Contents lists available at ScienceDirect

Journal of Systems Architecture

journal homepage: www.elsevier.com/locate/sysarc

Formal analysis of the continuous dynamics of cyber–physical systems using theorem proving

Adnan Rashid *, Osman Hasan

School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan

ARTICLE INFO

Keywords:
Transform methods
Laplace transform
Fourier transform
Cyber–physical systems
Formal analysis
Higher-order logic
Theorem proving
HOL Light

ABSTRACT

Transform methods, such as the Laplace and the Fourier transforms, are widely used for analyzing the continuous dynamics of the physical components of Cyber–physical Systems (CPS). Traditionally, the transform methods based analysis of CPS is conducted using paper-and-pencil proof methods, computer-based simulations or computer algebra systems. However, all these methods cannot capture the continuous aspects of physical systems in their true form and thus unable to provide a complete analysis, which poses a serious threat to the safety of CPS. To overcome these limitations, we propose to use higher-order-logic theorem proving to reason about the dynamical behavior of CPS, based on the Laplace and the Fourier transforms, which ensures the absolute accuracy of this analysis. For this purpose, this paper presents a higher-order-logic formalization of the Laplace and the Fourier transforms, including the verification of their classical properties and uniqueness. This formalization plays a vital role in formally verifying the solutions of differential equations in both the time and the frequency domain and thus facilitates formal dynamical analysis of CPS. For illustration, we formally analyze an industrial robot and an equalizer using the HOL Light theorem prover.

1. Introduction

Cyber–physical Systems (CPS) [1,2] are engineered systems involving a cyber component that controls the physical components. The cyber elements include embedded systems and network controllers, which are usually modeled as discrete events. Whereas, the physical components exhibit continuous dynamics, such as the physical motion of a robot in space or the working of an analog circuit, and are commonly modeled using the differential equations. CPS are widely used in advanced automotive systems (autonomous vehicles and smart cars), avionics, medical systems and devices, industrial process control [3], smart grids, traffic safety and control, robotics and telecommunication networks etc. For example, the smart (self-driving) cars are considered as the highly complex autonomous CPS composed of an array of sensors and actuators that interact with the external environment, like the road infrastructures and often internet.

To study the continuous dynamical behavior of the physical components of these CPS, their differential equation based models need to be analyzed. Transform methods [4], which include the Laplace [5] and the Fourier [6] transforms, are widely used for analyzing these differential equation based models. These transform methods are the integral based techniques, which convert a time varying function to its corresponding frequency domain representation, i.e., s and ω-domain representations based on the Laplace and the Fourier transforms, respectively. Moreover, this transformation converts the integral and differential operators in the time domain (differential equation) models to their corresponding algebraic operators, namely, division and multiplication, in the frequency domain and thus makes the arithmetic manipulation of the resulting equations quite straightforward. These algebraic expressions corresponding to the differential equations can further be used to perform the transfer function and the frequency response analysis of these systems. The Laplace transform is used for analyzing the systems with causal input, whereas, in the case of systems with non-causal input, the Fourier transform is used.

The conventional techniques for analyzing the continuous dynamics of CPS include paper-and-pencil proofs, computer-based numerical methods or symbolic techniques. However, these techniques suffer from their inherent limitations, like human-error proneness in the case of paper-and-pencil proofs, discretization and numerical errors in the case of numerical methods and the usage of unverified simplification algorithms in symbolic tools [7] and thus cannot ensure absolute accuracy of the corresponding analysis. Due to the safety critical-nature of CPS, accuracy of analyzing their continuous dynamics is becoming a dire need. For example, the fatal crash of Uber's self-driving car in March 2018 that killed a pedestrian in Tempe, Arizona, USA was found to be

* Corresponding author.
E-mail addresses: adnan.rashid@seecs.nust.edu.pk (A. Rashid), osman.hasan@seecs.nust.edu.pk (O. Hasan).

https://doi.org/10.1016/j.sysarc.2020.101850
Received 26 February 2020; Received in revised form 13 June 2020; Accepted 2 August 2020

caused by the sensor's anomalies [8]. A more rigorous analysis of CPS could have avoided this incident.

Formal methods [9] have been used to overcome the above-mentioned inaccuracy limitations for analyzing the continuous dynamics of CPS. There are mainly two types of formal methods, i.e., model checking [10] and higher-order-logic theorem proving [11] that can be used in this context. Model checking involves the development of a state–space based model of the underlying system and the formal verification of its intended properties that are specified in temporal logic. It has been used (e.g., [10,12,13]) for analyzing the continuous dynamics (differential equation based models) of CPS. However, this kind of analysis involves the discretization of the differential equations based models and thus compromises the accuracy of the corresponding analysis. Moreover, it also suffers from the state–space explosion problem [14]. Higher-order-logic theorem proving [11] is a computer based mathematical analysis technique that requires developing a mathematical model of the given system in higher-order logic and the formal verification of its intended behavior as a mathematically specified property based on mathematical reasoning within the sound core of a theorem prover. The involvement of the formal model and its associated formally specified properties along with the sound nature of theorem proving ascertains the accuracy and completeness of the analysis. Based on the same motivation, the Laplace transform has been formalized in the HOL Light theorem prover and it has been utilized to conduct the transfer function analysis of the Linear Transfer Converter (LTC) circuit [15], Sallen–Key low-pass filters [16], Unmanned Free-swimming Submersible (UFSS) vehicle [17] and a platoon of the automated vehicles [18]. Similarly, the Fourier transform [6] has also been formalized in the same theorem prover and has been successfully utilized for the frequency response analysis of an Automobile Suspension System (ASS) [19], Microelectromechanical Systems (MEMs) accelerometer [20] and an audio equalizer [20]. However, both of these formalizations can only provide the frequency domain (s or ω-domain) analysis of these systems. To relate the s-domain analysis of CPS to their corresponding time domain models, i.e., linear differential equations models, we have recently formalized Lerch's theorem, which provides the uniqueness of the Laplace transform and utilized it for the formal analysis of 4-π soft error crosstalk model for the Integrated Circuits (ICs) [21].

In this paper, we further extend our formalization of transform methods in higher-order logic [17,19–21] with the formal verification of the uniqueness of the Fourier transform, which plays a vital role in solving the linear differential equations in the ω-domain and thus relates the ω-domain analysis of the continuous dynamics of CPS to their corresponding time-domain analysis (linear differential equations based models), which was not possible with our earlier formalization of the Fourier transform. Thus, it can be utilized to completely analyze the differential equation based models of CPS with non-causal input. Moreover, based on our contributions of formalizations of the Laplace and the Fourier transforms, we also propose a framework to analyze the continuous dynamics of CPS in this paper. For illustration, we utilize our proposed framework for formally analyzing the continuous dynamics of some widely used physical components of CPS, i.e., a positional controller of an industrial robot and an equalizer used in telecommunication, using HOL Light.

The main contributions of this paper are as follows:

- *Formalization of the Uniqueness of the Fourier Transform:* The formal verification of the uniqueness of the Fourier transform, which plays a vital role in solving the linear differential equations in the ω-domain and thus relates the ω-domain analysis of the continuous dynamics of CPS to their corresponding time domain analysis.
- *A Novel Framework to analyze the continuous dynamics of CPS:* Based on our contributions of formalizations of the Laplace and the Fourier transforms, we propose a novel framework to formally analyze the continuous dynamics of CPS.
- *Formal Analysis of an Industrial Robot and an Equalizer:* We utilize our proposed framework for formally analyzing the continuous dynamics of some widely used physical components of CPS, i.e., a positional controller of an industrial robot and an equalizer used in telecommunication.
- *Tactics for Automating the Proofs/Analysis*: We develop tactics for automating the formal analysis of an industrial robot and an equalizer. Similar tactics can be developed for the formal analysis of most of the real-world systems. This fact makes the proposed framework quite interesting from the practical point of view as the expressiveness of higher-order-logic theorem proving can be benefited from without the overwhelming task of manually guiding the proof process.

The rest of the paper is organized as follows: We provide some related work regarding formal analysis of the continuous dynamics of CPS in Section 2. Section 3 presents a brief introduction about theorem proving, the HOL Light theorem prover and the multivariable calculus theories of HOL Light, which act as preliminaries for the proposed transform methods based analysis of CPS. Section 4 provides the proposed framework for analyzing the continuous dynamics of CPS. We describe the formalizations of the Laplace and the Fourier transforms in Section 5. Section 6 provides the formal verification of the uniqueness of the Fourier transform, which enables us to completely analyze the continuous dynamics of CPS. Section 7 presents our formal analysis of the industrial robot and the equalizer. Finally, Section 8 concludes the paper.

2. Related work

Model checking has been used for performing the dynamical analysis of CPS. Akella et al. [12] provided an approach, based on process algebra and model checking, for analyzing the physical components of CPS. The authors modeled the continuous dynamics of CPS as an event-based discrete system using the process algebra and formally verified the Bisimulation-based Non Deducibility on Compositions (BNDC) properties using the CoPS model checker. Similarly, Clarke et al. [10] used statistical model checking for the formal analysis of CPS. Their proposed approach is based on developing the stochastic state–space model of the system and its certification using the properties expressed in Bounded Linear Temporal Logic (BLTL). However, it involves sampling the continuous dynamical behavior of the system. Bu et al. [22] proposed a hybrid model checking approach for formally analyzing CPS. It involves sampling the numeric values of various state-parameters and development of a hybrid system model based on these values. It also provides the verification of the time-bounded behavior of the system in short-run future only, instead of the long-run behavior, thus ensuring a considerable reduction in the state–space. Recently, Sardar et al. [13] used the probabilistic model checker PRISM to formally model the continuous dynamics of the robotic cell injection systems. However, their proposed approach involves the discretization of the differential equations based models to obtain the corresponding state–space model of the underlying system. Model checking can provide the automatic analysis of the dynamical behavior of CPS. However, as evident from the above-mentioned works, it cannot model the continuous dynamics of their physical components in their true form. Also, it suffers from the state–space explosion problem, which poses questions on the scalability of this technique.

Theorem proving can overcome the above-mentioned limitations and can thus provide a rigorous analysis of the continuous dynamics of the physical components of CPS. KeYmaera, i.e., a theorem prover for formally analyzing the hybrid systems, has been widely used for analyzing the continuous dynamics of CPS. Platzer et al. [23] developed an algorithm for the verification of the safety properties of CPS. The authors used the notion of continuous generalization of induction to compute the differential invariants, which do not require solving the differential equations capturing the dynamics of CPS. Moreover, they used their proposed algorithm for formally verifying the collision avoidance properties in car controls and aircraft roundabout maneuvers [24] using KeYmaera. Similarly, Platzer et al. [25] verified the safety, controllability, liveness, and reactivity properties of the European Train Control System (ETCS) protocol using KeYmaera. KeYmaera has also been widely used for the dynamical analysis of various CPS, such as a distributed car control system [26], freeway traffic control [27], autonomous robotic vehicles [28] and industrial airborne collision avoidance system [29]. All these analysis performed using KeYmaera are based on the differential dynamics logic, which captures both the continuous and discrete dynamics of CPS and their interaction. This logic allows the suitable automation of the verification process as well. However, it is a first-order logic based modeling [30], which lacks the expressiveness and thus involves abstractions of the formal models of the underlying systems.

Higher-order logic theorem proving has also been used for formally analyzing the dynamics of CPS. Bernardeschi et al. [31] proposed a framework, based on the integration of PVS theorem prover and Simulink, for formally analyzing CPS. The authors used PVS for the formal verification of the discrete system components of CPS, whereas the continuous processes are analyzed using the Simulink based models. Thus, the continuous dynamics of CPS were only validated using simulations in their proposed framework. Similarly, Sanwal et al. [32] used HOL4 to formally analyze the continuous models of CPS. The authors formalized the solutions of second-order homogeneous linear differential equations, which restricts the utilization of their proposed approach for analyzing systems up to second-order only. Therefore, none of the works based on theorem proving, provides the transform methods based analysis of the continuous dynamics of CPS, which is the main scope of this paper.

Transform methods are formalized using various higher-order-logic theorem provers and have been used for formally analyzing the control and signal processing components of CPS. Taqdees et al. [15] formalized the Laplace transform using multivariate calculus theories of HOL Light. Moreover, the authors utilized their formalization of the Laplace transform for formally verifying the transfer function of the Linear Transfer Converter (LTC) circuit. Next, the authors extended their framework by providing a support to formally reason about the linear analog circuits, such as Sallen–Key low-pass filters [16] by formalizing the system governing laws, such as Kirchhoff's Current Law (KCL) and Kirchhoff's Voltage Law (KVL) using HOL Light. Later, Rashid et al. [33] proposed a new formalization of the Laplace transform based on the notion of sets and used it for formally analyzing the control system of the Unmanned Free-swimming Submersible (UFSS) vehicle [17] and 4-π soft error crosstalk model [21]. The Laplace transform [34–36] has also been formalized in Isabelle, HOL4 and Coq theorem provers. Similarly, Rashid et al. [19] formalized the Fourier transform in HOL Light and used it to formally analyze an Automobile Suspension System (ASS), an audio equalizer, a drug therapy model and a MEMs accelerometer [37]. However, all these formalizations can only provide the frequency domain (s or ω-domain) analysis of the corresponding systems.

To perform the transfer function based analysis of the discrete-time systems, Siddique et al. [38] formalized z-transform using HOL Light and used it for the formal analysis of Infinite Impulse Response (IIR) Digital Signal Processing (DSP) filter. Later, the authors extended their proposed framework by providing the formal support for the inverse z-transform and used it for formally analyzing a switched-capacitor interleaved DC–DC voltage doubler [39]. Similarly, Shi et al. [40] formalized discrete Fourier transform using HOL4 theorem prover and formally verified Fast Fourier Transform (FFT) algorithms. Recently, Guan et al. [41] presented some foundational formalization of the continuous Fourier transform using HOL4 and used it for performing the frequency domain analysis of a RLC circuit. However, the authors have only verified the linearity, frequency shifting, differentiation and integration properties of the Fourier transform. Moreover, their proposed approach only provides the frequency domain analysis of CPS. However, our formalization of the transform methods provides the formal verification of some more properties, in particular, the uniqueness of the Fourier transform, which enables us to perform the time-domain analysis of the continuous dynamics of CPS, which is not possible due to the unavailability of the uniqueness of the Fourier transform in its formalization in HOL4.

3. Preliminaries

This section presents some introduction about theorem proving, the HOL Light theorem prover and the multivariate calculus theories of HOL Light, which are required for the understanding of the rest of the paper.

3.1. *Theorem proving and HOL Light*

Theorem proving [11] involves constructing the mathematical proofs using a computer program based on axioms and hypothesis. Based on the decidability or undecidability of the underlying logic, i.e., propositional or higher-order logic, theorem proving can be automatic or interactive, respectively. Every theorem prover comes with a set of axioms and inference rules, which, along with the already verified theorems, are the only ways to prove the new theorems. This purely deductive feature ensures soundness, i.e., every sentence proved in the system is actually true. HOL Light consists of a rich set of formalized theories of the multivariable calculus, i.e., integration, differential, topology, transcendental, L_p spaces and vector calculus theories. The availability of these theories was the main motivation for choosing HOL Light for the proposed formalization as these foundations are required for preforming the transform methods based analysis of CPS.

3.2. *Multivariate calculus theories of HOL Light*

A N-dimensional vector is represented as a $\mathbb{R}^N$ column matrix with each of its element representing a real number in HOL Light [42]. All of the vector operations are thus performed using matrix manipulations. A complex number is defined as a 2-dimensional vector, i.e., a $\mathbb{R}^2$ column matrix or the data-type $\mathbb{C}$, in HOL Light. All of the theorems of multivariable calculus theories in HOL Light are verified for functions with an arbitrary data-type $\mathbb{R}^N \rightarrow \mathbb{R}^M$.

Some of the frequently used HOL Light functions in our proposed analysis are described below:

Definition 3.1. Cx and ii

$\vdash_{def}$ ∀a. Cx a = complex (a, &0)
$\vdash_{def}$ ii = complex (&0, &1)

The HOL Light function Cx type casts a real number ($\mathbb{R}$) to its corresponding complex number ($\mathbb{C}$). Also, the & operator type casts a natural number ($\mathbb{N}$) to its corresponding real number ($\mathbb{R}$). Similarly, the function ii (iota) represents a complex number having the real part equal to zero and the magnitude of the imaginary part equal to 1.

Definition 3.2. Re, Im, lift and drop

$\vdash_{def}$ ∀z. Re z = z$1
$\vdash_{def}$ ∀z. Im z = z$2
$\vdash_{def}$ ∀x. lift x = (lambda i. x)
$\vdash_{def}$ ∀x. drop x = x$1

The functions Re and Im take a complex number and return its real and imaginary parts, respectively. Here, the notation z$i represents the ith component of the vector z. The function lift maps a variable of type $\mathbb{R}$ to a 1-dimensional vector ($\mathbb{R}^1$) with the input variable as the only component. It uses the lambda operator for constructing a vector from its components in HOL Light [42]. Similarly, drop accepts a 1-dimensional vector and returns its single element as a real number. In order to make the understanding of functions lift and drop easier for a non-HOL user, we use symbols $\bar{\mathsf{t}}$ and $\underline{\mathsf{t}}$ for the functions lift t and drop t, respectively, in this paper.

Definition 3.3. Exponential, Complex Cosine and Sine
$\vdash_{def}$ ∀x. exp x = Re (cexp (Cx x))
$\vdash_{def}$ ∀z. ccos z = $\dfrac{\text{cexp (ii} * \text{z)} + \text{cexp (-ii} * \text{z)}}{\text{Cx (\&2)}}$
$\vdash_{def}$ ∀z. csin z = $\dfrac{\text{cexp (ii} * \text{z)} - \text{cexp (-ii} * \text{z)}}{\text{Cx (\&2)} * \text{ii}}$

The HOL Light functions cexp : $\mathbb{C} \to \mathbb{C}$ and exp : $\mathbb{R} \to \mathbb{R}$ represent the complex and real exponential functions, respectively. Similarly, the complex cosine and sine functions are modeled as ccos and csin in terms of cexp using the Euler's formula, respectively [42].

Definition 3.4. Vector and Real Integrals
$\vdash_{def}$ ∀f i. integral i f = (@y. (f has_integral y) i)
$\vdash_{def}$ ∀f i. real_integral i f = (@y. (f has_real_integral y) i)

The function integral models the vector integral and is defined using the Hilbert choice operator @ in the functional form. It accepts the integrand function f : $\mathbb{R}^N \to \mathbb{R}^M$ and a vector-space i : $\mathbb{R}^N \to \mathbb{B}$, which defines the region of convergence as $\mathbb{B}$ represents the Boolean data type, and returns a vector $\mathbb{R}^M$, which is the integral of f on i. The function has_integral represents the same relationship in the relational form. Similarly, the function real_integral models the real integral. It takes the integrand function f : $\mathbb{R} \to \mathbb{R}$ and a set of real numbers i : $\mathbb{R} \to \mathbb{B}$ and returns the real integral of the function f over i.

Definition 3.5. Vector Derivative
$\vdash_{def}$ ∀f net. vector_derivative f net =
(@f′. (f has_vector_derivative f′) net)

The function vector_derivative accepts a function f, having type $\mathbb{R}^1 \to \mathbb{R}^M$, and a net : $\mathbb{R}^1 \to \mathbb{B}$, which defines the point at which f has to be differentiated, and 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.

4. Proposed framework

The proposed framework for the transform methods based analysis of the physical aspects of CPS using HOL Light theorem prover is depicted in Fig. 1. In the first step of the analysis, our framework accepts the differential equation, which models the dynamics of the underlying system and the type of the input, i.e., causal or non-causal, from the user. The given differential equation is transformed to the corresponding model in higher-order logic. Next, we have to verify the required properties of the underlying system, which are usually expressed in terms of a transfer function, frequency response, and the time and frequency domain solutions of differential equations. To carry out the verification process of these properties, we developed a library of the transform methods, i.e., the theories of the Laplace and the Fourier transforms using the multivariate calculus theories of HOL Light. These theories include the formal definitions of the Laplace and the Fourier transforms, and the formal verification of various classical properties of the Laplace and the Fourier transforms, i.e., linearity, frequency shifting, time shifting, time scaling, time reversal, differentiation, integration, modulation and the uniqueness properties. Thus, the user can utilize the appropriate transform methods (Laplace or Fourier) based on the type of the system's input, i.e., the Laplace transform is used for the inputs that are described as a causal function and the Fourier transform is used in the case of a non-causal input to the underlying system.

5. Formalization of transform methods

In this section, we provide the formalization of the transform methods using the HOL Light theorem prover.

5.1. Formalization of the Laplace transform

5.1.1. Formal definition of the Laplace transform

The Laplace transform for a function $f : \mathbb{R}^1 \to \mathbb{C}$ is mathematically defined as [4]:

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

where s is a complex variable. The limit of integration is from 0 to ∞. We formalize Eq. (1) in HOL Light as [21]:

Definition 5.1. Laplace Transform
$\vdash_{def}$ ∀s f. laplace_transform f s =
integral {t | &0 ≤ $\underline{\mathsf{t}}$} (λt. cexp (-(s ∗ Cx $\underline{\mathsf{t}}$)) ∗ f t)

The function laplace_transform in the above definition, accepts a complex-valued function f : $\mathbb{R}^1 \to \mathbb{C}$ and a complex number s : $\mathbb{C}$ and returns the Laplace transform of f as represented by Eq. (1). Since the return data-type of the function f is $\mathbb{C}$, therefore, we used the complex exponential function cexp : $\mathbb{C} \to \mathbb{C}$. Moreover, t is a 1-dimensional vector, i.e., having type $\mathbb{R}^1$, and to multiply it with s : $\mathbb{C}$, it is first converted into a real number $\underline{\mathsf{t}}$ by using the HOL Light function drop (Definition 3.2) and then it is converted to data-type $\mathbb{C}$ using Cx (Definition 3.1). Next, we use the vector function integral (Definition 3.4) to integrate the expression $f(t)e^{-st}$ over the positive real line since the data-type of this expression is $\mathbb{C}$. The region of the integration, i.e., the positive real line, is represented in HOL Light as {t | &0 ≤ $\underline{\mathsf{t}}$}.

The Laplace transform of a function f exists, if f is piecewise smooth and is of exponential order on the positive real line [4]. A function is said to be piecewise smooth on an interval if it is piecewise differentiable on that interval. We model the Laplace existence condition in HOL Light as [21]:

Definition 5.2. Laplace Existence
$\vdash_{def}$ ∀s f. laplace_exists f s ⇔
(∀b. f piecewise_differentiable_on interval [$\underline{\mathsf{\&0}}$,$\underline{\mathsf{b}}$]) ∧
(∃M a. Re s > $\underline{\mathsf{a}}$ ∧ exp_order_cond f M a)

The function exp_order_cond captures the exponential order condition required for the existence of the Laplace transform [4] and is formalized as [15,21]:

Definition 5.3. Exponential Order Condition
$\vdash_{def}$ ∀f M a. exp_order_cond f M a ⇔
&0 < M ∧ (∀t. &0 ≤ t ⇒ ||f $\bar{\mathsf{t}}$|| ≤ M ∗ exp ($\underline{\mathsf{a}}$ ∗ t))
where $\|\vec{x}\|$ represents the norm of the vector $\vec{x}$.

5.1.2. Formally verified properties of the Laplace transform

We used the definitions, given in Section 5.1.1 to formally verify some of the classical properties of the Laplace transform, namely linearity, time shifting, frequency shifting, cosine and sine-based modulations, time scaling, integration in time-domain, differentiation in time domain and transfer function of a n-order system, given in Table 1. The assumptions of these theorems express the conditions for the existence of the corresponding Laplace transforms. For example, the predicate laplace_exists_higher_deriv in the theorem corresponding to the higher-order differentiation ensures that the Laplace transform of all the derivatives up to the order n of the function f exist. Similarly, the predicate differentiable_higher_derivative of the same theorem presents the differentiability of the function f and its higher derivatives up to the nth order [21]. The verification of these properties not only

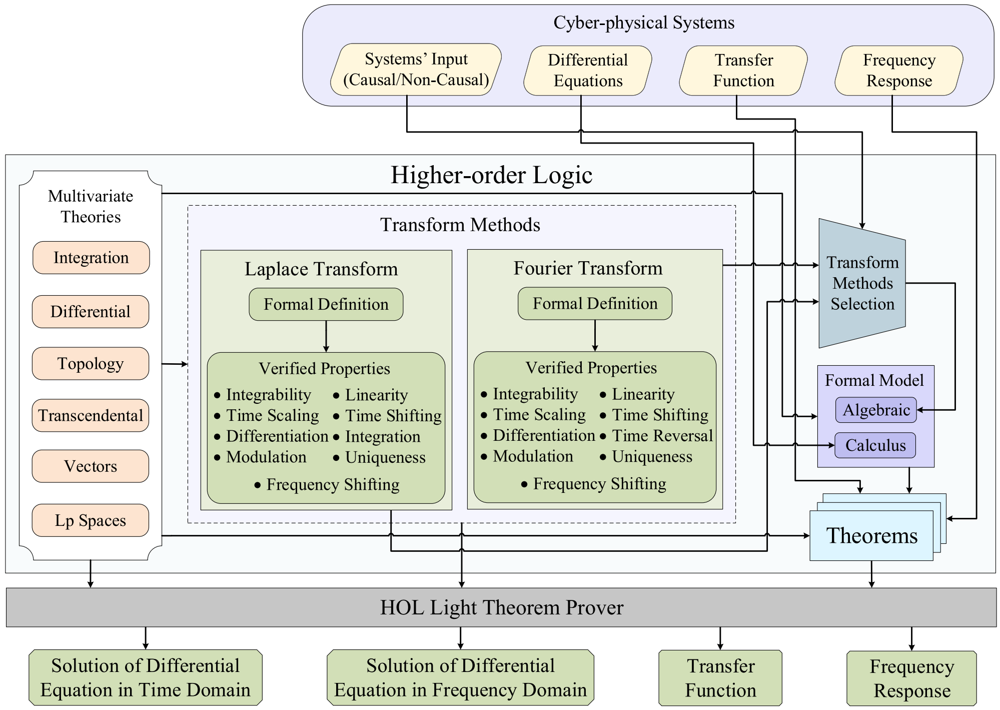

Fig. 1. Proposed Framework.

ensures the correctness of our definitions, presented in Section 5.1.1, but also plays a vital role in minimizing the user effort in reasoning about the Laplace transform based analysis of systems, as will be depicted in Section 7.1 of the paper.

5.1.3. *Uniqueness of the Laplace transform*

The section presents the formal proof of Lerch's theorem, which represents the uniqueness of the Laplace transform.

If Eq. (1) is satisfied by a continuous function f, then there exists no continuous function other than f that satisfies Eq. (1). This statement can alternatively be interpreted by assuming that there is another continuous function g, which satisfies the following condition:

$$\mathcal{L}[g(t)] = G(s) = \int_0^{\infty} g(t)e^{-st}dt, \qquad Re\ s \geq \gamma \tag{2}$$

and if $\mathcal{L}[f(t)] = \mathcal{L}[g(t)]$, then both functions f and g are the same, i.e., $f(t) = g(t)$ for all $0 \leq t$ [43,44].

We formally verify the statement of Lerch's theorem in HOL Light as [21]:

Theorem 5.1. *Lerch's Theorem*
$\vdash_{thm}$ ∀f g r.
  [A1] &0 < Re r ∧
  [A2] (∀s. Re r ≤ Re s ⇒ laplace_exists f s) ∧
  [A3] (∀s. Re r ≤ Re s ⇒ laplace_exists g s) ∧
  [A4] (∀s. Re r ≤ Re s ⇒ laplace_transform f s =
      laplace_transform g s)
    ⇒ (∀t. &0 ≤ t ⇒ f t = g t)

where f and g are complex-valued functions. Similarly, r and s are complex variables. The assumption A1 of the above theorem describes the non-negativity of the real part of the Laplace variable r. The assumptions A2--A3 present the Laplace existence conditions for functions f and g, respectively. The assumption A4 provides the condition that the Laplace transforms of the two functions f and g are equal. Finally, the conclusion models the equivalence of functions f and g for all values of their argument t in $0 \leq t$ since t represents time that is always non-negative. The verification of Theorem 5.1 is mainly based on the properties of sets, vectors, integrals and L^p spaces along with some real arithmetic reasoning [21].

5.2. *Formalization of the Fourier transform*

5.2.1. *Formal definition of the Fourier transform*

The Fourier transform of a function $f : \mathbb{R}^1 \rightarrow \mathbb{C}$ is mathematically defined as [19,20]:

$$\mathcal{F}[f(t)] = F(\omega) = \int_{-\infty}^{+\infty} f(t)e^{-i\omega t}dt, \ \omega \in \mathbb{R} \tag{3}$$

where ω is a real variable. The limit of integration is from $-\infty$ to $+\infty$. We formalize Eq. (3) in HOL Light as [20]:

Definition 5.4. Fourier Transform
$\vdash_{def}$ ∀w f. fourier_transform f w =
    integral UNIV (λt. cexp (-((ii ∗ Cx w) ∗ Cx t̲)) ∗ f t)

The function fourier_transform in the above definition takes a complex-valued function f and a real number w and returns the Fourier transform of f as represented by Eq. (3). The region of the integration, i.e., the whole real line is represented in HOL Light as UNIV : $\mathbb{R}^1$.

The Fourier transform of a function f exists if f is piecewise smooth and is absolutely integrable on the whole real line [4]. We formalize the Fourier existence condition in HOL Light as [19,20]:

Definition 5.5. Fourier Exists
$\vdash_{def}$ ∀f. fourier_exists f ⇔
    (∀a b. f piecewise_differentiable_on interval [a̅, b̅]) ∧
    f absolutely_integrable_on UNIV

In the above function, the first conjunct provides the piecewise smoothness condition for the function f. Whereas, the second conjunct expresses the absolute integrability of the function f on the whole real line.

Table 1
Properties of Laplace transform [21].

Mathematical Form	Formalized Form
Linearity	
$\mathcal{L}[\alpha f(t) + \beta g(t)] = \alpha F(s) + \beta G(s)$	$\vdash_{thm}$ ∀f g s a b. [A1] laplace_exists f s ∧ [A2] laplace_exists g s ⇒ laplace_transform (λt. a ∗ f t + b ∗ g t) s = a ∗ laplace_transform f s + b ∗ laplace_transform g s
Time Shifting	
$\mathcal{L}\left[f(t-t_0)u(t-t_0)\right] = e^{-t_0 s}F(s)$	$\vdash_{thm}$ ∀f s t0. [A1] &0 < t0 ∧ [A2] laplace_exists f s ⇒ laplace_transform (shifted_fun f t0) s = cexp (-(s ∗ Cx t0)) ∗ laplace_transform f s
Frequency Shifting	
$\mathcal{L}[e^{s_0 t}f(t)] = F(s-s_0)$	$\vdash_{thm}$ ∀f s s0. [A] laplace_exists f s ⇒ laplace_transform (λt. cexp (s0 ∗ Cx t) ∗ f t) s = laplace_transform f (s - s0)
Modulation (Cosine and Sine Based Modulation)	
$\mathcal{L}\left[f(t)cos(s_0 t)\right] = \dfrac{F(s-s_0)}{2} + \dfrac{F(s+s_0)}{2}$	$\vdash_{thm}$ ∀f s s0. [A] laplace_exists f s ⇒ laplace_transform (λt. ccos (s0 ∗ Cx t) ∗ f t) s = $\dfrac{\text{laplace\_transform f } (s - s0)}{\text{Cx}(\&2)} + \dfrac{\text{laplace\_transform f } (s + s0)}{\text{Cx}(\&2)}$
$\mathcal{L}\left[f(t)sin(s_0 t)\right] = \dfrac{F(s-s_0)}{2i} - \dfrac{F(s+s_0)}{2i}$	$\vdash_{thm}$ ∀f s s0. [A] laplace_exists f s ⇒ laplace_transform (λt. csin (s0 ∗ Cx t) ∗ f t) s = $\dfrac{\text{laplace\_transform f } (s - s0)}{\text{Cx } (\&2) * \text{ii}} - \dfrac{\text{laplace\_transform f } (s + s0)}{\text{Cx } (\&2) * \text{ii}}$
Time Scaling	
$\mathcal{L}\left[f(ct)\right] = \dfrac{1}{c}F\left(\dfrac{s}{c}\right), \quad 0 < c$	$\vdash_{thm}$ ∀f s c. [A1] &0 < c ∧ [A2] laplace_exists f s ∧ [A3] laplace_exists f $\left(\dfrac{\text{s}}{\text{Cx c}}\right)$ ⇒ laplace_transform (λt. f(c % t)) s = $\dfrac{\text{Cx}(\&1)}{\text{Cx c}}$ ∗ laplace_transform f $\left(\dfrac{\text{s}}{\text{Cx c}}\right)$
Integration of Time Domain	
$\mathcal{L}\left[\int_0^t f(\tau)d\tau\right] = \dfrac{1}{s}F(s)$	$\vdash_{thm}$ ∀f s. [A1] &0 < Re s ∧ [A2] laplace_exists f s ∧ [A3] laplace_exists (λx. integral (interval [&0,x]) f) s ∧ [A4] (∀x. f continuous_on interval [&0,x]) ⇒ laplace_transform (λx. integral (interval [&0,x]) f) s = $\dfrac{\text{Cx}(\&1)}{\text{s}}$ ∗ laplace_transform f s
First-order Differentiation in Time Domain	
$\mathcal{L}\left[\dfrac{d}{dt}f(t)\right] = sF(s) - f(0)$	$\vdash_{thm}$ ∀f s. [A1] laplace_exists f s ∧ [A2] (∀t. f differentiable at t) ∧ [A3] laplace_exists (λt. vector_derivative f (at t)) s ⇒ laplace_transform (λt. vector_derivative f (at t)) s = s ∗ laplace_transform f s - f (&0)
Higher-order Differentiation in Time Domain	
$\mathcal{L}[\dfrac{d^n}{dt^n}f(t)] = s^n F(s) - \sum_{k=1}^{n} s^{k-1}\dfrac{d^{n-k}f(0)}{dx^{n-k}}$	$\vdash_{thm}$ ∀f s n. [A1] laplace_exists_higher_deriv n f s ∧ [A2] (∀t. differentiable_higher_derivative n f t) ⇒ laplace_transform (λt. higher_vector_derivative n f t) s = s^{n} ∗ laplace_transform f s - vsum (1..n) (λx. $\text{s}^{(\text{x - 1})}$ ∗ higher_vector_derivative (n - x) f (&0))
Transfer Function of a *n*-order System	
$\dfrac{Y(s)}{X(s)} = \dfrac{\sum_{k=0}^{m}\beta_k s^k}{\sum_{k=0}^{n}\alpha_k s^k}$	$\vdash_{thm}$ ∀y x m n inlst outlst s. [A1] (∀t. differentiable_higher_derivative n y t) ∧ [A2] laplace_exists_higher_deriv n y s ∧ [A3] (∀t. differentiable_higher_derivative m x t) ∧ [A4] laplace_exists_higher_deriv m x s ∧ [A5] (0 < n ⇒ zero_init_conditions (n - 1) y) ∧ [A6] (0 < m ⇒ zero_init_conditions (m - 1) x) ∧ [A7] (vsum (0..n) (λt. EL t outlst ∗ s^{t}) ≠ Cx (&0)) ∧ [A8] (laplace_transform x s ≠ Cx (&0)) ∧ [A9] diff_eq_n_order_sys m n inlst outlst y x ⇒ $\dfrac{\text{laplace\_transform y s}}{\text{laplace\_transform x s}} = \dfrac{\text{vsum (0..m) } (\lambda\text{t. EL t inlst} * \text{s}^{\text{t}})}{\text{vsum (0..n) } (\lambda\text{t. EL t outlst} * \text{s}^{\text{t}})}$

5.2.2. Formally verified properties of the Fourier transform

We used the definitions, given in Section 5.2.1, to formally verify some of the classical properties of the Fourier transform, namely linearity, time shifting, frequency shifting, cosine and sine-based modulation, time scaling, time reversal, differentiation in time domain and frequency response of a n-order system, given in Table 2. The assumptions of these theorems describe the conditions for the existence of the corresponding Fourier transforms. Whereas, the last two assumptions of the *first-order differentiation* property model the condition that $\lim_{t \to \pm\infty} f(t) = 0$ [19,20]. The verification of these properties not only ensures the correctness of our definitions presented in Section 5.2.1 but also plays a vital role in minimizing the user effort in reasoning about the Fourier transform based analysis of systems, as will be depicted in Section 7.2 of the paper.

6. Uniqueness of the Fourier transform

The section provides the formal proof of the uniqueness of the Fourier transform.

6.1. Mathematical proof of the uniqueness of the Fourier transform

Assume, $g : \mathbb{R}^1 \to \mathbb{C}$ is a continuous function satisfying Eq. (3), i.e.,

$$\mathcal{F}[g(t)] = G(\omega) = \int_{-\infty}^{+\infty} g(t)e^{-i\omega t}dt, \ \omega \in \mathbb{R} \tag{4}$$

Assume, there is another continuous function h, which satisfies the following condition:

$$\mathcal{F}[h(t)] = H(\omega) = \int_{-\infty}^{+\infty} h(t)e^{-i\omega t}dt, \ \omega \in \mathbb{R} \tag{5}$$

and if $\mathcal{F}[g(t)] = \mathcal{F}[h(t)]$, then both of the functions g and h are the same, i.e., $g(t) = h(t)$. Alternatively, we can interpret the above statement by assuming that there is another continuous function f, such that $f(t) = g(t) - h(t)$ and if $\mathcal{F}[f(t)] = 0$, then $f(t) = 0$ [45].

The proof of the uniqueness of the Fourier transform is based on L^1 spaces [45,46]. Suppose $f \in L^1(\mathbb{R})$, i.e., $\int_{-\infty}^{+\infty} |f(t)| < \infty$ or $\int_{\mathbb{R}} |f(t)| < \infty$, and

$$\mathcal{F}[f(t)] = F(\omega) = \int_{\mathbb{R}} f(t)e^{-i\omega t}dt = 0, \ \omega \in \mathbb{R} \tag{6}$$

Table 2
Properties of Fourier transform [19,20].

Mathematical Form	Formalized Form
Linearity	
$\mathcal{F}[\alpha f(t)+\beta g(t)] = \alpha F(\omega)+\beta G(\omega)$	$\vdash_{thm}$ ∀f g w a b. [A1] fourier_exists f ∧ [A2] fourier_exists g ⇒ fourier_transform (λt. a ∗ f t + b ∗ g t) w = a ∗ fourier_transform f w + b ∗ fourier_transform g w
Time Shifting (Time Advance and Time Delay)	
$\mathcal{F}\left[f(t+t_0)\right] = e^{+i\omega t_0}F(\omega)$	$\vdash_{thm}$ ∀f w t0. [A] fourier_exists f ⇒ fourier_transform (λt. f (t + t0)) w = cexp ((ii ∗ Cx w) ∗ Cx t0) ∗ fourier_transform f w
$\mathcal{F}\left[f(t-t_0)\right] = e^{-i\omega t_0}F(\omega)$	$\vdash_{thm}$ ∀f w t0. [A] fourier_exists f ⇒ fourier_transform (λt. f (t - t0)) w = cexp (-((ii ∗ Cx w) ∗ Cx t0)) ∗ fourier_transform f w
Frequency Shifting (Right and Left Shifting)	
$\mathcal{F}[e^{i\omega_0 t}f(t)] = F(\omega-\omega_0)$	$\vdash_{thm}$ ∀f w w0. [A] fourier_exists f ⇒ fourier_transform (λt. cexp ((ii ∗ Cx w0) ∗ Cx t) ∗ f t) w = fourier_transform f (w - w0)
$\mathcal{F}[e^{-i\omega_0 t}f(t)] = F(\omega+\omega_0)$	$\vdash_{thm}$ ∀f w w0. [A] fourier_exists f ⇒ fourier_transform (λt. cexp (-(ii ∗ Cx w0) ∗ Cx t) ∗ f t) w = fourier_transform f (w + w0)
Modulation (Cosine and Sine Based Modulation)	
$\mathcal{F}\left[f(t)cos(\omega_0 t)\right] = \dfrac{F(\omega-\omega_0)}{2} + \dfrac{F(\omega+\omega_0)}{2}$	$\vdash_{thm}$ ∀f w w0. [A] fourier_exists f ⇒ fourier_transform (λt. ccos (Cx w0 ∗ Cx t) ∗ f t) w = $\dfrac{\text{fourier\_transform f (w − w0)}}{\text{Cx(\&2)}} + \dfrac{\text{fourier\_transform f (w + w0)}}{\text{Cx(\&2)}}$
$\mathcal{F}\left[f(t)sin(\omega_0 t)\right] = \dfrac{F(\omega-\omega_0)}{2i} - \dfrac{F(\omega+\omega_0)}{2i}$	$\vdash_{thm}$ ∀f w w0. [A] fourier_exists f ⇒ fourier_transform (λt. csin (Cx w0 ∗ Cx t) ∗ f t) w = $\dfrac{\text{fourier\_transform f (w − w0)}}{\text{Cx (\&2) ∗ ii}} - \dfrac{\text{fourier\_transform f (w + w0)}}{\text{Cx (\&2) ∗ ii}}$
Time Scaling	
$\mathcal{F}\left[f(at)\right] = \dfrac{1}{\lvert a\rvert}F\left(\dfrac{\omega}{a}\right)$	$\vdash_{thm}$ ∀f w a. [A1] (a ≠ &0) ∧ [A2] fourier_exists f ⇒ fourier_transform (λt. f(a % t)) w = $\dfrac{\text{Cx(\&1)}}{\text{Cx (abs a)}}$ ∗ fourier_transform f $\left(\dfrac{\text{w}}{\text{a}}\right)$
Time Reversal	
$\mathcal{F}[f(-t)] = F(-\omega)$	$\vdash_{thm}$ ∀f w. [A] fourier_exists f ⇒ fourier_transform (λt. f (-t)) w = fourier_transform f (-w)
First-order Differentiation in Time Domain	
$\mathcal{F}[\frac{d}{dt}f(t)] = i\omega F(\omega)$	$\vdash_{thm}$ ∀f w. [A1] fourier_exists f [A2] fourier_exists (λt. vector_derivative f (at t)) ∧ [A3] (∀t. f differentiable at t) ∧ [A4] ((λt. f t) → vec 0) at_posinfinity ∧ [A5] ((λt. f t) → vec 0) at_neginfinity ⇒ fourier_transform (λt. vector_derivative f (at t)) w = ii ∗ Cx w ∗ fourier_transform f w
Higher-order Differentiation in Time Domain	
$\mathcal{F}[\frac{d^n}{dt^n}f(t)] = (i\omega)^n F(\omega)$	$\vdash_{thm}$ ∀f w n. [A1] fourier_exists_higher_deriv n f ∧ [A2] (∀t. differentiable_higher_derivative n f t) ∧ [A3] (∀k. k < n ⇒ ((λt. higher_vector_derivative k f t) → vec 0) at_posinfinity) ∧ [A4] (∀k. k < n ⇒ ((λt. higher_vector_derivative k f t) → vec 0) at_neginfinity) ⇒ fourier_transform (λt. higher_vector_derivative n f t) w = (ii ∗ Cx w)$^{\text{n}}$ ∗ fourier_transform f w
Frequency Response of a *n*-order System	
$\dfrac{Y(\omega)}{X(\omega)} = \dfrac{\sum_{k=0}^{m}\alpha_k(i\omega)^k}{\sum_{k=0}^{n}\beta_k(i\omega)^k}$	$\vdash_{thm}$ ∀y x m n inlst outlst w. [A1] (∀t. differentiable_higher_derivative n y t) ∧ [A2] fourier_exists_of_higher_deriv n y ∧ [A3] (∀t. differentiable_higher_derivative m x t) ∧ [A4] fourier_exists_of_higher_deriv m x ∧ [A5] (∀k. k < n ⇒ ((λt. higher_vector_derivative k y t) → vec 0) at_posinfinity) ∧ [A6] (∀k. k < n ⇒ ((λt. higher_vector_derivative k y t) → vec 0) at_neginfinity) ∧ [A7] (∀k. k < m ⇒ ((λt. higher_vector_derivative k x t) → vec 0) at_posinfinity) ∧ [A8] (∀k. k < m ⇒ ((λt. higher_vector_derivative k x t) → vec 0) at_neginfinity) ∧ [A9] (fourier_transform x w ≠ Cx (&0)) ∧ [A10] (vsum (0..n) (λk. EL k outlst ∗ (ii ∗ Cx w)$^{\text{k}}$) ≠ Cx (&0)) ∧ [A11] (∀t. diff_eq_n_order_sys m n inlst outlst x y t) ⇒ $\dfrac{\text{fourier\_transform y w}}{\text{fourier\_transform x w}} = \dfrac{\text{vsum (0..m) (λk. EL k inlst ∗ (ii ∗ Cx w)}^{\text{k}}\text{)}}{\text{vsum (0..n) (λk. EL k outlst ∗ (ii ∗ Cx w)}^{\text{k}}\text{)}}$

Consider $a \in \mathbb{R}$ and define $F_a : \mathbb{R} \rightarrow \mathbb{C}$ as:

$$F_a(\omega) = \int_{-\infty}^{a} f(t)e^{-i\omega(t-a)}dt = -\int_{a}^{\infty} f(t)e^{-i\omega(t-a)}dt$$

Extending the domain of F_a to the complex plane, i.e., for $\omega \in \mathbb{H}^+ = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$, whereas, $\mathbb{H}^+$: $\mathbb{C}^+ \rightarrow \mathbb{C}$, define $F_a(\omega)$ as:

$$F_a(\omega) = \int_{-\infty}^{a} f(t)e^{-i\omega(t-a)}dt \tag{7}$$

and for $\omega \in \mathbb{H}^- = \{z \in \mathbb{C} : \mathrm{Im}(z) < 0\}$, define $F_a(\omega)$ as:

$$F_a(\omega) = -\int_{a}^{\infty} f(t)e^{-i\omega(t-a)}dt \tag{8}$$

It is clearly seen that F_a is bounded and continuous on $\mathbb{C}$, i.e., F_a of Eq. (7) is bounded and continuous on $\{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ and F_a of Eq. (8) is bounded and continuous on $\{z \in \mathbb{C} : \mathrm{Im}(z) < 0\}$. Moreover, F_a is also analytic/entire function [47] on $\mathbb{C}$ and it is sufficient to show by Morera's theorem [47] that $\int_{\partial R} F_a(\omega) = 0$ for any rectangle R with a positively oriented boundary. Without loss of generality, we can assume that $R \subset \overline{H}^+$ (the argument for $R \subset \overline{H}^-$ is completely analogous). Since ∂R is compact, $\int_{-\infty}^{a} \lvert f(t)e^{-i\omega(t-a)}\rvert dt < \infty$ and therefore,

$$\int_{\partial R} F_a(\omega)d\omega = \int_{\partial R}\int_{-\infty}^{a} f(t)e^{-i\omega(t-a)}dtd\omega < \infty \tag{9}$$

We need to swap the order of the integration in the above equation, which is done using Fubini's theorem [48] as:

$$\int_{\partial R} F_a(\omega)d\omega = \int_{-\infty}^{a} f(t)\left(\int_{\partial R} e^{-i\omega(t-a)}d\omega\right)dt \tag{10}$$

Since $e^{-i\omega(t-a)}$ is an analytic function of ω for fixed t, i.e., $\int_{\partial R} e^{-i\omega(t-a)} d\omega = 0$. Therefore,

$$\int_{\partial R} F_a(\omega) d\omega = \int_{-\infty}^{a} f(t)(0) dt = 0 \tag{11}$$

F_a is a bounded entire function, therefore, by Liouville's theorem [49], it is a constant. Moreover, this constant is equal to zero, i.e., $F_a = 0$, which can be proved using the Lebesgue dominated convergence theorem [50] as:

$$\begin{aligned} \lim_{\omega \to \infty} F_a(i\omega) &= \lim_{\omega \to \infty} \int_{-\infty}^{a} f(t) e^{-i(i\omega)(t-a)} dt \\ &= \lim_{\omega \to \infty} \int_{-\infty}^{a} f(t) e^{\omega(t-a)} dt = 0 \end{aligned} \tag{12}$$

Thus,

$$0 = F_a(0) = \int_{-\infty}^{a} f(t) dt \tag{13}$$

and this holds for each $a \in \mathbb{R}$. Finally, differentiating Eq. (13) (application of the Lebesgue differentiation theorem [51]) yields $f(a) = 0$.

6.2. Formal proof of the uniqueness of the Fourier transform

We formally verify the uniqueness of the Fourier transform as the following HOL Light theorem:

Theorem 6.1. *Uniqueness of the Fourier Transform*

```
⊢thm ∀g h.
    [A1] fourier_exists g ∧
    [A2] fourier_exists h ∧
    [A3] (∀w. fourier_transform g w = fourier_transform h w)
        ⇒ (∀t. g t = h t)
```

where f and g are complex-valued functions and w is a real variable. The assumptions A1--A2 of the above theorem capture the Laplace existence conditions for the functions f and g, respectively. The assumption A3 expresses the condition that the Fourier transforms of the functions f and g are equal. Finally, the conclusion provides the equivalence of the functions f and g for all values of their argument t. The proof of Theorem 6.1 mainly depends on the alternate representation of uniqueness of the Fourier transform, which is verified as:

Theorem 6.2. *Alternate Representation of Uniqueness of the Fourier Transform*

```
⊢thm ∀f. [A1] fourier_exists f ∧
    [A2] (∀w. fourier_transform f w = 0)
        ⇒ (∀t. f t = 0)
```

Using the function $f(t) = g(t) - h(t)$ in the above theorem along with the linearity property of the Fourier transform provides the straightforward verification of Theorem 6.1. Next, we proceed with the proof of Theorem 6.2 by applying the properties of sets along with some complex arithmetic simplification, which results into the following subgoal:

Subgoal 6.1. `∀t. t IN UNIV ⇒ f t = vec 0`

The proof of the above subgoal is mainly based on the following lemma:

Lemma 6.1.

```
⊢thm ∀f s a.
    [A1] convex s ∧
    [A2] (interior s = {} ⇒ s = {}) ∧
    [A3] f continuous_on s ∧
    [A4] negligible {x | x IN s ∧ (f x ≠ a)}
        ⇒ (∀x. x IN s ⇒ f x = a)
```

Applying the above lemma on Subgoal 6.1 results into a subgoal, where it is required to verify all the assumptions of Lemma 6.1. The assumptions A1--A3 are verified using the properties of continuity and sets along with some complex arithmetic reasoning. Finally, the assumption A4, after simplification, results into the following subgoal:

Subgoal 6.2. `negligible {t | (f t ≠ 0)}`

By applying the properties of negligible sets and integrals, we obtain a new subgoal as:

Subgoal 6.3. `∀a b. (f has_integral vec 0) (interval [a,b])`

We start the proof process of the above subgoal by formally verifying the following lemma, which captures the absolute integrability of the integrands provided in Eqs. (7) and (8) as:

Lemma 6.2. *Absolute Integrability of* F_a

```
⊢thm ∀f. f absolutely_integrable_on UNIV ⇒
    [C1] (∀a z. &0 ≤ Im z ⇒
            (λx. f x * cexp (-ii * Cx (x - a) * z))
                absolutely_integrable_on {x | x ≤ a}) ∧
    [C2] (∀a z. Im z ≤ &0 ⇒
            (λx. f x * cexp (-ii * Cx (x - a) * z))
                absolutely_integrable_on {x | a ≤ x})
```

The above lemma is verified using properties of the integrals, differentials, Lebesgue measures, limits, sets and transcendental functions along with some arithmetic (real and complex) reasoning. Moreover, this verified lemma also serves as one of the assumptions for Subgoal 6.3.

Next, we verify the continuity of the function F_a (Eqs. (7) and (8)) as the following subgoal:

Subgoal 6.4. `∀a. h a continuous_on UNIV`

where UNIV models the whole complex plane. The function h, having data-type $\mathbb{R} \to \mathbb{C} \to \mathbb{C}$, modeling the function F_a is formalized in HOL Light as:

Subgoal 6.5.

```
h = (λz. if &0 ≤ Im z then
    integral {x | x ≤ a} (λx. f x * cexp (-ii * Cx (x - a) * z)) else
    - integral {x | a ≤ x} (λx. f x * cexp (-ii * Cx (x - a) * z)))
```

After applying the properties of the continuity and sets, the above subgoal becomes:

Subgoal 6.6.

```
[C1] (λz. integral {x | x ≤ a}
    (λx. f x * cexp (-ii * Cx (x - a) * z)))
        continuous_on {z | &0 ≤ Im z} ∧
[C2] (λz. integral {x | a ≤ x}
    (λx. f x * cexp (-ii * Cx (x - a) * z)))
        continuous_on {z | Im z ≤ &0}
```

The verification of the conjunct C1 of the above subgoal is mainly based on the following HOL Light theorem along with the properties of integrals and some complex arithmetic reasoning.

Theorem 6.3. *Dominated Convergence Theorem*

```
⊢thm ∀f g h s.
    [A1] (∀k. f k integrable_on s) ∧
    [A2] h integrable_on s ∧
    [A3] (∀k x. x IN s ⇒ ||f k x|| ≤ h x) ∧
    [A4] (∀x. x IN s ⇒ ((λk. f k x) → g x) sequentially)
        ⇒ g integrable_on s ∧
            ((λk. integral s (f k)) → integral s g) sequentially
```

The proof of the conjunct C2 is quite similar to C1. The verified Subgoal 6.4 also serves as one of the assumptions for Subgoal 6.3.

Next, we verify the following subgoal, which also becomes one of the assumptions of Subgoal 6.3.

Subgoal 6.7. ∀a z. h a z = Cx (&0)

After applying the Liouville theorem, the above subgoal transforms into the following subgoal:

Subgoal 6.8. [A1] (h a holomorphic_on UNIV ∧
[A2] bounded (IMAGE (h a) UNIV)
⇒ [C] (∃c. ∀z. h a z = c))
⇒ [C′] h a z = Cx (&0)

This requires verifying that the function h a is holomorphic and bounded on UNIV and the constant c is equal to zero, i.e.,

c = Cx (&0)

By applying the properties of the limit, the above expression becomes:

((λn. h a (ii ∗ Cx (&n))) → Cx (&0)) sequentially

The proof of the above expression is mainly based on the dominated convergence theorem (Theorem 6.3) along with the properties of integrals, vectors, limits and complex numbers.

Now, in the proof process of the assumption A1 of Subgoal 6.8, we use the properties of differentials and complex numbers to obtain the following subgoal:

Subgoal 6.9. [C1] h a holomorphic_on {z | &0 < Im z} ∧
[C2] h a holomorphic_on {z | Im z < &0}

The above subgoal requires verifying the conjuncts C1 and C2. We only present the verification of C1 here and the reasoning process of C2 is very similar. As we know that every analytic function is always a holomorphic function and thus, to formally verify C1, we only need to verify the analyticity of the function h a. We apply the Morera triangle theorem, which is given as:

Theorem 6.4. *Morera Triangle Theorem*
$\vdash_{thm}$ ∀f s.
[A1] open s ∧
[A2] f continuous_on s ∧
[A3] (∀a b c. convex hull a, b, c SUBSET s ⇒
path_integral (linepath (a,b)) f +
path_integral (linepath (b,c)) f +
path_integral (linepath (c,a)) f = Cx (&0))
⇒ [C] f analytic_on s

The assumption A1 ensures that s is an open set. The assumption A2 expresses the continuity of the function f on s. The assumption A3 models the condition that the integral of the function f on a closed path is zero.

After applying the Morera triangle theorem, it is required to verify all the assumptions of Theorem 6.4. The first two assumptions are verified using the properties of sets and continuity. The verification of Assumption A3 is mainly based on the following subgoal:

Subgoal 6.10. ∀p q. [A1] &0 < Im p ∧ [A2] &0 < Im q
⇒ ((λy. f y ∗ (g y q - g y p)) has_integral
(path_integral (linepath (p,q)) (h a))) {y | $\underline{y}$ ≤ a}

By applying the properties of the integrals, the above subgoal becomes:

Subgoal 6.11. ((λy. integral (interval [vec 0,vec 1])
(λx. f y ∗ cexp (-ii ∗ Cx ($\underline{y}$ - a) ∗
linepath (p,q) x) ∗ (q - p))) has_integral
(integral (interval [vec 0,vec 1]) (λx. integral
{x | $\underline{x}$ ≤ a} (λx′. f x′ ∗ cexp (-ii ∗ Cx ($\underline{x'}$ - a) ∗
linepath (p,q) x)) ∗ (q - p)))) {y | $\underline{y}$ ≤ a}

Now, to swap the order of the integration, we require the Fubini's theorem, which is given in HOL Light as:

Theorem 6.5. *Fubini's Theorem*
$\vdash_{thm}$ ∀f. f absolutely_integrable_on UNIV
⇒ ((λy. integral UNIV (λx. f (pastecart x y)))
has_integral integral UNIV
(λx. integral UNIV (λy. f (pastecart x y)))) UNIV

The application of Fubini's theorem along with the other properties of integrals, continuity, limits and complex numbers, concludes our proof of the conjunct C1 of Subgoal 6.9. The verification of C2 is performed on the same lines as that of C1. Similarly, we verified the assumption A2 of Subgoal 6.8, i.e., boundedness of the function h a using the upper bound properties of the integrals, sets along with some complex arithmetic reasoning. This concludes our proof of Subgoal 6.7. This verified subgoal also serves as one of the assumptions for Subgoal 6.3.

Finally, applying the properties of integrals on Subgoal 6.3, results into the following subgoal:

Subgoal 6.12. [C1] integral {x | $\underline{x}$ ≤ $\underline{b}$} f = vec 0 ∧
[C2] integral {x | $\underline{x}$ ≤ $\underline{a}$} f = vec 0

The verification of the conjuncts C1 and C2 of the above subgoal is based on all the assumptions (generated by verified Subgoals 6.4 and 6.7, and Lemma 6.2 along with the properties of integrals. This concludes our formal proof of the uniqueness of the Fourier transform. More details about its verification can be found in our proof script [52].

The verification of the uniqueness of the Fourier transform enables us to establish a relationship between the differential equation based models expressed in time-domain and the corresponding ω-domain model, i.e., frequency response, which was not possible using our earlier formalization of the Fourier transform [19,20] that can only provide the analysis in the frequency domain. Thus, it can be used to formally verify the time-domain solutions of the differential equations modeling the continuous dynamics of CPS as will be depicted in Section 7.2.

7. Case studies

7.1. Formal analysis of an industrial robot

Industrial robots [53] are primarily serial link manipulators such that their dynamical behavior depends on the orientation and movement of each of the links or joints, which are mainly controlled by employing various linear feedback controllers. The commercially available robots, such as Cincinnati Milacron Model T3, Unimation PUMA 600 and Stanford manipulator, typically consist of three to seven joints, including hand, which is commonly termed as a gripper or an end effector, providing one degree of freedom for each of the joints. Each joint of these robots is usually driven hydraulically or electrically with a feedback control loop and thus has its own positional control system.

The industrial robots are the autonomous CPS composed of actuators and sensors interacting with the external environment and are widely employed in various applications, such as die casting, robotic glass deburring system, machine tending, robotic girder gouging and welding, material handling, painting, assembling product, automated storage and retrieval system, waterjet cutting and drilling etc. [53,54]. Due to these safety-critical applications of the industrial robots, the accurate analysis of their dynamical behavior and their associated controllers is of utmost importance.

An actuator-gear-load assembly model [54] for a single joint of an industrial robot is depicted in Fig. 2. The variables J_a, J_m and J_l model the actuator inertia, robot (manipulator) inertia of the joint fixtures on the side of the actuator and the inertia of the manipulator link, respectively. Similarly, θ_m and θ_s are the angular displacements at actuator shaft and load side, respectively. The variables τ_m and τ_l express the torques generated at the actuator shaft and due to load, respectively. The variable n represents the gear ratio that basically relates the angular displacements, i.e., θ_m and θ_s.

The actuator is an essential part of a system, which works on the principle of converting any form of the energy to motion and thus, it is responsible for controlling various tasks of the underlying system. The commonly used industrial robots, i.e., Unimation PUMA and Stanford manipulators contain the armature controlled actuators that are composed of an electrical system using permanent magnet dc motors. This electrical drive system for these robots [54] is depicted in Fig. 3.

The variable $v_b(t)$ models the Electromotive Force (emf), which is mathematically expressed as:

$$v_b(t) = K_b\dot{\theta}_m(t) \tag{14}$$

where $\dot{\theta}_m(t)$ and K_b represent the angular velocity (first-order derivative of the angular displacement) at the actuator shaft and the back emf constant, respectively. Next, applying Kirchhoff's Voltage Law (KVL) on the armature circuit (Fig. 3), we obtain:

$$v(t) - v_b(t) = L\frac{di(t)}{dt} + Ri(t) \tag{15}$$

Since the voltages $v(t)$ and $v_b(t)$, and the current $i(t)$ are causal functions, thus, applying the Laplace transform on Eqs. (14) and (15) and after simplification, we get:

$$V(s) - K_b s\Theta_m(s) = (Ls + R)I(s) \tag{16}$$

Similarly, the torque generated by the dc motor operating in the linear region is mathematically expressed as:

$$\tau_m(t) = K_I i(t) \tag{17}$$

Application of the Laplace transform results into the following equation:

$$T_m(s) = K_I I(s) \tag{18}$$

The motor shaft has a mechanical connection with an actuator-gear-load assembly as depicted in Fig. 3. The mathematical relationship between various mechanical components, depicted in Fig. 2, is given as follows:

$$\tau_m(t) = (J_a + J_m + n^2 J_l)\ddot{\theta}_m + (B_m + n^2 B_l)\dot{\theta}_m \tag{19}$$

Taking the Laplace transform on both sides of the above equation results into the following equation:

$$T_m(s) = [(J_a + J_m + n^2 J_l)s^2 + (B_m + n^2 B_l)s]\Theta_m(s) \tag{20}$$

By eliminating $T_m(s)$ and $I(s)$ from Eqs. (16), (18) and (20) and after simplification, we obtain the transfer function, which is the feedforward gain, from the applied voltage to the dc motor (input), to the angular displacement of the motor shaft (output) [54].

$$\frac{\Theta_m(s)}{V(s)} = \frac{K_I}{LJ_{eff}s^3 + (RJ_{eff} + LB_{eff})s^2 + (RB_{eff} + K_I K_b)s} \tag{21}$$

where,
$J_{eff} = J_a + J_m + n^2 J_l$
$B_{eff} = B_m + n^2 B_l$

In order to verify the above transfer function, we need to formalize the corresponding differential equation (dynamics of the armature circuit (electrical drive system)).

Definition 7.1. Differential Equation of Electrical Drive System

```
⊢def ∀Kl. inlst_eds Kl = [Cx Kl]
⊢def ∀Kl Kb R Bm Bl L Ja Jm n Jl.
        outlst_eds Kl Kb R L Ja Jm Jl Bm Bl n =
             [Cx (&0); Cx (R * Beff + Kl * Kb);
                  Cx (R * Jeff + L * Beff); Cx (L * Jeff)]
⊢def ∀Kb R L Ja Jm Jl Bm Bl n Thetam Kl V t.
    diff_eq_eds Kl Kb R L Ja Jm Jl Bm Bl n V Thetam t ⇔
    diff_equ 3 (outlst_eds Kl Kb R L Ja Jm Jl Bm Bl n) Thetam t =
    diff_equ 0 (inlst_eds Kl) V t
```

where the function diff_eq_eds accepts the function variables V and Thetam and the lists of coefficients inlst_eds and outlst_eds and returns the corresponding differential equation. Moreover, the elements Jeff and Beff of the list outlst_eds are:

```
Jeff = Ja + Jm + n^2 * Jl
Beff = Bm + n^2 * Bl
```

Now, we formally verify the transfer function (Eq. (21)) as the following HOL Light theorem:

Theorem 7.1. *Transfer Function Verification of Electrical Drive System*

```
⊢thm ∀V Thetam Ja Jm Jl L R Bm n Bl Kl Kb s.
  [A1] &0 < Kl ∧ [A2] &0 < Kb ∧ [A3] &0 < R ∧
  [A4] &0 < L ∧  [A5] &0 < n ∧  [A6] &0 < Ja ∧
  [A7] &0 < Jm ∧ [A8] &0 < Jl ∧ [A9] &0 < Bm ∧
  [A10] &0 < Bl ∧
  [A11] laplace_transform V s ≠ Cx (&0) ∧
  [A12] (Cx (L * Jeff) * s^3 + Cx (R * Jeff + L * Beff) * s pow 2 +
                      Cx (R * Beff + Kl * Kb) * s ≠ Cx (&0)) ∧
  [A13] (∀t. differentiable_higher_derivative 0 V t) ∧
  [A14] (∀t. differentiable_higher_derivative 3 Thetam t) ∧
  [A15] zero_initial_conditions 2 Thetam ∧
  [A16] laplace_exists_higher_deriv 0 V s ∧
  [A17] laplace_exists_higher_deriv 3 Thetam s ∧
  [A18] (∀t. diff_eq_eds Kl Kb R L Ja Jm Jl Bm Bl n V Thetam t)
        ⇒ laplace_transform Thetam s / laplace_transform V s =
          Cx Kl / (Cx (L * Jeff) * s^3 + Cx (R * Jeff + L * Beff)
                   * s^2 + Cx (R * Beff + Kl * Kb) * s)
```

The assumptions A1--A12 express the design constraints for the electrical drive system. The assumptions A13--A14 provide the differentiability conditions for the input V and output Thetam up to the order 0 and 3, respectively. Similarly, the assumption A15 presents the *zero initial conditions* for the function Thetam. The assumptions A16--A17 ensure that the Laplace transform of the functions V and Thetam exist up to order 0 and 3, respectively. The assumption A18 provides the differential equation model of the underlying system. Finally, the conclusion represents the considered transfer function (Eq. (21)). A notable feature of our formal analysis of an industrial robot is that the verification of Theorem 7.1 is done almost automatically using the automatic tactic DIFF_EQ_2_TRANS_FUN_TAC, which is based on the application of *Transfer Function of a n-order System*, presented in Table 1, and developed as a part of our proposed formalization. It requires the differential equation and the transfer function of the underlying system and automatically verifies the theorem corresponding to the transfer function of the system.

Next, we verify the differential equation of the electrical drive system based on its transfer function as:

Theorem 7.2. *Differential Equation Verification of Electrical Drive System*

```
⊢thm ∀V Thetam Ja Jm Jl L R Bm n Bl Kl Kb s.
  [A1] &0 < Kl ∧ [A2] &0 < Kb ∧ [A3] &0 < R ∧ [A4] &0 < L ∧
  [A5] &0 < Ja ∧ [A6] &0 < Jm ∧ [A7] &0 < n ∧
  [A8] &0 < Jl ∧ [A9] &0 < Bm ∧ [A10] &0 < Bl ∧
```

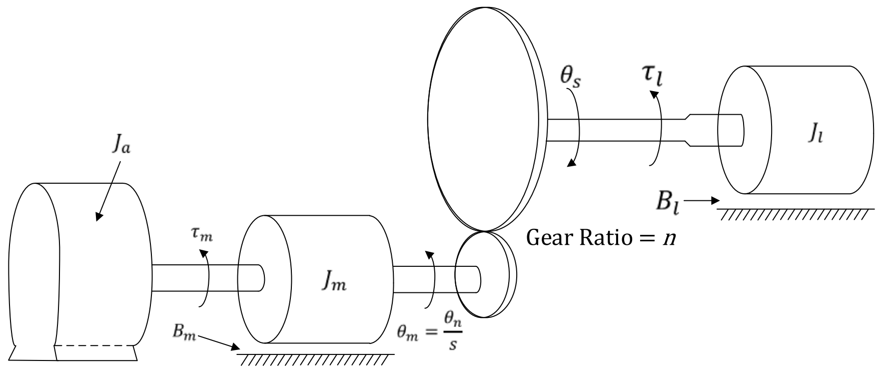

Fig. 2. An Actuator-gear-load Assembly for a Single Joint.

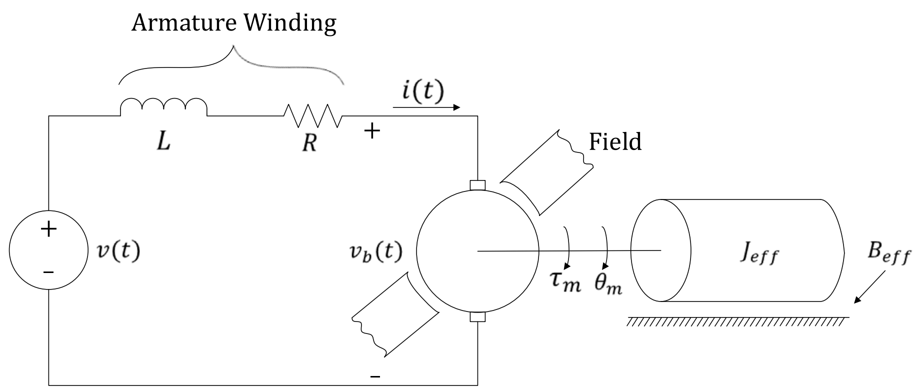

Fig. 3. Electrical Drive System for Industrial Robots.

[A11] (∀s. Re r ≤ Re s ⇒ laplace_transform V s ≠ Cx (&0)) ∧
[A12] (∀s. Re r ≤ Re s ⇒
Cx (L ∗ Jeff) ∗ s^3 + Cx (R ∗ Jeff + L ∗ Beff) ∗ s^2 +
Cx (R ∗ Beff + KI ∗ Kb) ∗ s ≠ Cx (&0)) ∧
[A13] (∀t. differentiable_higher_derivative 0 V t) ∧
[A14] (∀t. differentiable_higher_derivative 3 Thetam t) ∧
[A15] zero_initial_conditions 2 Thetam ∧
[A16] &0 ≤ Re r ∧
[A17] (∀s. Re r ≤ Re s ⇒ laplace_exists_higher_deriv 0 V s) ∧
[A18] (∀s. Re r ≤ Re s ⇒
laplace_exists_higher_deriv 3 Thetam s) ∧
[A19] (∀s. Re r ≤ Re s ⇒ $\frac{\texttt{laplace\_transform Thetam s}}{\texttt{laplace\_transform V s}}$ =
$\frac{\texttt{Cx KI}}{\texttt{Cx (L * Jeff) * s}^3\texttt{ + Cx (R * Jeff + L * Beff) * s}^2\texttt{ + Cx (R * Beff + KI * Kb) * s}}$)
⇒ (∀t. diff_eq_eds KI Kb R L Ja Jm Jl Bm Bl n V Thetam t)

The assumptions A1--A15 are the same as that of Theorem 7.1. The assumption A16 ensures that the real part of the Laplace variable r is always positive. The assumptions A17--A18 ensure that the Laplace transform of the functions V and Thetam exist up to order 0 and 3, respectively. The assumption A19 provides the transfer function of the electrical drive system. Finally, the conclusion provides its corresponding differential equation model. The verification of Theorem 7.2 is done almost automatically using the automatic tactic TRANS_FUN_2_DIFF_EQ_TAC, which is based on the application of Theorem 5.1 and *Laplace Transform of a n-order System*, presented in Table 1, and also developed in our proposed formalization. It requires the differential equation and the transfer function of the underlying system and automatically verifies the theorem corresponding to the differential equation of the system.

Now, to construct a positional controller, we need to transform the angular displacement of the shaft to an electrical signal for actuating the motor. The closed-loop transfer function of the positional controller obtained as a result of this conversion, is mathematically modeled as:

$$\frac{\Theta_s(s)}{\Theta_d(s)} = \frac{nK_\theta K_I}{RJ_{eff}s^2 + (RB_{eff} + K_I K_b)s + K_\theta K_I} \tag{22}$$

We formally verified the above closed-loop transfer function and the corresponding differential equation of this controller. In addition, we also verified the transfer function and the corresponding differential equation of a another controller, which is developed as a result of selecting the feedback voltage at the motor armature circuit as $v_b(t) = (K_b + K_1 K_t)\dot{\theta}_m(t)$. Further details about the formal analysis of the industrial robot can be found in our proof script [52].

7.2. Formal analysis of an equalizer

Equalization [55] is the process of reversing the distortion produced when a signal is transmitted over a communication channel and is commonly used in signal processing and telecommunication. Equalizers are usually used for recovering the frequency response of systems by eliminating the distortion associated with the channel. Fig. 4 depicts the process of transmitting a signal $x(t)$ over a set of N channels to obtain an output signal $y(t)$ at the receiver. These N sub-channels would create distortions in the components of the input signal, i.e., $x_1(t)$, $x_3(t)$, …, $x_n(t)$, that can be delayed or attenuated, or may exhibit the phase or group delays in their corresponding frequency components. The equalizer is used to cancel out these effects and to reproduce the actual transmitted signal at the receiver end. It is widely used in CPS, like autonomous vehicles, medical systems, smart grids and avionics.

An equalizer [55,56] is composed of different sets of filters that can be high-pass, low-pass, band-pass, band-stop and all-pass filters depending on the frequency components that need to be allowed

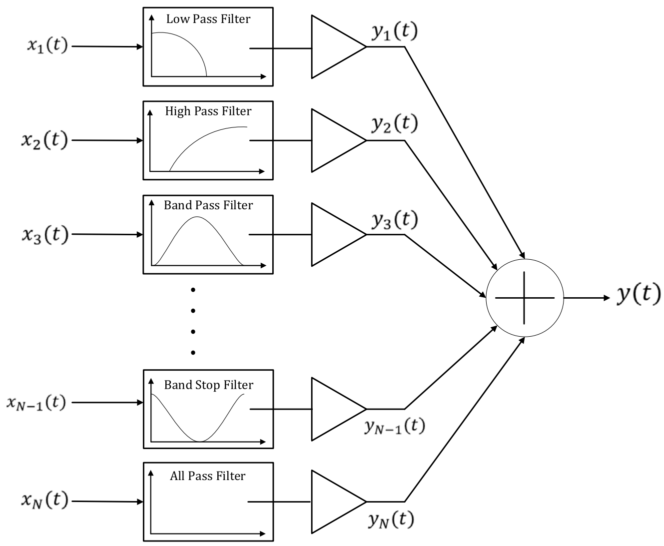

Fig. 5. Equalizer.

to pass. For example, a microphone can be more sensitive to lower frequency components of the sound than the higher ones. Thus, the corresponding equalizer would be used to increase the volume at high frequency sounds and to suppress the low frequency components and the high pass filter of the equalizer can capture this functionality. Similarly, in the case of telephone lines, we use equalizers for correcting the reduced level of the high frequencies of the audio signal in long cables that act as channels. Similarly, various frequency components of the transmitted signal over a channel can be distorted by the presence of the noise, which can be recovered by suppressing the noise effect using different filters of the equalizer. Fig. 5 depicts an equalizer that is mainly composed of different filters. The process of equalization starts by applying the individual filters on each component of the input signal based on the requirement. After each of the filtering stages, some signal amplification with gain (g_i) is applied to enhance the quality of the signal. Being an integral part of an equalizer, we performed the Fourier transform based analysis of each of the individual filters, since the input and the output of the filters are non-causal functions. Here, we present the analysis of the band-stop filter only due to space restrictions and the verification of the rest of the filters can be found in the proof script [52].

The frequency response of the band-stop filter is mathematically expressed as [57]:

$$\frac{Y(\omega)}{X(\omega)} = \frac{(i\omega)^2 + {\omega_0}^2}{(i\omega)^2 + 2\omega_c(i\omega) + (\omega_0)^2} \tag{23}$$

where ω_c and ω_0 express the width of the rejection band and the central rejected frequency, respectively. In order to verify the above frequency response, we first model its corresponding differential equation as:

Definition 7.2. Differential Equation of Band-stop Filter

```
⊢def ∀w0 wc. outlst_bsf_equ wc w0 =
        [Cx (w0²); Cx (&2 ∗ wc); Cx (&1)]
⊢def ∀w0. inlst_bsf_equ w0 = [Cx (w0²); Cx (&0); Cx (&1)]
⊢def ∀w0 wc x y t. diff_eq_BSF_EQU x y t wc w0 ⇔
          diff_equ 2 (outlst_bsf_equ wc w0) y t =
          diff_equ 2 (inlst_bsf_equ w0) x t
```

where the function diff_eq_BSF_EQU accepts the function variables x and y and the lists of coefficients inlst_bsf_equ and outlst_bsf_equ and returns the corresponding differential equation of the band-stop filter.

Now, we verified the above frequency response as the following HOL Light theorem:

Theorem 7.3. *Frequency Response Verification of Band-stop Filter*

```
⊢thm ∀y x w wc w0. [A1] &0 < wc ∧ [A2] &0 < w0 ∧
  [A3] (fourier_transform x w ≠ Cx (&0)) ∧
  [A4] ((ii ∗ Cx w)² +
          Cx (&2) ∗ Cx wc ∗ ii ∗ Cx w + Cx w0² ≠ Cx (&0)) ∧
  [A5] (∀t. differentiable_higher_derivative 2 y t) ∧
  [A6] (∀t. differentiable_higher_derivative 2 x t) ∧
  [A7] fourier_exists_higher_deriv 2 y ∧
  [A8] fourier_exists_higher_deriv 2 x ∧
  [A9] (∀k. k < 2 ⇒ ((λt. higher_vector_derivative
                    k y t̄) → vec 0) at_posinfinity) ∧
  [A10] (∀k. k < 2 ⇒ ((λt. higher_vector_derivative
                    k y t̄) → vec 0) at_neginfinity) ∧
  [A11] (∀k. k < 2 ⇒ ((λt. higher_vector_derivative
                    k x t̄) → vec 0) at_posinfinity) ∧
  [A12] (∀k. k < 2 ⇒ ((λt. higher_vector_derivative
                    k x t̄) → vec 0) at_neginfinity) ∧
  [A13] (∀t. diff_eq_BSF_EQU x y t wc w0)
```

$$\Rightarrow \frac{\text{fourier\_transform y w}}{\text{fourier\_transform x w}} = \frac{(\text{ii} * \text{Cx w})^2 + \text{Cx w0}^2}{(\text{ii} * \text{Cx w})^2 + \text{Cx (\&2)} * \text{Cx wc} * \text{ii} * \text{Cx w} + \text{Cx w0}^2}$$

The assumptions A1--A4 provide the design constraints for the band-pass filter. The assumptions A5--A6 capture the differentiability conditions of the functions y and x up to order 2, respectively. The assumptions A7--A8 ensure that the Fourier transform of the functions y and x exist up to order 2, respectively. The assumptions A9--A12 provide the conditions $\lim_{t\to\pm\infty} y^{(k)}(t) = 0$ and $\lim_{t\to\pm\infty} x^{(k)}(t) = 0$ for each $k = 0, 1$. The assumption A13 presents the corresponding differential equation. Finally, the conclusion represents the frequency response given by Eq. (23). The verification of Theorem 7.3 is done almost automatically using the automatic tactic DIFF_EQ_2_FREQ_RES_TAC, which is based on the application of *Frequency Response of a n-order System*, presented in Table 2, and developed in our proposed formalization. It requires the differential equation and the frequency response of the underlying system and automatically verifies the theorem corresponding to the frequency response of the system.

Next, we verified the corresponding differential equation as the following HOL Light theorem:

Theorem 7.4. *Differential Equation Verification of Band-stop Filter*

```
⊢thm ∀y x wc w0. [A1] &0 < wc ∧ [A2] &0 < w0 ∧
  [A3] (∀w. fourier_transform x w ≠ Cx (&0)) ∧
  [A4] (∀w. (ii ∗ Cx w)² + Cx (&2) ∗ Cx wc ∗
                    ii ∗ Cx w + Cx w0² ≠ Cx (&0)) ∧
  [A5] (∀t. differentiable_higher_derivative 2 y t) ∧
  [A6] (∀t. differentiable_higher_derivative 2 x t) ∧
  [A7] fourier_exists_higher_deriv 2 y ∧
  [A8] fourier_exists_higher_deriv 2 x ∧
  [A9] (∀k. k < 2 ⇒ ((λt. higher_vector_derivative
                    k y t̄) → vec 0) at_posinfinity) ∧
  [A10] (∀k. k < 2 ⇒ ((λt. higher_vector_derivative
                    k y t̄) → vec 0) at_neginfinity) ∧
  [A11] (∀k. k < 2 ⇒ ((λt. higher_vector_derivative
                    k x t̄) → vec 0) at_posinfinity) ∧
  [A12] (∀k. k < 2 ⇒ ((λt. higher_vector_derivative
                    k x t̄) → vec 0) at_neginfinity) ∧
```

$$[\text{A13}] \left(\forall \text{w}. \frac{\text{fourier\_transform y w}}{\text{fourier\_transform x w}} = \frac{(\text{ii} * \text{Cx w})^2 + \text{Cx w0}^2}{(\text{ii} * \text{Cx w})^2 + \text{Cx (\&2)} * \text{Cx wc} * \text{ii} * \text{Cx w} + \text{Cx w0}^2}\right)$$

$$\Rightarrow (\forall \text{t. diff\_eq\_BSF\_EQU x y t wc w0})$$

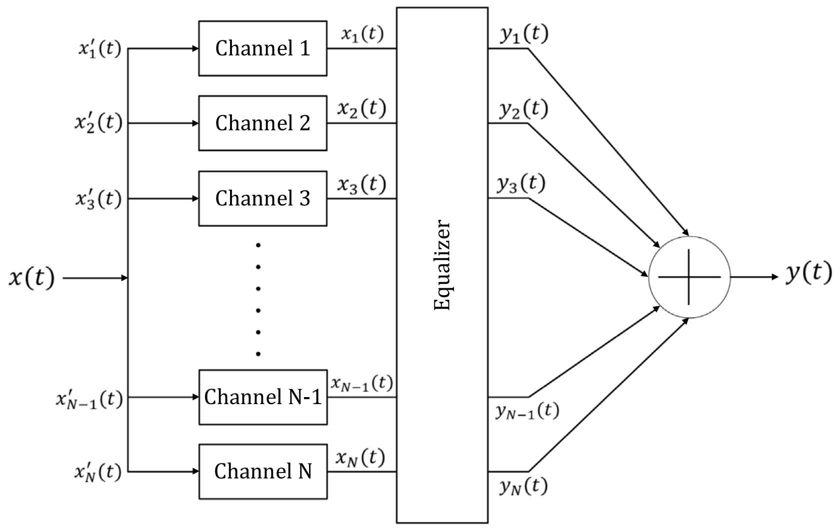

Fig. 4. Transmitting a Signal over a Communication Channel.

The assumptions A1--A12 are the same as that of Theorem 7.3. The assumption A13 models the frequency response of the band-stop filter. Finally, the conclusion of the above theorem represents the corresponding differential equation. The verification of Theorem 7.4 is done almost automatically using the automatic tactic FREQ_RES_2_DIFF_EQ_TAC, which is based on the application of the uniqueness of the Fourier transform (Theorem 6.1) and *Fourier Transform of a n-order System*, presented in Table 2, and also developed in our proposed formalization. The uniqueness of the Fourier transform (Theorem 6.1) plays a vital role in solving the linear differential equations in the ω-domain and thus relates the ω-domain analysis of the continuous dynamics of the band-pass filter to their corresponding time-domain analysis (linear differential equations based models), which is not possible with our earlier formalization of the Fourier transform. Moreover, the automatic tactic FREQ_RES_2_DIFF_EQ_TAC only requires the differential equation and the frequency response of the underlying system and automatically verifies the theorem corresponding to the differential equation of the system. The details about verification of the other filters can be found in the proof script [52].

The distinguishing feature of our proposed formalization as compared to the traditional analysis techniques is that all of the verified theorems are of generic nature, i.e., all of the functions and variables are universally quantified and thus we can specialize them to obtain the results for any given values. Moreover, the inherent soundness of the theorem proving technique ensures that all the required assumptions are explicitly present along with the theorem. Similarly, the verification of the transfer function and frequency response of a generic n-order system, given in Tables 1 and 2, can be specialized for formally analyzing any system as presented in Section 7. Whereas, in the computer based simulation methods, it is required to model each of the systems individually. Moreover, the high expressiveness of the higher-order logic enables us to model the differential equation, the corresponding transfer function and frequency response in their true continuous form, whereas, in the model checking based analysis, they are mostly discretized and modeled using a state-transition system, which may compromise the accuracy of the analysis.

The formalization of the transform methods presented in Sections 5 and 6 is mostly done interactively. However, we tried to automate the formal analysis of the industrial robot and the equalizer, presented in Section 7, by writing some automatic tactics. We developed DIFF_EQ_2_TRANS_FUN_TAC and TRANS_FUN_2_DIFF_EQ_TAC that have enabled us to formally analyze the industrial robot almost automatically. Similarly, we performed the automatic analysis of the equalizer using the tactics DIFF_EQ_2_FREQ_RES_TAC and FREQ_RES_2_DIFF_EQ_TAC that are also developed in our proposed formalization. The details about these automatic tactics can be found in the proof script [52].

8. Conclusion

This paper presented a framework for the formal transform methods based analysis of CPS. We mainly extended our formalization of the transform methods, which includes the formal definitions of the Laplace and the Fourier transforms, and verification of their various classical properties such as linearity, time shifting, frequency shifting, cosine and sine-based modulation, differentiation in time domain, time shifting, time scaling, time reversal and integration in time domain. We also formally verified the uniqueness properties of the Laplace and the Fourier transforms that enabled us to relate the frequency (s and ω) domain analysis of the continuous dynamics of CPS to their corresponding time-domain representations and thus completely analyze the differential equation based models of CPS. Finally, we used our proposed framework for formally analyzing an industrial robot and an equalizer using HOL Light.

In future, we plan to formalize the Vectorial Laplace transform [58], which is widely used for analyzing the Multiple-input Multiple-output (MIMO) control systems [58] modeled using the state space representations. Another future direction is to formalize the two-dimensional Fourier transform [4], which is widely used for analyzing the electromagnetic [59] and the optical systems [59].

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

We would like to thank John Harrison from Amazon Web Services for providing us guidance in the proof of the uniqueness of the Fourier transform.

References

[1] R. Rajkumar, I. Lee, L. Sha, J. Stankovic, Cyber-physical systems: The next computing revolution, in: Design Automation Conference, IEEE, 2010, pp. 731–736.
[2] M. Wazid, A.K. Das, R. Hussain, G. Succi, J.J. Rodrigues, Authentication in cloud-driven IoT-based big data environment: Survey and outlook, J. Syst. Archit. 97 (2019) 185–196.
[3] T. Goldschmidt, S. Hauck-Stattelmann, S. Malakuti, S. Grüner, Container-based architecture for flexible industrial control applications, J. Syst. Archit. 84 (2018) 28–36.
[4] R.J. Beerends, H.G. Morsche, J.C. Van den Berg, E.M. Van de Vrie, Fourier and Laplace Transforms, Cambridge University Press, 2003.
[5] J.L. Schiff, The Laplace Transform: Theory and Applications, Springer Science & Business Media, 2013.
[6] R.N. Bracewell, The Fourier Transform and its Applications, McGraw-Hill, 1978.
[7] A.J. Durán, M. Pérez, J.L. Varona, Misfortunes of a mathematicians' trio using computer algebra systems: Can we trust? 2013, CoRR abs/1312.3270.
[8] 2018. https://arstechnica.com/tech-policy/2018/05/report-software-bug-led-to-death-in-ubers-self-driving-crash/?amp=1.
[9] O. Hasan, S. Tahar, Formal verification methods, Encycl. Inf. Sci. Technol. IGI Global Pub (2015) 7162–7170.
[10] E.M. Clarke, P. Zuliani, Statistical model checking for cyber-physical systems, in: Automated Technology for Verification and Analysis, in: LNCS, vol. 6996, Springer, 2011, pp. 1–12.
[11] J. Harrison, Handbook of Practical Logic and Automated Reasoning, Cambridge University Press, 2009.
[12] R. Akella, B.M. McMillin, Model-checking BNDC properties in cyber-physical systems, in: Computer Software and Applications Conference, vol. 1, IEEE, 2009, pp. 660–663.
[13] M.U. Sardar, O. Hasan, Towards probabilistic formal modeling of robotic cell injection systems, in: Models for Formal Analysis of Real Systems, 2017, pp. 271–282.
[14] C. Baier, J.P. Katoen, K.G. Larsen, Principles of Model Checking, MIT press, 2008.
[15] S.H. Taqdees, O. Hasan, Formalization of laplace transform using the multivariable calculus theory of HOL-light, in: Logic for Programming, Artificial Intelligence, and Reasoning, in: LNCS, vol. 8312, Springer, 2013, pp. 744–758.
[16] S.H. Taqdees, O. Hasan, Formally verifying transfer functions of linear analog circuits, Design Test 34 (5) (2017) 30–37, http://dx.doi.org/10.1109/MDAT.2017.2713388.
[17] A. Rashid, O. Hasan, Formal analysis of linear control systems using theorem proving, in: Formal Engineering Methods, in: LNCS, vol. 10610, Springer, 2017, pp. 345–361.
[18] A. Rashid, U. Siddique, O. Hasan, Formal verification of platoon control strategies, in: Software Engineering and Formal Methods, in: LNCS, vol. 10886, Springer, 2017, pp. 223–238.
[19] A. Rashid, O. Hasan, On the formalization of fourier transform in higher-order logic, in: Interactive Theorem Proving, in: LNCS, vol. 9807, Springer, 2016, pp. 483–490.
[20] A. Rashid, O. Hasan, Formal analysis of continuous-time systems using fourier transform, J. Symbolic Comput. 90 (2019) 65–88.
[21] A. Rashid, O. Hasan, Formalization of lerch's theorem using HOL light, J. Appl. Logics IFCoLog J. Logics Appl. 5 (8) (2018) 1623–1652.
[22] L. Bu, Q. Wang, X. Chen, L. Wang, T. Zhang, J. Zhao, X. Li, Toward online hybrid systems model checking of cyber-physical systems' time-bounded short-run behavior, ACM SIGBED Rev. 8 (2) (2011) 7–10.
[23] A. Platzer, E.M. Clarke, Computing differential invariants of hybrid systems as fixedpoints, Form. Methods Syst. Des. 35 (1) (2009) 98–120.
[24] A. Platzer, E.M. Clarke, Formal verification of curved flight collision avoidance maneuvers: A case study, in: Formal Methods, in: LNCS, vol. 5850, Springer, 2009, pp. 547–562.
[25] A. Platzer, J.D. Quesel, European train control system: A case study in formal verification, in: Formal Engineering Methods, in: LNCS, vol. 5885, Springer, 2009, pp. 246–265.
[26] S.M. Loos, A. Platzer, L. Nistor, Adaptive cruise control: Hybrid, distributed, and now formally verified, in: Formal Methods, in: LNCS, vol. 6664, Springer, 2011, pp. 42–56.
[27] S. Mitsch, S.M. Loos, A. Platzer, Towards formal verification of freeway traffic control, in: Cyber-Physical Systems, IEEE Computer Society, 2012, pp. 171–180.
[28] S. Mitsch, K. Ghorbal, A. Platzer, On provably safe obstacle avoidance for autonomous robotic ground vehicles, in: Robotics: Science and Systems, 2013.
[29] J.B. Jeannin, K. Ghorbal, Y. Kouskoulas, R. Gardner, A. Schmidt, E. Zawadzki, A. Platzer, Formal verification of ACAS X, an industrial airborne collision avoidance system, in: Embedded Software, IEEE, 2015, pp. 127–136.
[30] A. Platzer, Differential dynamic logic for verifying parametric hybrid systems, in: Automated Reasoning with Analytic Tableaux and Related Methods, in: LNCS, vol. 4548, Springer, 2007, pp. 216–232.
[31] C. Bernardeschi, A. Domenici, P. Masci, A PVS-simulink integrated environment for model-based analysis of cyber-physical systems, Trans. Softw. Eng. 44 (6) (2018) 512–533.
[32] M.U. Sanwal, O. Hasan, Formal verification of cyber-physical systems: Coping with continuous elements, in: Computational Science and Its Applications, in: LNCS, vol. 7971, Springer, 2013, pp. 358–371.
[33] A. Rashid, O. Hasan, Formalization of transform methods using HOL light, in: Intelligent Computer Mathematics, in: LNCS, vol. 10383, Springer, 2017, pp. 319–332.
[34] F. Immler, Laplace Transform - archive of formal proofs, 2018, https://www.isa-afp.org/entries/Laplace_Transform.html.
[35] Z. Gang, Z. Chun-na, G. Yong, L. Xing-li, L. Xiao-juan, Formalization of Laplace transform calculus in HOL4, J. Chin. Comput. Syst. 35 (9) (2014) 2177–2181.
[36] Y. Wang, G. Chen, Formalization of Laplace transform in Coq, in: Dependable Systems and their Applications, IEEE, 2017, pp. 13–21.
[37] A. Rashid, O. Hasan, Formal analysis of continuous-time systems using fourier transform, J. Symbolic Comput. 90 (2019) 65–88.
[38] U. Siddique, M.Y. Mahmoud, S. Tahar, On the formalization of Z-Transform in HOL, in: Interactive Theorem Proving, in: LNCS, vol. 8558, Springer, 2014, pp. 483–498.
[39] U. Siddique, M.Y. Mahmoud, S. Tahar, Formal analysis of discrete-time systems using Z-transform, J. Appl. Logics IFCoLog J. Logics Appl. 5 (4) (2018).
[40] Z. Shi, Y. Zhang, Y. Guan, L. Li, J. Zhang, The formalization of discrete fourier transform in HOL, Math. Probl. Eng. 2015 (2015).
[41] Y. Guan, J. Zhang, Z. Shi, Y. Wang, Y. Li, Formalization of continuous fourier transform in verifying applications for dependable cyber-physical systems, J. Syst. Archit. (2020) 101707.
[42] J. Harrison, The HOL light theory of euclidean space, J. Automat. Reason. 50 (2) (2013) 173–190.
[43] A.M. Cohen, Numerical Methods for Laplace Transform Inversion, vol. 5, Springer Science & Business Media, 2007.
[44] J. Orloff, Uniqueness of Laplace transform, 2015, http://web.mit.edu/jorloff/www/18.03-esg/notes/extra/laplaceuniqueness.pdf.
[45] D. Newman, Fourier uniqueness via complex variables, Amer. Math. Monthly 81 (4) (1974) 379–380.
[46] P.D. Lax, L. Zalcman, Complex Proofs of Real Theorems, vol. 58, American Mathematical Society, 2011.
[47] T. Gamelin, Complex Analysis, Springer Science & Business Media, 2003.
[48] C. Swartz, Introduction to Gauge Integrals, World Scientific, 2001.
[49] B. Fine, G. Rosenberger, The Fundamental Theorem of Algebra, Springer Science & Business Media, 2012.
[50] H.J. Wilcox, D.L. Myers, An Introduction to Lebesgue Integration and Fourier Series, Courier Corporation, 2012.
[51] J. Yeh, Real Analysis: Theory of Measure and Integration, World Scientific Publishing Company, 2006.
[52] A. Rashid, Formal analysis of the continuous dynamics of cyber-physical systems using theorem proving, 2020, http://save.seecs.nust.edu.pk/projects/facdcpstp/.
[53] J. Luh, An anatomy of industrial robots and their controls, Trans. Autom. Control 28 (2) (1983) 133–153.
[54] J. Luh, Conventional controller design for industrial robots—A tutorial, Trans. Syst. Man Cybern. (3) (1983) 298–316.
[55] F.L. Luo, C. Zhang, Signal Processing for 5G: Algorithms and Implementations, John Wiley & Sons, 2016.
[56] L. Tan, J. Jiang, Fundamentals of Analog and Digital Signal Processing, AuthorHouse, 2007.
[57] H. Zumbahlen, Basic Linear Design, Analog Devices Norwood, MA, 2007.
[58] C.H. Houpis, S.N. Sheldon, Linear Control System Analysis and Design with MATLAB, CRC Press, 2013.
[59] M. Born, E. Wolf, Principles of Optics: Electromagnetic Theory of Propagation, Interference and Diffraction of Light, Elsevier, 1980.

Adnan Rashid received his Ph.D. degree in Information Technology from School of Electrical Engineering and Computer Science (SEECS), National University of Science and Technology (NUST), Islamabad, Pakistan, in 2019. Prior to this, he received the M.Sc. and M.Phil. degree in Electronics from the Department of Electronics, Quaid-iAzam University (QAU), Islamabad, Pakistan, in 2008 and 2012, respectively. Currently, he is working as a Research Associate with the System Analysis and Verification (SAVe) laboratory in SEECS, NUST, Islamabad, Pakistan. He has also worked as a Visiting Researcher at Hardware Verification Group (HVG), Concordia University, Canada in 2018. He has a strong interest in Formal Methods, with their applications in Control Systems, Analog Circuits, Biological Systems, Robotic Systems, Communication Systems and Transportation Systems. He has served as a chair of the Doctoral program at Conference on Intelligent Computer Mathematics, Edinburgh, UK, in 2017.

Osman Hasan received his BEng (Hons) degree from the University of Engineering and Technology, Peshawar Pakistan in 1997, and the MEng and PhD degrees from Concordia University, Montreal, Quebec, Canada in 2001 and 2008, respectively. Before his Ph.D., he worked as an ASIC Design Engineer from 2001 to 2004 at LSI Logic. He worked as a postdoctoral fellow at the Hardware Verification Group (HVG) of Concordia University for one year until August 2009. Currently, he is an Associate Professor and the Head of Department of Electrical Engineering at the School of Electrical Engineering and Computer Science of National University of Science and Technology (NUST), Islamabad, Pakistan. He is the founder and director of System Analysis and Verification (SAVe) Lab at NUST, which mainly focuses on the design and formal verification of energy, embedded and ehealth related systems. He has received several awards and distinctions, including the Pakistan's Higher Education Commission's Best University Teacher (2010) and Best Young Researcher Award (2011) and the President's gold medal for the best teacher of the University from NUST in 2015. Dr. Hasan is a senior member of IEEE, member of the ACM, Association for Automated Reasoning (AAR) and the Pakistan Engineering Council.