EasyChair Preprint

№ 8009

Formalization of Transform Methods in Higher-Order Logic: a Survey

Muhammad Ahmed and Adnan Rashid

May 22, 2022

Formalization of Transform Methods in Higher-order Logic: A Survey

Muhammad Ahmed and Adnan Rashid

School of Electrical Engineering and Computer Science (SEECS)
National University of Sciences and Technology (NUST)
Islamabad, Pakistan
{mahmed.mscs19seecs,adnan.rashid}@seecs.nust.edu.pk

Abstract

Most of the engineering and physical systems are generally characterized by differential equations or difference equations based on their continuous-time and discrete-time dynamics, respectively. Moreover, these dynamical models are analyzed using transform methods to find out solutions of the differential/difference equations and prove their various properties, such as, transfer function, frequency response and stability. The Laplace and the Fourier transforms are used for analyzing systems exhibiting continuous dynamics. Whereas, the Discrete Fourier Transform (DFT) and the z-transform are their counterpart in the discrete time. The conventional techniques for performing the transform methods based analysis cannot provide an accurate analysis of the corresponding systems due to their inherent limitations. To overcome these limitations, formal methods, in particular, theorem proving, has been used, as a complementary technique, for analyzing systems based on transform methods and thus ascertain an accurate analysis. In this paper, we survey the developments in the use of higher-order-logic theorem proving for transform methods based analysis and overview the corresponding real world case studies from the avionics, medicine and transportation domains that have been analyzed based on these developments.

1 Introduction

The engineering and physical systems exhibiting dynamical behaviours are generally modeled using differential [Y+13] and difference [KP01] equations based on their corresponding dynamics that can be continuous-time and discrete-time, respectively. To analyze these models capturing the dynamics of such systems, transform methods, such as, the Laplace transform [BMVdBVdV03], the Fourier transform [BB86], the Discrete Fourier Transform (DFT) [Sun01] and the z-Transform [OBS01], have been widely used. These transform methods facilitate finding out solutions of these differential and difference equations based models and analyzing their various important properties, such as, transfer function, frequency response and stability, as shown in Figure 1.
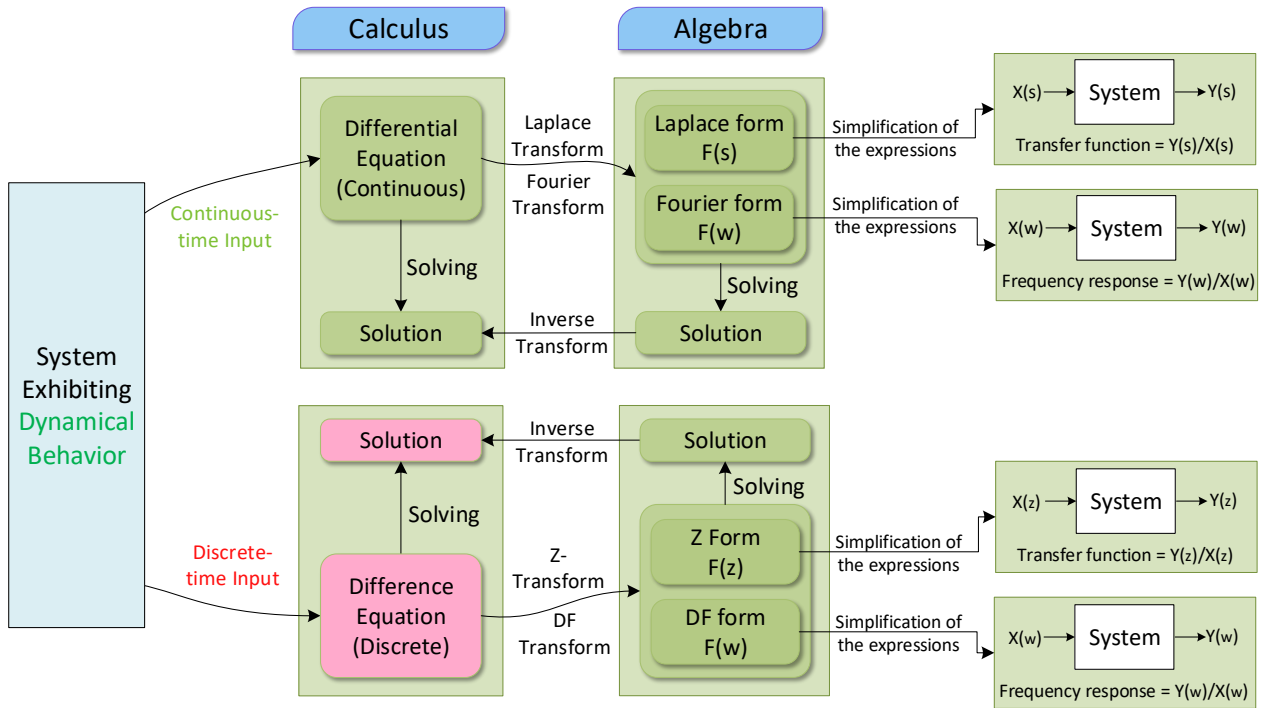
Figure 1: Transform Methods

The continuous-time dynamical behaviour of a system is generally modeled using differential equations. These differential equations based modeled are not easier to analyze in time-domain, especially, for the case of larger systems (n-order differential equations for larger n). Transform methods, which include the Laplace and the Fourier transforms have been widely used to analyze these differential equations. These methods involve a transformation of the time-domain model to its corresponding frequency domain representation (s-domain for the Laplace and ω-domain for the Fourier transform), which converts the differential equations involving integrals and differentials to their corresponding algebraic equations having multiplication and division operators, as shown in Figure 1. These equations are further solved to analyze various properties of the system, such as, transfer function and frequency response, and to obtain solutions in frequency domain [BMVdBVdV03, BB86]. Finally, the inverse transforms (the inverse Laplace and the inverse Fourier) are applied to obtain the time-domain solutions of the differential equations based models.

Similarly, the dynamics of a discrete-time system are captured using difference equations. These difference equations based models are analyzed using the discrete-time transform methods, which include the Discrete Fourier Transform (DFT) and the z-transform. These transform methods perform a conversion of the discrete time model to its corresponding frequency domain representation (z-domain for the z-transform and ω for the DFT), as shown in Figure 1. These representations are further solved to analyze various properties of the given system, such as, transfer function and frequency response, and to obtain solutions in frequency domain [Sun01, OBS01]. Finally, the inverse transforms are applied to obtain the time-domain solutions of the difference equations based models.

Conventionally, the transform methods based analysis has been performed using paper-and-pencil based proofs and computer based symbolic and numerical techniques. However, these methods suffer from their inherent limitations and thus compromise the accuracy of the analysis [DPV13]. Formal methods [HT15], in particular, higher-order-logic theorem proving [Har09] can overcome the limitations of the conventional methods and thus provides an accurate transform methods based analysis of the systems. It has been widely used for the transform methods based analysis of the engineering and physical systems. These transform methods have been formalized using various higher-order-logic theorem provers, such as, HOL Light [Har96], HOL4 [SN08], Coq [BC13] and Isabelle [Pau94]. Moreover, these formalizations have been used for analyzing various safety-critical systems, such as, linear analog circuits, automobile suspension systems, a drug therapy model, unmanned aerial vehicles, synthetic biological circuits, power converters and digital filters. In this paper, we survey all these contributions

regarding formalization of transform methods that have been done using higher-order-logic theorem proving.

The rest of the paper is organized as follows: Section 2 provides the developments of the Laplace and the Fourier transforms in various theorem provers and their associated analysis of the continuous-time systems. We provide the formalization of the DFT and the z-transform and the associated analysis of the discrete-time systems in Section 3. Section 4 presents a discussion about the features and availability of the transform methods based analysis and its comparison in different theorem provers. Finally, Section 5 concludes the paper.

2 Transform Methods for Analyzing Continuous-time Systems

The Laplace and the Fourier transforms have been formalized using various higher-order-logic theorem provers. Moreover, these formalizations have been used for formally analyzing many engineering and physical systems. Taqdees et al. [TH13] formalized the Laplace transform using multivariate calculus theories of HOL Light. This formalization mainly includes the formal definition of the Laplace transform and the formal verification of its various properties, such as, linearity, frequency shifting, first-order differentiation, higher-order differentiation and integration in time-domain. Moreover, the authors used their formalization of the Laplace transform for formally verifying the transfer function of a 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 first-order and second-order Sallen-Key low-pass filters by formalizing the system governing laws such as Kirchhoff's Current Law (KCL) and Kirchhoff's Voltage Law (KVL) using HOL Light [TH17]. Later, Rashid et al. [RH17] proposed a new formalization of the Laplace transform based on the notion of sets and verified some more properties of the Laplace transform, such as, time shifting, time scaling, the Laplace transform a n-order differential equation and uniqueness [RH18]. The authors also formally verified the Laplace transform of some commonly used functions, such as, exponential function, sine and cosine functions. Finally, they used their proposed formalization of the Laplace transform for analyzing the control system of an Unmanned Free-swimming Submersible (UFSS) vehicle[RH17] and 4-π soft error cross talk model [RH18]. Similarly, the formalization of the Laplace transform has been used for formally analyzing the unmanned aerial vehicles [ARH20b] and synthetic biological circuits [ARH20a, RH+20].

Wang et al. [WC17] provided a formalization of the Laplace transform using the Coq theorem prover. The authors formally defined the Laplace transform and formally verified a few of its classical properties, such as, linearity, frequency shifting and differentiation in time domain. Moreover, they applied their proposed formalization for formally verifying a flight control system using Coq. Similarly, Immler [Imm21] formalized the Laplace transform using the Isabelle theorem prover. The authors mainly verified some of the classical properties of the Laplace transform, such as, linearity, frequency shifting, uniqueness, differentiation and integration in time-domain. Gang et al. [GCnY+14] used HOL4 for the formalization of the Laplace transform. The authors formally modeled the Laplace transform and verified some of its classical properties, such as, linearity, frequency shifting, differentiation and integration in time domain. Next, they used their proposed formalization for formally verifying the transfer function of a motor.

Table 1: Continuous-time Transform Methods in Various Theorem Provers

Transform Methods	Theorem Prover	Formalization Details/ Verified Properties
Laplace Transform	Coq	Linearity, frequency shifting, differential [WC17]
	HOL Light	Linearity, frequency shifting, integration, time shifting, time scaling, first-order and higher-order differentiations in time domain [TH13, RH18]
	Isabelle	Linearity, frequency shifting, integration, first-order and higher-order differentiations in time domain, integration [Imm21]
	HOL4	Linearity, frequency shifting, differentiation and integration in time domain [GCnY+14]
Fourier Transform	HOL Light	Linearity, frequency shifting, modulation, time reversal, first-order and higher-order differentiations in time domain [RH19]
	HOL4	Linearity, time reversal, frequency shifting, differentiation, and integration in time domain [GZS+20]

Rashid et al. [RH16] formalized the Fourier transform using the HOL Light theorem prover. The authors

provided a formal definition of the Fourier transform and formally verified its various classical properties, such as, linearity, frequency shifting, modulation, time reversal, first-order and higher-order differentiations in time-domain. Also, they formally verified the Fourier transform of some commonly used functions, such as, exponential, sine and cosine functions. Moreover, they used their proposed formalization for formally analyzing an Automobile Suspension System (ASS), an audio equalizer, a drug therapy model and a MEMs accelerometer [RH19]. Similarly, Guan et al. [GZS$^+$20] formalized the Fourier transform using HOL4. The authors provided a formal definition of the Fourier transform and formally verified its various properties, such as, linearity, time reversal, frequency shifting, differentiation and integration in time domain. Moreover, they used their proposed formalization for formally verifying the frequency response of a RLC circuit. A summary of the formalizations of the Laplace and the Fourier transforms in various theorem provers and the systems that have been formally analyzed using these transform methods can be found in Tables 1 and 2

Table 2: Analysis of Continuous-time Systems using Transform Methods

Transform Methods	Theorem Provers	Applications
Laplace Transform	Coq	Flight control system [WC17]
	HOL Light	LTC [TH13], UFSS vehicle [RH17], 4-π soft error cross talk model [RH18], Sallen-Key low-pass filter [TH17], unmanned aerial vehicles [ARH20b], synthetic biological circuits [ARH20a, RH$^+$20]
	Isabelle	No application
	HOL4	Motor [GCnY$^+$14]
Fourier Transform	HOL Light	Automobile suspension system [RH16], a drug therapy model [RH19], an audio equalizer [RH19], MEMs accelerometer [RH19]
	HOL4	RLC circuit [GZS$^+$20]

3 Transform Methods for Analyzing Discrete-time Systems

The DFT and z-Transform have been formalized using various higher-order-logic theorem provers. Moreover, these formalizations have been used for formally analyzing many discrete-time systems. Siddique et al. [SMT14] formalized z-transform using the HOL Light theorem prover. The authors provided a formal definition of the z-transform and formally verified its various properties, such as, linearity, time shifting and scaling in z-domain. Moreover, they used their proposed formalization 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 verification of some more properties, such as, time scaling, complex conjugate and a formal support for the inverse z-transform and used it for formally analyzing a switched-capacitor interleaved DC-DC voltage doubler [SMT18].

Table 3: Discrete-time Transform Methods in Various Theorem Provers

Transform Methods	Theorem Prover	Formalization Details/ Verified Properties
DFT	HOL4	Implicit periodicity, linearity, symmetry, frequency shifting, time shifting, convolution [SZG$^+$15]
FFT	HOL4	FFT, inverse FFT [AT04]
	Coq	FFT [Cap01]
z-Transform	HOL Light	linearity, time shifting and scaling in z-domain, time scaling, complex conjugation, inverse z-transform [SMT18]

Shi et al. [SZG$^+$15] proposed a formalization of DFT using the HOL4 theorem prover. The authors presented a formal definition of the DFT and formally verified its various properties, such as, implicit periodicity, linearity, symmetry, frequency shifting, time sifting and convolution. Moreover, the authors used their proposed formalization for formally verifying Fast Fourier Transform (FFT) and cosine frequency shifting. Capretta et al. [Cap01] formally verified the FFT using the Coq theorem prover. Similarly, Akbarpour et al. [AT04] provided a formal specification and verification of the FFT at different abstraction levels using the HOL4 theorem prover. A summary of the formalization of the transform methods for discrete-time systems in various theorem provers and their associated applications can be found in Tables 3 and 4.

Table 4: Analysis of Discrete-time Systems using Transform Methods

Transform methods	Theorem Provers	Formalization Details / Verified Properties
DFT	HOL4	FFT, cosine frequency shifting [SZG$^+$15]
FFT	HOL4	FFT at different levels of abstraction and inverse FFT [AT04]
	Coq	FFT [Cap01]
Z-Transform	HOL Light	IIR DSP filter [SMT14], switched-capacitor interleaved DC-DC voltage doubler [SMT18]

4   Theorem Proving Support for Transform Methods based Analysis

Figure 2 depicts the formal libraries of transform methods that are available in various higher-order-logic theorem provers for performing the analysis of the engineering and physical systems. For example, the Laplace transform is available in most of the theorem provers. Moreover, its formal library in the HOL Light theorem prover is quite dense and has been frequently used for analyzing various safety-critical systems as given in Table 2. Similarly, the transform methods for formally analyzing the continuous-time systems, i.e., the Laplace and the Fourier transforms, are only available in HOL Light. Also, the z-transform is only available in HOL Light. Similarly, HOL4 contains both the continuous-time and discrete-time Fourier transforms. Moreover, no transform methods is available in the PVS theorem prover.
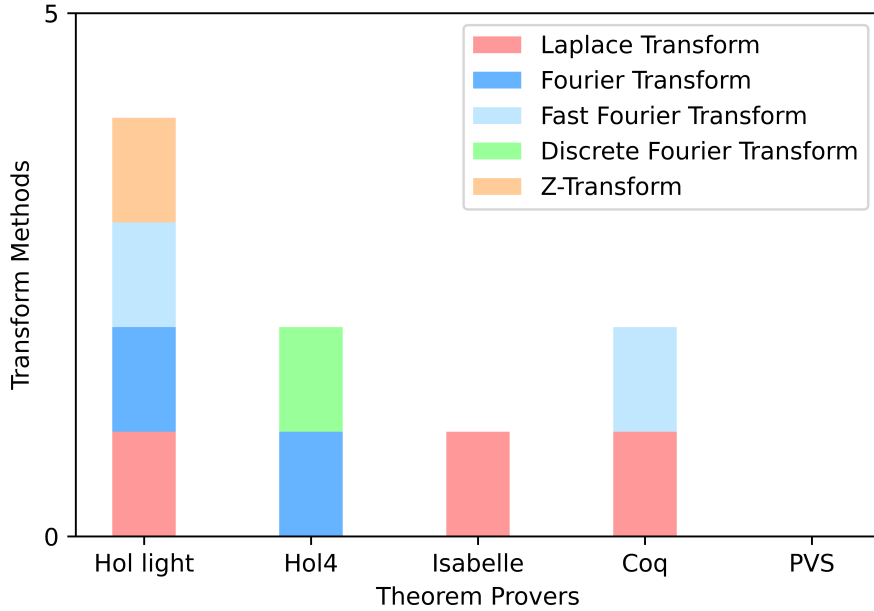

Figure 2: Transform Methods in Higher-order-logic Theorem Provers

5   Conclusion

Transform methods are widely used for analyzing the engineering and physical systems exhibiting dynamical behaviours. Due to the safety-critical nature of these system, their accurate analysis is of utmost importance. This paper surveys the transform methods that have been formalized using different theorem provers by highlighting various safety-critical systems that have been formally analyzed based on transform methods. In this regard, only HOL Light theorem prover contains most number of transform methods, such as, the Laplace and the Fourier transforms, and the z-transform. Similarly, PVS contains no transform methods library and we need to develop these libraries that can be used for performing transform methods based analysis using PVS.

References

[ARH20a]   Sa'ed Abed, Adnan Rashid, and Osman Hasan. Formal Analysis of the Biological Circuits using Higher-order-logic Theorem Proving. In *ACM Symposium on Applied Computing*, pages 3–7, 2020.

[ARH20b]   Sa'ed Abed, Adnan Rashid, and Osman Hasan. Formal Analysis of Unmanned Aerial Vehicles Using Higher-Order-Logic Theorem Proving. *Journal of Aerospace Information Systems*, 17(9):481–495, 2020.

[AT04]   Behzad Akbarpour and S Tahar. Verification of the Fast Fourier Transform using HOL Theorem Proving. *Techincal Report, Concordia University, Montreal-Canada*, 2004.

[BB86]   Ronald Newbold Bracewell and Ronald N Bracewell. *The Fourier Transform and its Applications*, volume 31999. McGraw-Hill, 1986.

[BC13]   Yves Bertot and Pierre Castéran. *Interactive Theorem Proving and Program Development: Coq'Art: the Calculus of Inductive Constructions*. Springer Science & Business Media, 2013.

[BMVdBVdV03]   R. J. Beerends, H. G. Morsche, J. C. Van den Berg, and E. M. Van de Vrie. *Fourier and Laplace Transforms*. Cambridge University Press, 2003.

[Cap01]   Venanzio Capretta. Certifying the Fast Fourier Transform with Coq. In *Theorem Proving in Higher Order Logics*, volume 2152 of *LNCS*, pages 154–168. Springer, 2001.

[DPV13]   Antonio J Durán, Mario Pérez, and Juan L Varona. The Misfortunes of a Mathematicians' Trio using Computer Algebra Systems: Can We Trust? *CoRR*, abs/1312.3270, 2013.

[GCnY+14]   Zhao Gang, Zhao Chun-na, Guan Yong, Lv Xing-li, and Li Xiao-juan. Formalization of Laplace Transform Calculus in HOL4. *Journal of Chinese Computer Systems*, 35(9):2177–2181, 2014.

[GZS+20]   Yong Guan, Jie Zhang, Zhiping Shi, Yi Wang, and Yongdong Li. Formalization of Continuous Fourier Transform in Verifying Applications for Dependable Cyber-physical Systems. *Journal of Systems Architecture*, 106:101707, 2020.

[Har96]   John Harrison. HOL Light: A Tutorial Introduction. In *Formal Methods in Computer-Aided Design*, volume 1166 of *LNCS*, pages 265–269. Springer, 1996.

[Har09]   John Harrison. *Handbook of Practical Logic and Automated Reasoning*. Cambridge University Press, 2009.

[HT15]   Osman Hasan and Sofiène Tahar. Formal Verification Methods. *Encyclopedia of Information Science and Technology, IGI Global Pub*, pages 7162–7170, 2015.

[Imm21]   Fabian Immler. Laplace Transform. 2021.

[KP01]   Walter G Kelley and Allan C Peterson. *Difference Equations: an Introduction with Applications*. Academic Press, 2001.

[OBS01]   Alan V Oppenheim, John R Buck, and Ronald W Schafer. *Discrete-time Signal Processing*. Prentice Hall, 2001.

[Pau94]   Lawrence C Paulson. *Isabelle: A Generic Theorem Prover*, volume 828. Springer Science & Business Media, 1994.

[RH16]   Adnan Rashid and Osman Hasan. On the Formalization of Fourier Transform in Higher-order Logic. In *Interactive Theorem Proving*, volume 9807 of *LNCS*, pages 483–490. Springer, 2016.

[RH17]   Adnan Rashid and Osman Hasan. Formal Analysis of Linear Control Systems using Theorem Proving. In *Formal Engineering Methods*, pages 345–361. Springer, 2017.

[RH18]   Adnan Rashid and Osman Hasan. Formalization of Lerch's Theorem using HOL Light. *Journal of Applied Logics*, 5(8):1623–1652i, 2018.

[RH19]   Adnan Rashid and Osman Hasan. Formal Analysis of Continuous-time Systems using Fourier Transform. *Journal of Symbolic Computation*, 90:65–88, 2019.

[RH+20]   Adnan Rashid, Osman Hasan, et al. Formal Reasoning about Synthetic Biology using Higher-order-logic Theorem Proving. *IET Systems Biology*, 14(5):271–283, 2020.

[SMT14]   Umair Siddique, Mohamed Yousri Mahmoud, and Sofiene Tahar. On the Formalization of z-Transform in HOL. In *Interactive Theorem Proving*, volume 8558 of *LNCS*, pages 483–498. Springer, 2014.

[SMT18]   Umair Siddique, Mohamed Yousri Mahmoud, and Sofiène Tahar. Formal Analysis of Discrete-Time Systems using z-Transform. *Journal of Applied Logics*, 5(4):875–906, 2018.

[SN08]   Konrad Slind and Michael Norrish. A Brief Overview of HOL4. In *Theorem Proving in Higher Order Logics*, pages 28–32. Springer, 2008.

[Sun01]   Duraisamy Sundararajan. *The Discrete Fourier Transform: Theory, Algorithms and Applications*. World Scientific, 2001.

[SZG+15]   Zhiping Shi, Yupeng Zhang, Yong Guan, Liming Li, and Jie Zhang. The Formalization of Discrete Fourier Transform in HOL. *Mathematical Problems in Engineering*, 2015, 2015.

[TH13]   Syeda Hira Taqdees and O. Hasan. Formalization of Laplace Transform Using the Multivariable Calculus Theory of HOL-Light. In *Logic for Programming, Artificial Intelligence, and Reasoning*, volume 8312 of *LNCS*, pages 744–758. Springer, 2013.

[TH17]   Syeda Hira Taqdees and Osman Hasan. Formally Verifying Transfer Functions of Linear Analog Circuits. *IEEE Design & Test*, 34(5):30–37, 2017.

[WC17]   Yifei Wang and Gang Chen. Formalization of Laplace Transform in Coq. In *Dependable Systems and Their Applications*, pages 13–21. IEEE, 2017.

[Y+13]   Xin-She Yang et al. *Mathematical Modeling with Multidisciplinary Applications*. Wiley, 2013.