv_{out}(t)}{dt} + v_{out}(t) = v_{in}(t) \tag{4.4}$$

$$\frac{V_{out}(s)}{V_{in}(s)} = \frac{1}{R_1C_1R_2C_2s^2 + C_2(R_1+R_2)s + 1} \tag{4.5}$$

By using our formal analog library definitions, the implementation model for the second-order low-pass filter is obtained as follows:

Definition 4.6: *Implementation of* 2^{nd}*-order LP Filter*

```
⊢ ∀ R1 C1 R2 C2 Vin Vout Va Vb.
  LP_imp R1 C1 R2 C2 Vin Vout Va Vb =
   (∀t.  0 < t ⇒
    kcl[res_cur R1 (λt.Vin t - Va t);
    res_cur R2 (λt.-(Va t - Vb t));
    cap_cur C1 (λt.-(Va t - Vout t))] t ) ∧
   (∀t.  0 < t ⇒
    kcl [res_cur R2 (λt.Va t - Vb t);
    cap_cur C2 (λt.-Vb t)] t) ∧
   (∀t.  0 < t ⇒ Vb t = Vout t)
```

where `Va` represents the voltage at the node joining R1, R2 and C1 and `Vb` represents the voltage at non-inverting input of the op-amp in Figure 4.3. The first conjunct represents the node joining R1, R2 and C1 using the formalized KCL while the second conjunct represents the node at the non-inverting input of the op-amp. In the given circuit, the op-amp is being used in the negative-feedback configuration. The third conjunct in the above definition represents this negative-feedback configured op-amp, which ensures that the voltage at the inverting input of op-amp is equal to the output voltage [28].

According to the proposed methodology, the next step is to formalize the differential equation and the required transfer function of the given second-order low-pass filter as follows:

Definition 4.7: *Differential Eq. Spec. of 2^{nd}-order LP Filter*

```
⊢ ∀ R1 C1 R2 C2 Vout Vin y.
  LP_behav R1 C1 R2 C2 Vout Vin y =
   diff_eq_lhs [λt.1; λt.C2 * (R1 + R2);
   λt.R1 * C1 * R2 * C2] Vout 3 y = Vin y
```

Definition 4.8: *Transfer Function Spec. of 2^{nd}-order LP Filter*

$\vdash \forall$ `R1 C1 R2 C2 Vin Vout s.`

`tf_spec R1 C1 R2 C2 Vin Vout s`

$(\frac{laplace\ \ Vout\ \ s}{laplace\ \ Vin\ \ s} = \frac{1}{R1*C1*R2*C2*s^2+C2*(R1+R2)*s+1})$

The following theorem representing the implication between the implementation and the formal differential equation specification can be verified:

Theorem 4.3: *Relationship between Implementation and Differential Eq. Spec.*

$\vdash \forall$ `R1 C1 R2 C2 Vin Va Vb Vout.(0 < R1)` $\wedge$

`(0 < C1)` $\wedge$ `(0 < R2)` $\wedge$ `(0 < C2)` $\wedge$

`(`$\forall$`t. differentiable 2 Vout (at t))` $\wedge$

`(`$\forall$`t. differentiable 2 Vin (at t))` $\wedge$

`(`$\forall$`t. differentiable 2 Va (at t))` $\wedge$

`(LP_imp R1 C1 R2 C2 Vin Vout Va Vb)` $\Rightarrow$

`(`$\forall$`t.(0 < t)` $\Rightarrow$ `LP_behav R1 C1 R2 C2 Vin`

`Vout t)`

In the above theorem, the first four assumptions ensure that the resistors and capacitors values in the given circuit must be greater than zero, which is the necessary condition for the circuits to exhibit the behavior of Equation 4.4. In the next three assumptions, the `differentiable` function is used to ensure the differentiability of the input, output and the nodal voltage of the circuit which is also a necessary condition. Note that we have not put the differentiability condition for `Vb` as it is equal to the `Vout` according to the implementation. Finally, the last assumption represents the implementation model of the given circuit. The proof of Theorem 4.3 is based on the function definitions along with some multivariable arithmetic reasoning and is thus very straightforward.

Once, the modeling differential equation is formally verified, the following theorem is verified indicating the implication between differential equation and transfer function specification using formalized Laplace Transform Theory.

Theorem 4.4: *Relationship between Diff. Eq. and Transfer Function Spec.*

```
⊢ ∀ R1 C1 R2 C2 Vin Vout t s.(0 < R1) ∧
  (0 < C1) ∧ (0 < R2) ∧ (0 < C2) ∧
  (∀t. differentiable 2 Vout (at t)) ∧
  (∀t. differentiable 2 Vin (at t)) ∧
  (∀t. differentiable 2 Va (at t)) ∧
  (laplace_exists_higher_deriv 2 Vout s) ∧
  (laplace_exists_higher_deriv 2 Vin s) ∧
```

$(s \neq \frac{-C2*(R1+R2)+\sqrt{C2^2*(R1+R2)^2-4*R1*C1*R2*C2}}{2*R1*C1*R2*C2})$ $\wedge$

$(s \neq \frac{-C2*(R1+R2)-\sqrt{C2^2*(R1+R2)^2-4*R1*C1*R2*C2}}{2*R1*C1*R2*C2})$ $\wedge$

```
  (laplace Vin s ≠ 0) ∧ (∀t.(0 < t ⇒
    LP_behav R1 C1 R2 C2 Vin Vout t) ∧
    ((t = 0) ⇒ Vin = 0 ∧ Vout = 0)) ⇒
  tf_spec R1 C1 R2 C2 Vin Vout s
```

Besides the assumptions, used in Theorem 4.3, the predicate `laplace_exists_higher_deriv` is used to ensure the Laplace transform existence of `Vin` and `Vout` and their first two derivatives as well for `s`, which indicates the frequency domain variable in our analysis. These conditions are necessary for the translation of Equation 4.4 to the s-domain [31]. The next two assumptions are used to avoid singularities in the transfer function and are also indicating the poles of the transfer function. Similarly, the next assumption represents the non-zero condition of the Laplace transform of the input voltage `Vin` [31]. Finally, the last assumption represents the differential equation of the given circuit. The above theorem is proved by using the functions and theorems of the formalized Laplace transform theory and multivariable calculus reasoning. This concludes the formal verification of the transfer function of the second-order Sallen-Key low-pass filter.

4.4.4 Linear Transfer Converter (LTC) circuit

Linear Transfer Converter (LTC) circuit, depicted in Figure (4.4), is widely used for converting the voltage and current levels in power electronics systems [26]. 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 [19]. 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

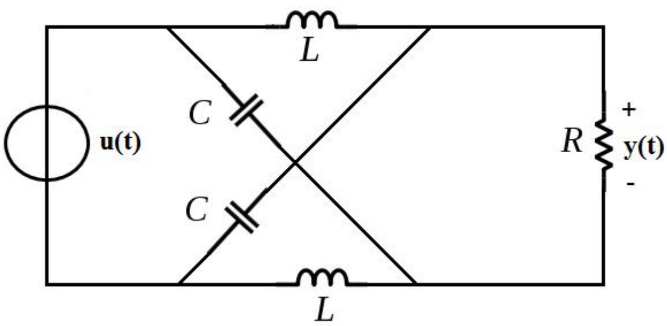

Figure 4.4: Linear Transfer Converter (LTC) Circuit

circuit, with input complex voltage $u(t)$ across the voltage generator, and the output complex voltage $y(t)$, across the resistor R, can be expressed using the following differential equation [3]:

$$\frac{d^2y}{dt^2} - \frac{2}{RC}\frac{dy}{dt} + \frac{1}{LC}y = \frac{d^2u}{dt^2} - \frac{1}{LC}u \tag{4.6}$$

The corresponding transfer function of this given circuit is as follows [3]:

$$\frac{Y(s)}{U(s)} = \frac{s^2 - \frac{1}{LC}}{s^2 - \frac{2s}{RC} + \frac{1}{LC}} \tag{4.7}$$

The objective of this section is to verify this transfer function using Equation (4.6). In order to be able to formally express Equation (4.6), we formalized the following function to model an n-order differential equation in HOL-Light:

Definition 4.9: *Differential Equation*

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

Now, Equation (4.6) can be formalized as follows:

Definition 4.10: *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 (4.6) in the summation form.

Now, the transfer function of the given LTC circuit, given in Equation (4.7), can be verified as the following theorem in HOL-Light.

Theorem 4.5: *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) ∧
∼((Cx(&1/(L*C)) - Cx(&2/(R*C))*s) + s pow 2 = Cx(&0) )∧
∼(laplace u s = Cx(&0)) ∧ (∀t.  diff_eq_LTC y u t L C R) ⇒
 (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 last assumption represents the formalization of Equation (4.6) and the conclusion of the theorem represents Equation (4.7). The reasoning about the correctness of Theorem 4.5 is very straightforward and is primarily based on Definition 3.1 and Theorem 3.6 and some simple arithmetic reasoning.

The usefulness of our proposed technique is that for verifying the transfer function of analog circuits using higher-order-logic theorem proving, the analog circuit designers do not need to go into the subtle details of the Laplace transform mathematics and they can easily formalize the transfer functions by using the already formalized Laplace transform definition and properties. The foundational Laplace transform and analog circuit library formalization 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. Utilizing this work, the proof script of corresponding to the Sallen-Key Low-pass filters verification consists of approximately 650 lines of HOL-Light code and the proof process took just a couple of hours, which clearly indicates the usefulness of our work. All of the assumptions have to be explicitly mentioned along with the theorems in order to prove them in HOL-Light. For instance, the positive values of the circuit components and differentiability of the voltages are often ignored in the analog circuit design literature [31] but has been explicitly indicated in our analysis. Similarly, the poles of the given circuit can also explicitly observed from the formally verified theorem.

4.5 Summary

We applied our formalized Laplace transform theory to develop a formal verification scheme for transfer functions of analog circuits as shown in Figure 4.1. Existing formal verification techniques employ model checking; however these provide inaccurate analysis because of inherent approximations involved in modeling the continuous behavior of analog circuits.

Chapter 5

Conclusions

This thesis 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 work 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 the formalization of Laplace transform theory, we are able to use the higher-order-logic theorem proving for verifying the transfer functions of analog circuits, which is an essential step in analog circuit design. We can formally model the structure of the given analog circuit and the differential equation depicting its behavior and by using the formalized Laplace transform theory, its transfer function can also be deduced within the sound core of theorem prover. Theorem proving captures the continuous nature of analog signals and their Laplace transform without introducing any discretization and thus providing the complete and most accurate form of verification. We have formally verified the transfer functions of low-pass Sallen-Key filters and LTC circuit which are commonly used electronic circuit in a very straightforward way

5.1 Future Work

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 [3]. Our formalization can also be used to formalize other mathematical transforms. For instance, Fourier transform [10], 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. Moreover, circuits whose transfer functions have been verified by our proposed technique can be added as formalized components in the Formalized Analog Library and then can be used to verify other circuits. For instance, the verified models of first and second-order Sallen-Key low-pass filters, presented in this paper, can be used to verify the transfer function of the third-order Sallen-Key low-pass filters.

References

[1] B. Akbarpour and L. C. Paulson. MetiTarski: An Automatic Prover for the Elementary Functions. In *Serge Autexier et al. (editors), Intelligent Computer Mathematics*, volume 5144 of *LNCS*, pages 217–231. Springer, 2008.

[2] H. Aridhi, M. H. Zaki, and S. Tahar. Towards Improving Simulation of Analog Circuits using Model Order Reduction. In *IEEE/ACM Design Automation and Test in Europe*, volume 1522 of *LNCS*, pages 1337–1342, 2012.

[3] R. J. Beerends, H. G. Morsche, J. C. Van den Berg, and E. M. Van de Vrie. *Fourier and Laplace Transforms.* Cambridge: Cambridge University Press, 2003.

[4] W. K. Chen. *Passive and Active Filters: Theory and Implementations.* Wiley, 1986.

[5] W. Denman, B. Akbarpour, S. Tahar, M. Zaki, and L. C. Paulson. Formal Verification of Analog Designs using MetiTarski. In *Formal Methods in Computer Aided Design*, pages 93–100. IEEE, 2009.

[6] C.A. Desoer and Kuh E.S. *Basic Circuit Theory.* McGraw-Hill, 1969.

[7] L. Dorcak, I. Petras, E. Gonzalez, J. Valsa, J. Terpak, and M. Zecova. Application of PID Retuning Method for Laboratory Feedback Control System Incorporating FO Dynamics. In *International Carpathian Control Conference (ICCC)*, pages 38–43. IEEE, 2013.

[8] G. Frehse. PHAVer: Algorithmic Verification of Hybrid Systems Past HyTech. In *Hybrid Systems: Computation and Control*, volume 3414 of *LNCS*, pages 258–273. Springer, 2005.

[9] G. Frehse, C. Le Guernic, A. Donzé, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, and O. Maler. Spaceex: Scalable Verification of Hybrid Systems. In *Computer Aided Verification*, volume 6806 of *LNCS*, pages 379–395. Springer, 2011.

[10] P. Gaydecki. *Foundations of Digital Signal Processing: Theory, Algorithms and Hardware Design*. IET, 2004.

[11] A. Ghosh and R. Vemuri. Formal Verification of Synthesized Analog Circuits. In *ACM/IEE International Conference on Computer Design*, volume 31, pages 40–45, 1999.

[12] A. P. Godse and U. A. Bakshi. *Analog Integrated Circuits - Design And Applications*. Technical Publications, 2009.

[13] S. Gupta, B.H. Krogh, and R.A. Rutenbar. Towards Formal Verification of Analog Designs. In *IEEE/ACM International Conference on Computer Aided Design*, pages 210–217, 2004.

[14] K. Hanna. Automatic Verification of Mixed-level Logic Circuits. In *IEEE International Conference on Formal Methods in Computer-Aided Design*, volume 1522 of *LNCS*, pages 133–166. Springer, 1998.

[15] K. Hanna. Reasoning about Analog Level Implementation of Digital Systems. *Formal Methods in System Design*, 16(2):127–158, 2000.

[16] J. Harrison. HOL Light: An overview. In *Proceedings of the 22nd International Conference on Theorem Proving in Higher Order Logics, TPHOLs 2009*, volume 5674 of *LNCS*, pages 60–66. Springer-Verlag, 2009.

[17] J. Harrison. The HOL Light Theory of Euclidean Space. *Automated Reasoning*, 50(2):173–190, 2013.

[18] M. H.Zaki, S. Tahar, and G. Boisr. Formal Verification of Analog and Mixed Signal Designs: A survey. In *Microelectronics Journal*, volume 39, pages 1395–1404. Elsevier, 2008.

[19] A. Ioinovici. *Power Electronics and Energy Conversion Systems, Fundamentals and Hard-switching Converters.* John Wiley & Sons, 2013.

[20] S. Little, D. Walter, N. Seegmiller, C.J. Myers, and T. Yoneda. Verification of Analog and Mixed-Signal Circuits using Timed Hybrid Petri Nets. In *Automated Technology for Verification and Analysis*, volume 3299 of *LNCS*, pages 426–440. Springer, 2004.

[21] D. A. Meador. *Analog Signal Processing with Laplace Transforms and Active Filter Design.* Delmar, 2002.

[22] R. Narayanan, B. Akbarpour, M. H. Zaki, S. Tahar, and L. C. Paulson. Formal Verification of Analog Circuits in the Presence of Noise and Process Variation. In *Design, Automation and Test in Europe*, pages 1309–1312, 2010.

[23] B. Paul. *Industrial Electronics and Control.* PHI Learning Pvt. Ltd., 2004.

[24] L.C. Paulson. *ML for the Working Programmer.* Cambridge University Press, Cambridge, 1996.

[25] I. Podlubny. The Laplace Transform Method for Linear Differential Equations of the Fractional Order. Technical report, Slovak Acad. Sci., Kosice, 1994.

[26] M. Rashid. *Power Electronics Handbook*. Elsevier, 2011.

[27] J.L. Schiff. *The Laplace Transform: Theory and Applications*. Springer, 1999.

[28] A. S. Sedra and K. C. Smith. *Microelectronic Circuits*. Oxford University Press, 2004.

[29] S. Seshadri and J.A. Abraham. Frequency Response Verification of Analog Circuits using Global Optimization Techniques. pages 395–408, 2001.

[30] A. Ucar, E. Cetin, and I. Kale. A Continuous-Time Delta-Sigma Modulator for RF Subsampling Receivers. In *IEEE Transactions on Circuits And Systems*, pages 272 – 276. IEEE, 2012.

[31] M. E. Valkenburg. *Analog Filter Design*. John Wiley & Sons, 1982.

[32] J.R. Westra, C.J.M. Verhoeven, and A.H.M. van Roermund. *Oscillators and Oscillator Systems: Classification, Analysis and Synthesis*. Springer, 1999.

[33] W.Jung. *Op Amp Applications Handbook*. Newnes, 2004.

[34] J. Xiao. *Integral and Functional Analysis*. Nova Publishers, 2008.

[35] X. Yang. *Mathematical Modeling with Multidisciplinary Applications*. John Wiley & Sons, 2013.

[36] M.H. Zaki, S. Tahar, and G. Bois. Formal Verification of Analog and Mixed Signal Designs: A Survey. *Microelectronics Journal*, 39(12):1395–1404, 2008.