

# Formal Analysis of Power Electronics Circuits using Theorem Proving



By

Asad Ahmed

(Registration No: NUST201490133PSEECSS2014S)

Thesis Supervisor: Dr. Osman Hasan

Department of Computing  
School of Electrical Engineering and Computer Science,  
National University of Sciences & Technology (NUST)

Islamabad, Pakistan

(2022)

# Formal Analysis of Power Electronics Circuits using Theorem Proving



By

**Asad Ahmed**

(Registration No: NUST201490133PSEECSS2014S)

A thesis submitted to the National University of Sciences and Technology, Islamabad,

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in  
Information Technology

Thesis Supervisor: Dr. Osman Hasan

Department of Computing  
School of Electrical Engineering and Computer Science,  
National University of Sciences & Technology (NUST)

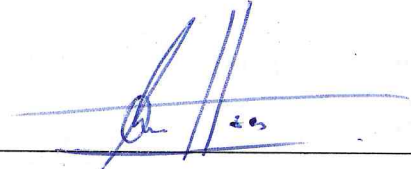
Islamabad, Pakistan

(2022)

**THESIS ACCEPTANCE CERTIFICATE**

Certified that final copy of PhD Thesis written by Mr. **Asad Ahmed**, Registration No. **NUST201490133PSEECSS2014S**, of School of Electrical Engineering and Computer Science (SEECSS), National university of Sciences and Technology (NUST) has been vetted by undersigned, found complete in all respects as per NUST Statutes / Regulations / PhD Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of PhD degree. It is further certified that necessary amendments as pointed out by GEC members and foreign/local evaluators of the scholar have also been incorporated in the said thesis.

Signature: \_\_\_\_\_



Name of Supervisor \_\_\_\_\_

Dr. Osman Hasan

Date: \_\_\_\_\_

28/1/2022

Signature (HOD): \_\_\_\_\_



Senior HOD DOC  
SEECSS-NUST  
Sector H-12 Islamabad

Date: \_\_\_\_\_

Signature (Dean/Principal) \_\_\_\_\_



Date: \_\_\_\_\_

31 JAN 2022

Principal  
NUST School of Electrical  
Engineering & Computer Science  
(Dr. Muhammad Ajmal)



**National University of Sciences & Technology**  
**REPORT OF DOCTORAL THESIS DEFENCE**

Name: Asad Ahmed NUST Regn No: NUST201490133PSEECs2014S

School/College/Centre: School of Electrical Engineering and Computer Science

Title: Formal Analysis of Power Electronics Circuits using Theorem Proving

**DOCTORAL DEFENCE COMMITTEE**

Doctoral Defence held on 20 January 2022

	<u>QUALIFIED</u>	<u>NOT QUALIFIED</u>	<u>SIGNATURE</u>
GEC Member-1: <u>Dr. Ammar Hasan</u>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
GEC Member-2: <u>Dr. Safdar Abbas Khan</u>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
GEC Member (External): <u>Dr. Muhammad Asif Farooq</u>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Supervisor: <u>Dr. Osman Hasan</u>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Co Supervisor (if appointed): _____	<input type="checkbox"/>	<input type="checkbox"/>	_____
External Evaluator-1: <u>Dr. Muhammad Zohaib Iqbal</u> (Local Expert)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
External Evaluator-2: <u>Dr. Muddassar Azam Sindhu</u> (Local Expert)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
External Evaluator-3: <u>Dr. Mohamed Zaki Hussein</u> (Foreign Expert)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	_____
External Evaluator-4: <u>Dr. Jacques Fleuriot</u> (Foreign Expert)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	_____

**FINAL RESULT OF THE DOCTORAL DEFENCE**  
 (Appropriate box to be signed by HOD)

**PASS**

**FAIL**

The student Asad Ahmed Regn No NUST201490133PSEECs2014S is accepted for Doctor of Philosophy Degree.

Dated: 28 JAN 2022

Principal  
 NUST School of Electrical  
 Engineering & Computer Science  
 (Dr. Muhammad Ajmal)

**Distribution:**

01 x original copy each for PGP Dte, Exam Branch Main Office NUST and Student's dossier at the School/College/Centre.

01 x photocopy each for HoD, Supervisor, Co-Supervisor (if appointed), sponsoring agency (if any) and 05 copies for insertion in Dissertation.

Note: \* Decision of External Evaluators (Foreign Experts) will be sought through video conference, if possible, on the same date and their decision will be intimated (on paper) to HQ NUST at a later date.



## Certificate of Approval

This is to certify that the research work presented in this thesis, titled “**Formal Analysis of Power Electronics Circuits using Theorem Proving**” was conducted by Mr. Asad Ahmed under the supervision of **Dr. Osman Hasan**. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the **School of Electrical Engineering and Computer Science (SEECS)** in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Field of **Information Technology** Department of **School of Electrical Engineering and Computer Science (SEECS)** University of **National University of Sciences and Technology (NUST), Islamabad, Pakistan**.

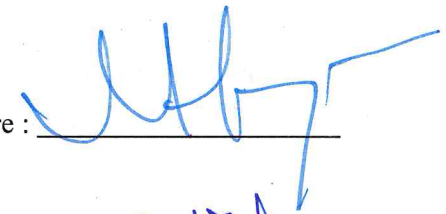
Student Name: Asad Ahmed

Signature : 


Examination Committee:

a) External Examiner 1: Dr. Muhammad Zohaib Iqbal Signature : 

Professor, Director at  
FAST-National University  
of Computer & Emerging Sciences,  
Islamabad Campus. Pakistan.

b) External Examiner 2: Dr. Muddassar Azam Sindhu Signature : 

Associate Professor,  
Department of Computer Science,  
Quaid-i-Azam University, Islamabad, Pakistan.

c) Internal Examiner: Dr. Safdar Abbas Khan Signature : 

HOD Department of Computing  
School of Electrical Engineering & Computer Science,  
National University of Sciences and Technology,  
Islamabad, Pakistan.

Supervisor: Dr. Osman Hasan

Signature : 

Name of Dean/HOD: Dr. Hasan Tahiro

Signature : 


Senior HOD DOC  
SEECS-NUST  
Sector H-12 Islamabad

## Author's Declaration

I **Asad Ahmed** hereby state that my PhD thesis title "**Formal Analysis of Power Electronics Circuits using Theorem Proving**" is my own work and has not been submitted previously by me for taking any degree from this University **National University of Sciences and Technology (NUST)**, Islamabad, Pakistan or anywhere else in the country/world.

At any time if my statement is found incorrect even after my Graduation the university has the right to withdraw my PhD degree.

Name of Student: **Asad Ahmed**

Signature: 

Date: 22-01-2022

# Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled "**Formal Analysis of Power Electronics Circuits using Theorem Proving**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and University **National University of Sciences and Technology, Islamabad, Pakistan** towards plagiarism. Therefore I as an Author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of PhD degree, the University reserves the rights to withdraw/revoke my PhD degree and that HEC and the University has right to publish my name on the HEC/University Website on which names of students are placed who submitted plagiarized thesis.

Student/Author Signature: \_\_\_\_\_

Name: Asad Ahmed

*Asad Ahmed*  
*22-01-2022*

# Dedication

To My Parents



# Acknowledgment

First and foremost, I wish to express my deepest appreciation to my supervisor, Dr. Osman Hasan, who introduced me to the exciting field of formal methods and provided me with an outstanding guidance during my doctoral degree. He was always accessible and his professional mentorship played a key role in shaping and strengthening this research. No doubt, his passion for quality research, phenomenal management skills, immense knowledge of the formal methods and refined and disciplined approach towards life has profoundly and positively affected and inspired me on both personal and professional levels. I would also like to thank him for providing me an opportunity to work as a Research Assistant at SAVe lab which significantly helped me to manage my finances and focus on my research.

I am also thankful to my GEC members for sparing time, from their busy schedule, for six monthly progress meetings. The valuable feedback and suggestions have been very useful for setting my research direction. Especially, I am very grateful to Dr. Ammar Hasan for instigating the idea of the formal analysis of power electronics circuits. No doubt, this well-thought and genuine idea ripen into this thesis.

I am also grateful to Prof. Falah Awwad, from Al-Ain, United Arab Emirates University, for his collaboration on the formal verification of the power electronics applications in smart grids. This experience was very useful and fruitful in terms of expanding the horizon of the research to incorporate the formal verification of state-of-the-art power processing applications.

Thanks are also extended to present and former fellow graduate students, especially, Dr. Waqar Ahmed and Mr. Syed Asadullah Bukhari, for their excellent company during my PhD studies.

Last but by no means least, I feel great pleasure in paying tribute to my family. I cannot express my gratitude in words for the contributions of my parents in my life. Their love and passion for learning and knowledge has always been the main motivation behind all my academic journeys. Despite having only basic education, they understood well the worth of knowledge and worked hard to facilitate their children in acquiring highest education degrees. I am also very thankful to my brothers, Ashiq, Faisal, Qamar and Umair, who stood beside me through all the thick and thins of life. My sister always motivated me to pursue my goals, wholeheartedly. Finally, it would have not been possible for me to go through all the uncertain and tough times of my PhD without an unconditional love and support provided by my better half. She not only took care of the family, when I was busy in research, but also encouraged me by trusting and believing in my convictions in very testing times. I would also like to mention my daughters, Ayma and Hania, and son, Rohan, for introducing me to a new and refreshing prospect of the life and renewed my motivation for achieving my goals.

# Abstract

Power electronics systems are extensively used in many engineering systems, such as hand-held devices, medical equipment, electric vehicles, aerospace artifacts, power grids, nuclear power plants and military equipment. Power electronics are characterized by the highly-nonlinear behavior due to the involvement of semiconductor switches for power conversion. Mathematical concepts of basic circuit theory, operational calculus, differential theory, integration theory and control theory are involved in modeling their behavior. Traditionally, paper-and-pencil proof methods and computer-based simulations are used to perform the analysis and design of power electronics systems. However, these traditional analysis techniques suffer from several limitations, such as human-error, discretization and truncation errors, and thus cannot guarantee an accurate analysis and verification of power electronics circuits. Whereas, accurate analysis and design of power electronic circuits is mandatory for the safety and mission-critical engineering applications, such as medical equipment, transportation and smart grids. To overcome the shortcomings of the traditional analysis techniques, we propose a higher-order-logic theorem proving based framework to formally analyze and verify power electronic systems accurately and exhaustively. Higher-order logic is highly expressive and allows modeling complex system behaviors, whereas, the soundness of theorem provers ensure accurate analysis and verification of the systems.

The proposed framework, mainly, enables time and complex-domain anal-

ysis and design of power electronics systems within the HOL `Light` theorem prover. The formalization in the time-domain paradigm allows to perform formal periodic steady-state analysis and design of the ideal and non-ideal equivalent circuits of power electronics circuits. In this regard, we propose: (i) formal modeling of ideal and non-ideal behavior of the circuit elements (ii) formal modeling of basic circuit theory notions, such as switching function technique (iii) formally verified results for the integration and differentiation of piecewise functions (iv) formal modeling of differential equations (v) formally verified results for the solutions of the differential equations (vi) formal modeling of steady-state characteristics and design parameters. To illustrate the usefulness of the proposed formalizations, they are used to formally analyze the time-domain based periodic steady-state analysis of ideal and non-ideal DC-DC Buck converters.

Formalization in the complex-domain is aimed at formally analyzing stability of the control systems in power electronics systems to control the flow of energy from input to output. Our main contributions in complex-domain analysis are: (i) formal modeling of stability criterion (ii) formally verified results of factorization of characteristic polynomials upto the fourth-order (iii) formally verified results for the stability of the characteristic polynomials. The proposed formalization allows to formally specify and verify the stability analysis of control systems based on the characteristic polynomials which are obtained from the transfer function of the system in complex-domain. To illustrate the practical effectiveness, we formally verify the stability of controllers in smart grids for efficient energy processing from wind turbines.

# Table of Contents

<b>List of Figures</b>	<b>vi</b>
<b>List of Tables</b>	<b>vii</b>
<b>Acronyms</b>	<b>viii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Motivation . . . . .	1
1.2 Basic Circuit Theory . . . . .	6
1.2.1 Circuit Components Models . . . . .	7
1.2.2 Switching Function Technique . . . . .	9
1.3 Periodic Steady-state Analysis . . . . .	10
1.3.1 Differential Equation Representation . . . . .	11
Solution of Differential Equations . . . . .	13
1.3.2 Steady-state Characteristics and Design Specifications .	14
1.4 Stability Analysis . . . . .	15
1.5 Related Work . . . . .	17
1.5.1 Traditional Analysis Techniques . . . . .	17
1.5.2 Formal Methods . . . . .	19
1.6 Problem Statement . . . . .	22
1.7 Proposed Solution . . . . .	22
1.8 Thesis Organization . . . . .	25

<b>2</b>	<b>Preliminaries</b>	<b>26</b>
2.1	HOL Light Theorem Prover . . . . .	26
2.2	Multivariate Theory in HOL Light . . . . .	28
2.2.1	Set Theory . . . . .	28
2.2.2	Multivariate Theory . . . . .	29
<b>3</b>	<b>Formalization of Basic Circuit Theory</b>	<b>33</b>
3.1	Circuit Components Models . . . . .	33
3.1.1	Formal Modeling of Ideal Circuit Components . . . . .	33
3.1.2	Formal Modeling of Non-ideal Circuit Components . . . . .	35
3.2	Switching Function Technique . . . . .	38
3.3	Properties of Generalized Function . . . . .	38
3.4	Summary and Discussions . . . . .	40
<b>4</b>	<b>Formalization of Periodic Steady-state Analysis</b>	<b>41</b>
4.1	Differential Equation Representation . . . . .	42
4.2	Solution Verification of Differential Equations . . . . .	45
4.3	Modeling of Steady-state Characteristics and Design Specifications . . . . .	47
4.4	Case study: Periodic Steady-state Analysis of Ideal DC-DC Buck Converter . . . . .	48
4.4.1	Topology . . . . .	50
4.4.2	Solution of Differential Equations . . . . .	52
4.4.3	Steady-state Expressions for Output Voltage . . . . .	54
4.5	Summary and Discussions . . . . .	55
<b>5</b>	<b>Formalization of Stability Theory</b>	<b>57</b>
5.1	Stability Model . . . . .	57
5.2	Factorization of Polynomials upto the Fourth Order . . . . .	58
5.3	Stability Analysis of Polynomials upto the Fourth Order . . . . .	61



5.4	Case Study: Current and Voltage Controllers in Smart Grids .	66
5.5	Summary and Discussions . . . . .	68
<b>6</b>	<b>Case Study: Non-ideal Power Converters</b>	<b>70</b>
6.1	Steady-state Behavior and Specification of Converters . . . . .	73
6.2	Steady-state Characteristics . . . . .	75
6.3	Periodic Steady-state Analysis of Non-ideal DC-DC Buck Con- verter . . . . .	77
6.3.1	Topology . . . . .	79
6.3.2	Steady-state Principle . . . . .	81
6.3.3	Steady-state Characteristics and Design Specifications .	82
6.4	Summary and Discussions . . . . .	83
<b>7</b>	<b>Conclusions and Future Work</b>	<b>87</b>
7.1	Conclusions . . . . .	87
7.2	Future Work . . . . .	89
	<b>Bibliography</b>	<b>90</b>
	<b>Publications</b>	<b>102</b>

# List of Figures

Figure 1.1	Power Electronics System . . . . .	2
Figure 1.2	Power Electronics Analysis and Design . . . . .	4
Figure 1.3	Switching function technique . . . . .	10
Figure 1.4	Dynamic behavior of power electronics circuits under switching action, $S_w$ , represented by the switching wave form.	12
Figure 1.5	Proposed Methodology . . . . .	23
Figure 4.1	DC-DC buck Converter . . . . .	49
Figure 5.1	Stability of Quadratic Polynomial . . . . .	64
Figure 5.2	Efficient energy harvesting using Power converter con- trollers in smart grids . . . . .	67
Figure 6.1	DC-DC power converters and equivalent ideal converter circuit models. . . . .	71
Figure 6.2	DC-DC Buck power converter and equivalent non-ideal converter circuit model. . . . .	78
Figure 6.3	Quantification and comparison of formal verification of ideal and non-ideal power converters . . . . .	85

# List of Tables

Table 1.1	Ideal models of the power converter circuit components	7
Table 1.2	Non-Ideal models of the power converter circuit components . . . . .	9
Table 1.3	Steady-state characteristics and design specifications . .	15
Table 2.1	Higher-order-logic (HOL) symbols and functions. . . . .	27

# Acronyms

**MOSFET** Metal Oxide Semiconductor Field Effect Transistors

**BJT** Bipolar Junction Transistors

**IGBT** Insulated-Gate Bipolar Transistor

**CCM** Continuous Conduction Mode

**DCM** Discontinuous Conduction Mode

**ATP** Automatic Theorem Proving

**ITP** Interactive Theorem Proving

**ESR** Equivalent Series Resistance

**HyST** Hybrid Source-transformer

**KVL** Kirchoff's Voltage Law

**KCL** Kirchoff's Current Law

**PWM** Pulse Width Modulator

**DAB** Dual Active Bridge

**FSM** Finite State Machine

**DC** Direct Current

**AC** Alternating Current

**IC** Integrated Circuits

**RMS** Root Mean Square

**TF** Transfer Function

**dL** Dynamic Logic

# 1

## Introduction

### 1.1 Motivation

Power electronics systems are an integral part of, almost, every realizable electrical/electronics system. Power electronics allows to process raw energy from various and different types of energy sources to fulfill complex and stringent energy demands of domestic, commercial [7], industrial [74] [46], utility [89], transportation [15] and aerospace engineering [22] applications. Advances in the semiconductors technology are one of the main conduits for the current state-of-the-art power electronics applications [13]. Semiconductor devices, mostly in switch mode, enable power electronics systems to channel raw input energy to output energy in the desired form of energy with high efficiency and performance. Thus, switching operation of semiconductor devices plays a central role in power processing of power. However, switching action introduces highly non-linear behavior in power electronics circuits and therefore poses serious challenges in the modeling, analysis, design and verification of these systems [48].

Power electronics systems mainly constitute power electronics and feedback control circuits [8], as shown in Figure 1.1. Power electronics circuits



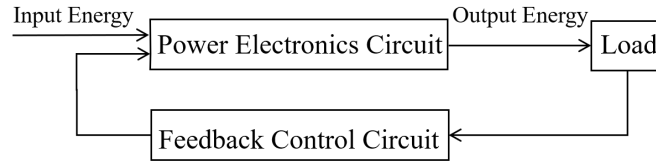


Figure 1.1: Power Electronics System

mainly consist of the power conversion stage and pre and post-filtration and rectification stages. Whereas, feedback control systems comprise of a control unit and switches to interface the power conversion stage and control system. Power conversion is mainly achieved using semiconductor devices, capacitors, inductors, transformers and resistive elements [24]. Power conversions are classified as choppers, rectifiers, inverters and ac-controller or cycloconverters [8]. Choppers are used to convert an input DC level to step-up or step-down output DC level. An AC type of input is converted into a DC type of output energy using rectifiers. A converse energy conversion operation is accomplished using inverter circuits. Whereas, AC-AC conversions are achieved using AC-controllers or cycloconverters. These power conversions can be achieved using different arrangements of active (semiconductor devices) and passive components (inductors and capacitors), referred to as topologies. Power electronics systems are further categorized as isolated and non-isolated topologies based on the isolation of input and output sides. The isolated topologies use transformers to isolate the input and output sides, whereas the output and input sides share a common DC path in non-isolated topologies. The feedback control is implemented using state-of-the-art IC technology, micro-controllers, microprocessors and digital and analogue circuitry to control the power flow from input to output.

The design process of a power electronics system involves selection of a suitable conversion topology for the desired conversion and steady-state and transient analysis to design control systems as per their specifications, as shown in Figure 1.2. Mathematically, basic circuit theory [20], differentia-

tion [14], integration [49], one-sided limits [43], piecewise functions [19] and control theory [64] are used in the design process. Basic circuit theory notions are used to analyze the power electronics circuit topologies using the individual behavior of the circuit components [55]. Differential equations and integral theory are used to express and analyze the system behaviors in steady-state and transient [24]. Whereas, piecewise functions and one-sided limits naturally arise due to switching functionality in power processing operation. Most of the power electronics design specifications are described as the steady-state parameters which are then employed to conduct small-signal analysis [24]. Small-signal analysis is used to determine the performance of the circuits in the presence of small disturbance. Finally, control theory is used to design control systems for power electronics systems [45]. Both time and frequency-domain are employed to analyze and design power electronics systems [61]. The system representation, circuit component models, steady-state parameters and design specifications are usually expressed in time-domain. Time domain based analysis allows to incorporate the effects of switching operations in power electronics circuits. Whereas, description of the power electronics system as a transfer function, in the frequency domain, allows to analyze and design controller stability and dynamic behavior by applying various techniques from control theory, such as stability theory and block diagrams. There are two possible operation modes for the working of power electronics circuits that are known as continuous conduction mode (CCM) and discontinuous conduction mode (DCM). A power electronics system is said to be operating in DCM, when the unidirectional assumption of semiconductor switch current or voltage is violated due to a switching ripple in an inductor current or capacitor voltage [24]. The scope of this thesis is on topology and steady-state analysis of power electronics circuits in the time domain, and stability analysis of power electronics systems in the frequency domain.

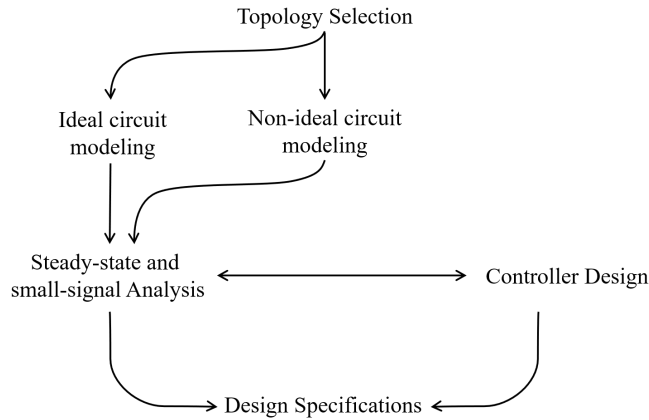


Figure 1.2: Power Electronics Analysis and Design

Traditionally, the design of power electronics systems is conducted using paper-and-pencil proof methods and simulations. However, paper-and-pencil methods are prone to human error due to manual manipulations and simplifications. Computer based general purpose simulators, such as SPICE [70] or SABER [53] and MathWorks Simulink [56], are commonly used to analyze and verify the circuit topologies and choices of circuit components, in time or frequency domain. However, these computer based packages utilize numerical methods [18] to simulate the systems, and hence, prone to digitization and truncation errors. Particularly, power electronics systems exhibit hybrid behavior, i.e., continuous behavior driven by discrete events, and therefore, cannot be accurately modeled using numerical methods which are, in essence, discrete in nature. For example, power and control design flaws in medical equipment have led to serious injuries and loss of lives of the patients in some cases [25] [26] [27]. Toyota Motor Corporation recalled about 807,329 Toyota Prius and Toyota Prius V models due to unattended interaction scenario between Boost converter and controller, and inverter failure under rarely high-voltage conditions [63]. Power electronics is also a key enabler of critical features of smart grids, such as integration of electric vehicles and renewable energy sources. Whereas, power outages and inter-

ruptions lead to huge financial losses for the economies all around the globe. In US, power outages and interruptions result in a loss of at least \$150 billion each year [65]. In China, electricity shortage in 2004 caused an estimated 0.64% decrease in the China's GDP growth [88]. In 2006, 20 countries in Western and Eastern Europe and North Africa suffered a loss of approximately \$100 million due to just a two hours power outage [83]. Moreover, smart grids for restoration of critical loads [86], such as hospitals and street lighting, demand highly reliable grid operations to avoid catastrophic events.

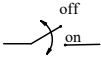
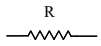
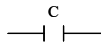
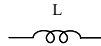
Formal methods [41] have been used to overcome the above-mentioned inaccuracy limitations for performing the accurate analysis and verification of power electronics systems. Formal methods are computer based mathematical techniques which are featured as sound and complete. Formal methods can be mainly categorized into two mainstream techniques, i.e., model checking [16] and theorem proving techniques [39], based on the logic, system modeling choice and supporting algebra and calculus [67]. Model checking is an approach which utilizes finite-state-machine (FSM) to model the systems and temporal logic [52] to express the system properties. A model checker—a piece of software—accepts the finite-state-machine representation of a system and its properties expressed in suitable temporal language. The model checker, then, exhaustively searches the state-space of the given FSM to formally verify the given system property and returns true if the property is valid, otherwise, returns a counter example. On the other hand, theorem proving employs logic to model and express the systems and its properties as a formula. A theorem prover—a piece of software—endowed with well-defined syntax, semantic and proof theory of specific logic allows to formally verify the systems. Theorem proving is further classified as automatic (ATP) [36] and interactive theorem proving (ITP) [54] depending upon the nature of the underlying logical framework. The use of decidable logics, such as first-order logic, allows to formally verify the systems in automatic fashion, whereas in

case of undecidable logical framework, such as higher-order logic, the formal proofs involve human and machine interaction. Both model checking and theorem proving has been used to formally verify various safety or mission critical aspects of the power electronics systems (e.g., [84] [12] [71]). However, model checking may suffer from the state-explosion problem due to very large state-space of underlying system [17], such as power electronics systems which exhibit hybrid behavior. Moreover, these techniques are not efficient in formally verifying functional models. Whereas formal verification of power electronics systems involve continuous time models, limit analysis and properties of generalized functions which cannot be accurately modeled and verified using model checking technique. Similarly, ATP also has limited expressiveness with respect to the aforementioned analysis framework for power electronics systems and therefore cannot be used to formally model and verify these systems. On the other hand, ITP uses undecidable logics, such as higher-order logic, which are highly expressive and therefore allow formally verifying complex system, such as power electronics systems. Therefore, in this thesis we propose a higher-order logic theorem proving framework for modeling, analyzing and verifying power electronics systems which are commonly used in many safety and mission-critical engineering applications.

## 1.2 Basic Circuit Theory

Topology selection is, usually, the first step in the design of a power conversion, such as DC-DC, AC-DC, DC-AC and AC-AC. Topological configurations of active and passive elements in power conversion stage, also called cell, serves as basis for classifying power electronics circuits into families of converters sharing specific properties [82]. This helps the designer to choose appropriate family of the converters to alleviate voltage and current stresses

Table 1.1: Ideal models of the power converter circuit components

Circuit component	Ideal model	Mathematical Model
Switch		$u(t - t_l) = \begin{cases} 1 & t_l < t \\ 1/2 & t = t_l \\ 0 & t < t_l \end{cases}$
Resistor		$V = IR \text{ or } I = \frac{V}{R}$
Capacitor		$i_C = C \frac{d}{dt} v_C \text{ or } v_C = \frac{1}{C} \int i_C dt$
Inductor		$v_L = L \frac{d}{dt} i_L \text{ or } i_L = \frac{1}{L} \int v_L dt$

for given power electronics application. Basic circuit theory furnishes fundamental mathematical models of circuit components and Kirchoff's laws to analyze the functionality of the circuits.

This section provides an introduction to conventional mathematical models of the commonly used power circuit components and Kirchoff's voltage and current laws which are utilized to analyze the power electronics circuits.

### 1.2.1 Circuit Components Models

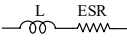
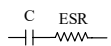


In practice, equivalent circuit modeling is applied to analyze and design power electronics circuits as per specifications. Ideal and non-ideal circuit modeling are two main approaches for the analysis and design of power electronics circuits [24]. In ideal circuit modeling, components of the circuits are assumed to behave ideally and hence only core functionality of these components is mathematically modeled. Table 1.1 shows ideal circuit models of capacitor, inductor and semi-conductor devices which are used in the power electronics circuits. The ideal circuit modeling approach is essential to understand the fundamental power conversion phenomenon of specific power electronics circuits. Although power electronics circuits have simple circuitry, however,



in many a cases, such as rectifiers, detailed analysis of these circuits is simply impossible due to resulting intractable mathematical formulations. In such situations, ideal equivalent circuit modeling is the ultimate choice to analyze these circuits. On the other hand, non-ideal circuit modeling is employed (wherever, possible) to meet design specification by incorporating losses, such as power and switching, in the equivalent circuit models [24]. The storage components and resistor are used widely in electronics circuitry to design analog circuits, however, switch component is particular to power electronics circuits. Characteristic of efficient power processing of power electronics is mainly due to switching functionality. Mathematically, switching functionality is modeled using Heaviside function (as described in Table 1.1). The function models *on* and *off* states for  $t > t_{switch}$  and  $t < t_{switch}$ , whereas, at switching instance  $t = t_{switch}$  function value is  $\frac{1}{2}$ . The value at switching instance is arithmetic mean of left- and right-hand limits.

Table 1.2 shows the equivalent non-ideal circuit models of the power electronics components. Non-ideal behavior of an inductor and a capacitor are modeled using an equivalent series resistance (ESR). The ESR models copper or core losses of the inductor and dielectric losses of the capacitor. The conduction losses in semiconductor devices occur due to the forward voltage drops of these devices and are thus incorporated as a voltage source and an on-resistance ( $R_{on}$ ). For the metal oxide semiconductor field-effect transistor (MOSFET) or bipolar junction transistor (BJT), an  $R_{on}$  is used to model the forward voltage drop of the device, whereas, an  $R_{on}$  in series with the voltage source ( $V_F$ ) is used to model a diode or an insulated-gate bipolar transistor (IGBT), or a thyristor. Once equivalent circuit models are obtained, they are analyzed using circuit theory notions. This allows to find voltages or currents of given circuit and derive many figure-of-merits which allow to design power electronics circuits for desired specifications.

Table 1.2: Non-Ideal models of the power converter circuit components

Circuit component	Non-Ideal model	Mathematical Model
Inductor		$i = i_L + i_{ESR}$ OR $v = v_L + v_{ESR}$
Capacitor		$i = i_L + i_{ESR}$ OR $v = v_L + v_{ESR}$
Diode, an IGBT or a Thyristor		$i = i_L + i_{ESR}$ OR $v = v_L + v_{ESR}$
MOSFET, or BJT		$i_{R_{on}} = \frac{v_{R_{on}}}{R_{on}}$ OR $v_{R_{on}} = i_{R_{on}} R_{on}$

## 1.2.2 Switching Function Technique

Power electronics circuits are characterized by switching element which introduces modes in the operation of a circuit. One of the main consequence is the singularity at the switching instance which hinders the use of basic Kirchoff's laws of voltage and current to these circuits. Switching function technique [55] alleviates this issue by introducing modified Kirchoff's voltage and current laws using superposition of voltages or currents at switching junction. These laws allow to express the behavior of these switching networks and derive switching functions for many interesting power electronics topologies.

According to switching function technique, the voltage and current expressions of modified Kirchoff's laws at a switching junction are:

$$V_{AB}(t) = \sum_{i=1}^n V_i(t) F_i(t) \quad n \in \mathbb{N} \quad (1.1a)$$

$$I_i(t) = I(t) \sum_{i=1}^n F_i(t) \quad n \in \mathbb{N} \quad (1.1b)$$

Equation 1.1(a), describes voltage at the switch junction, in a mesh, in terms of switching functions,  $F_i(t)$ . Figure 1.3a is a pictorial representation of the concept, where  $n$  voltage sources are connected to a point,  $A$ , through  $n$

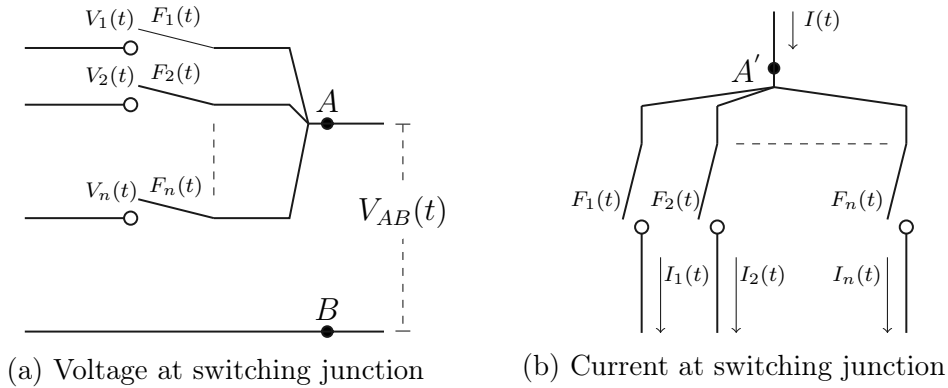


Figure 1.3: Switching function technique

switches. The voltage,  $V_{AB}$ , is then the superposition of the input voltages, however, the contribution of each voltage is dependent upon the associated switching function. Similarly, Equation 1.1(b), describes the current at a node,  $A'$ , which has  $n$  switches. Figure 1.3b describes the situation where current,  $I(t)$ , is supplied to  $n$  paths of the circuit through  $n$  switches. Each path receives the fraction of total current depending upon its switch status,  $F_n(t)$ .

We utilize mathematical models of circuit components, given in Table 1.1 and 1.2, and switching voltages and currents, i.e., Equation 1.1, to formally model the functionalities of these components in Section 3.1.

### 1.3 Periodic Steady-state Analysis

In periodic steady-state, the behavior of the power electronics circuits do not change with the passage of time. Most of the power electronics specifications are characterized by the steady-state parameters, e.g., converter ratio and efficiency. Therefore, steady-state analysis is a mandatory step in the design of the power electronics circuits.

In this section, we present the mathematical formulation of the periodic steady-state behavior of the power electronics circuits using differential

equations and analysis of the circuits using the solution of the corresponding system of differential equations.

### 1.3.1 Differential Equation Representation

A continuous switching operation in power electronics circuits leads to a sequence of modes, i.e., circuit configurations. Power electronics systems behavior can be described using  $n$ -th order linear differential equation in each mode. The order of the differential equations depends upon the number of storage elements involved in the energy conversion process in each circuit configuration. Power electronics systems exhibit hybrid behavior, i.e., continuous behavior driven by the discrete switching action. Therefore, overall system behavior is represented as a differential equation in each mode. These differential equations are obtained by applying circuit theory laws, i.e., Kirchoff's voltage and current laws, on the ideal or non-ideal equivalent circuit models of the power electronics circuits.

Mathematically, the behavior of these systems can be described as:

$$\begin{aligned}
 H(t, y_1, y_1^1, \dots, y_n^{m_n}) &= p(t) & t \in [t_{n-1}, t_n], n, m_n \in \mathbb{N} \\
 y_n^k(t_n) &= y_{n-1}^k(t_{n-1}) & k \in \mathbb{N} \\
 y_0(t_0) &= 0
 \end{aligned} \tag{1.2}$$

Where,  $H$  and  $p$  are functions of an independent variable  $t$ , a dependent variable  $y_n$  and its  $m_n$ -th order derivative in the corresponding  $n$ -th mode, respectively. In power converters, the time is considered as an independent variable, whereas, the voltage or current of the energy storage components is considered as a dependent variable. The order, i.e.,  $m_n$ , of an ordinary differential equation of the power converter, in the  $n$ -th mode, is determined by the number of energy storage elements constituting the mode. The function  $p(t)$  is referred to as a non-homogeneous term, which can be zero or non-zero in

the  $n$ -th mode, depending upon the presence of source in the  $n$ -th mode of a power converter. Initially, the value of dependent variable is considered zero, i.e.,  $y_0(t_0) = 0$ , however, later on the value of the dependent variable in one mode becomes an initial value for the next mode, i.e.,  $y_n^k(t_n) = y_{n-1}^k(t_{n-1})$ , when switching instance occurs. Whereas,  $k$  is the order of the derivative of the dependent variable evaluated at a specific time instance.

For the brevity of the notion, transient and steady-state time-domain behavior of a power electronics circuit is presented in Figure 1.4, based on the above-mentioned standard approach. Figure 1.4 illustrates the switch waveform,  $S_w$ , along with the differential equation for each mode in transient and steady-state of a power electronics system.

In periodic steady-state, the dependent variables of a power converter circuit attain an equilibrium and repeat the behavior over a time period,  $T_p$ , constituting  $l$  modes. Mathematically, the periodic steady-state behavior of a power converter over one time period, when  $t \rightarrow \infty$ , can be represented as:

$$H(t, y_n, y_n^1, \dots, y_n^{m_n}) = p(t) \quad t \in T, T \in \bigcup_{i=1}^l [t'_{i-1}, t'_i], m_n, n, l \in \mathbb{N} \quad (1.3)$$

$$y^k(t'_0) = y^k(t'_0 + T_p) \quad T_p = t'_{\max(i)} - t'_0, k \in \mathbb{N}$$

Equation (1.3) reduces the problem to the identification of the modes in one

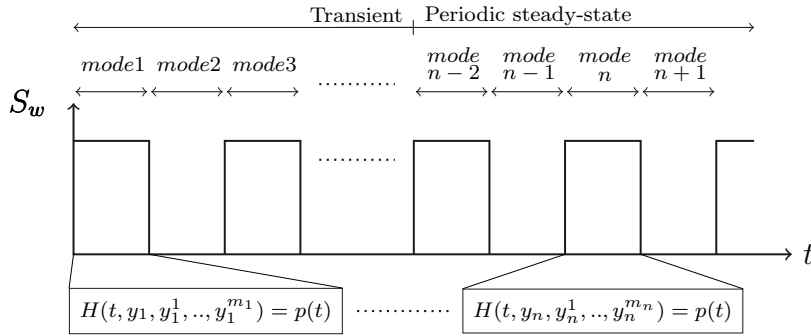


Figure 1.4: Dynamic behavior of power electronics circuits under switching action,  $S_w$ , represented by the switching wave form.

time period,  $T_p = t'_{max(i)} - t'_0$ , of the circuit, which is the length of time over which the modes of a power electronics circuit repeat themselves. The function  $y$  is a piecewise function defined over  $l$  modes. Whereas,  $y^k(t'_0) = y^k(t'_0 + T_p)$  refers to the steady-state conditions of the system variable at reference switching time instances,  $t'_0$ , and  $T_p$ , and  $k$  represents the  $k$ -th order derivative of the variable.

### Solution of Differential Equations

The general solution to  $n$ -th order differential equation is expressed as [14]:

$$y_l(t) = y_h(t) + y_p(t) = \sum_{i=1}^n c_i e^{s_i t} + y_p(t) \quad (1.4)$$

Where,  $y_h(t)$  is the linear combination of the fundamental solutions of Equation (1.4) when  $p(t) = 0$ , and  $y_p$  is the particular solution corresponding to Equation (1.4) when  $p(t) \neq 0$ .

The solution for the dependent variable is a piecewise function and is represented using Heaviside function.

$$y(t) = \sum_{i=0}^l y_i(t) u(t - t_i) \quad t \in T \quad (1.5)$$

Where,

$$u(t - t_i) = \begin{cases} 1 & t_i < t \\ 1/2 & t = t_i \\ 0 & t < t_i \end{cases} \quad (1.6)$$

The solution, i.e., Equation (1.5), represents the behavior of the circuit variable, either current or voltage, over one time period of the circuit.

The linearity property of the derivative operator plays a central role in the verification of the solution of the linear differential equations. Mathe-



matically, linear operator property is described as [14]:

$$L[af_1 + bf_2] = aL[f_1] + bL[f_2] \quad (1.7)$$

In Equation 1.7,  $L$  represents linear derivative operator and,  $a$  and  $b$  are real numbers. Where,  $f_1$  and  $f_2$  are functions which represent solution of the linear differential equation.

We use the framework described by Equations 1.3-1.7 in our proposed formalization to formally model, specify and verify the periodic steady-state behavior of power electronics circuits in Chapter 4.

### 1.3.2 Steady-state Characteristics and Design Specifications

In power electronics systems, periodic steady-state principle is characterized as [24]:

$$\frac{1}{T_p} \int_{t_0}^{t_0+T_p} y(t) = 0 \quad (1.8)$$

When the dependent variable  $y(t)$ , represents the inductor voltage then Equation (1.8) is referred to as the inductor volt-second principle, and, if the capacitor current is considered, then, it is called the capacitor-charge balance principle [24]. These principles ensure that the average energy stored in the inductor and capacitor is zero over one time period of the converter circuit. This way, the converter circuits exhibit a periodically repeating behavior in the steady-state.

Although, average current and voltage values in the converter are zero, however, due to switching and non-ideal behavior of the circuit components, circuits produce an alternating current (AC), termed as ripple  $\Delta f_r$ , at the output. Consequently, RMS values,  $f_{rms}$ , of the circuit parameters are used to specify currents and voltages, as mentioned in Table 1.3. Whereas, the

Table 1.3: Steady-state characteristics and design specifications

Specifications	Steady-state characterization
Average	$f_{avg}(t) = \frac{1}{T} \int_{t_o}^{t_o+T} f(t)dt$
Valley Value	$f_p = \min f(t)$
Peak Value	$f_p = \max f(t)$
Ripple	$\Delta f_r = f_p - f_v$
Ripple RMS [72]	$\Delta f_{r(rms)} = \frac{f_r}{2\sqrt{3}}$
Root Mean Square Value	$f_{rms} = \sqrt{f_{avg}^2 + \Delta f_{r(rms)}^2}$
Power Loss	$P_{loss} = I_{rms}^2 R$
Ripple Factor	$f_{RF} = \sqrt{f_{FF}^2 - 1}$
Conversion Ratio	$M = \frac{f_{out}}{f_{in}}$
Converter Efficiency	$\eta = \frac{P_{out}}{P_{out} + P_{loss}}$

ripple magnitude is determined using the peak,  $f_p$ , and minimum,  $f_v$ , values of the circuit parameters. The magnitude of the ripple determines the power losses of the circuit components, and hence, plays a vital role in the selection of the circuit components power ratings to meet the design specifications of the circuits, such as converter ratio ( $M$ ) and efficiency ( $\eta$ ) (given in Table 1.3).

The steady-state characteristics and design specifications presented in this section are used to formally verify the design of ideal and nonideal DC DC power converters in Section 4.4 and Chapter 6, respectively.

## 1.4 Stability Analysis

Control systems are an integral component of the power electronics systems [8]. Control systems are combinations of subsystems intended to control the output of the system [64]. Stability is the most important design requirement

of a linear time-invariant control system [64]. An unstable control system deployed in a safety-critical domain, e.g., in nuclear power plants or aircrafts, can lead to disastrous consequences, including the loss of human lives, and therefore stability is considered as a safety-critical system specification.

Generally, the design and analysis of linear time-invariant control systems [64] is done in the frequency domain. The main idea is to convert a differential equation representation of the system, e.g., Equation 1.3, into its frequency domain representation using a transform method, like Laplace or Fourier [21]. This transformation simplifies the modeling of interconnected subsystems and also generates a mathematical model of the system that algebraically relates the input to the output based on a transfer function,

$$TF(s) = \frac{O(s)}{I(s)} = \frac{a_m s^m + a_{m-1} s^{m-1} + \dots + a_0}{b_n s^n + b_{n-1} s^{n-1} + \dots + b_0} \quad (1.9)$$

where,  $a_i$  and  $b_i$  are the coefficients representing system parameters,  $s$  is a complex-variable and  $m$  and  $n$  are natural numbers. Whereas,  $\max\{m, n\}$  represents the order of the transfer function. The order of the transfer function depends on the order of the corresponding linear differential equations in the time domain representing a physical system. As most of the variables of the physical system can be represented using differentials upto the fourth order, such as capacitor current, inductor voltage, acceleration, velocity and momentum, therefore, control systems upto fourth order cover a wide spectrum of applications, including safety and mission-critical applications. Moreover, there are model reduction techniques [76] to reduce the higher-order transfer functions into their equivalent lower-order representations to facilitate the control system design. The denominator and the numerator of a transfer function, in Equation 1.9, are complex polynomials which are used to characterize the *zeros* and the *poles* of the system. These zeros and poles are roots of complex polynomials in the denominator and the numerator of

the transfer function, respectively. In particular, the stability of the system solely depends on the location of the poles of the system, obtained from:

$$b_n s^n + b_{n-1} s^{n-1} + \dots + b_0 = 0 \quad (1.10)$$

Equation 1.10 is also referred to as a *characteristic* equation of the system. The roots of the characteristic equation are used to express the behavior of the circuits, described by Equation 1.4. Therefore, a system is categorized as *stable*, *unstable* and *marginally stable* based on the location of the roots of Equation 1.10 in the complex-plane. The roots in left-half plane ensure exponentially decaying response of the system, the right-half roots results in exponentially growing response and roots on the imaginary axis corresponds to bounded oscillatory response of the system. Therefore, for a stable system, the roots of the characteristic equation lie in the left-half of the complex-plane, for an unstable system, the roots of the characteristic equation lie in the right-half of the complex-plane, and for a marginally stable system, the roots of the characteristic equation lie on the imaginary axis of the complex-plane.

Our proposed formalization of stability relies on the Equation 1.10 to formally model the stability of the control systems in Chapter 5.

## 1.5 Related Work

### 1.5.1 Traditional Analysis Techniques

Traditionally, the design of power electronics system is conducted using paper-and-pencil proof methods and simulations. One of the main strengths of the paper-and-pencil proof methods is availability of all mathematical theories and model abstractions which can be utilized by humans to aid or guide the analysis of given systems. This feature of the paper-and-pencil analysis

methods has been vital in introducing new analysis techniques [59] [44] [23] and simplifications, such as small-ripple or linear-ripple approximation [24], to ease the analysis of otherwise complex power electronics systems. However, these methods are subject to the issues of scalability and error-prone nature of humans. That is, the method does not suit well to the problems with many interrelated or intertwined aspects of the given phenomenon simply due to lack of the human capability to process large amount of data easily and efficiently. On the other hand, irrespective of the scale of the given problem, it is more likely that many assumptions are not documented which are employed intuitively and therefore can cause serious issue when neglected or overlooked in the later stages of the system development. Computer-based simulation methods are also an essential ingredient of the analysis and design process in power electronics. General purpose circuit simulators, such as SPICE [70] or SABER [53], are commonly used to analyze and verify the circuit topologies and choices of circuit components. Another category of digital simulators, such as MathWorks Simulink [56], allow to describe mathematical models, in time or frequency domain, of power electronics circuits to analyze the performance of these systems. However, these computer based packages utilize numerical methods [18] to simulate the systems, and hence are prone to digitization and truncation errors. To address this issue, computer algebra systems, such as Mathematica [85] and Maxima [58], which are software programs for the symbolic processing of mathematical expressions, are also employed for the analysis of power electronics systems [51]. However, the symbolic processing is based on the unverified program codes, and therefore prone to bugs [79]. Thus, given the aforementioned inaccuracies, these traditional techniques should not be relied upon for the analysis of power electronics systems, especially when they are used in safety-critical areas, such as implantable medical devices and automotive industry, and mission-critical areas, such as smart grids, where bugs may lead to heavy monetary

or human life loss.

### 1.5.2 Formal Methods

In order to overcome the above-mentioned inaccuracy limitations, formal methods have also been employed to analyze power converter circuits. Hybrid automaton has been widely used to formally model and verify hybrid systems using reachability analysis tools, such as SpaceEX [29], UPPAAL [11], HyTech [42], PHAVer [28], and HyLaa [5]. Recently, SpaceEx has been employed to formally verify the Buck and dual active bridge (DAB) converters [84]. Similarly, a hybrid automaton based formal verification of non-ideal PWM DC-DC converters is presented using SpaceEx tool [9]. The authors used the reachability analysis capability of the SpaceEx to formally verify the stability of the converters. A framework for translating the hybrid automation of the Buck, Boost and Buck-Boost power conversion circuits into Mathworks Simulink/Stateflow (SLSF) using an automatic source-to-source model translation and transformation tool, called Hybrid Source transformer (HyST), is presented in [10]. The formalization is mainly aimed at saving a significant amount of time and effort involved in modeling the hybrid automata for the formal verification of power electronics systems. Design of controllers for the single output and double output DC-DC Boost and Buck converter are presented using hybrid automata theory [60] [73]. However, such analysis involves many abstractions to capture the behavior of the circuits as a finite state transition system. Moreover, the inherent state-space explosion problem of model checking also restricts its usage for the continuous systems. Specifically, SpaceEx uses LGG algorithm to solve the first-order linear differential equations which are, in the strict sense, not sound [77]. Recently, an automatic theorem prover (ATP), KeYmaera X [66], has been developed to formally verify the hybrid systems. KeYmaera X uses differential dynamic logic (dL), which is a first-order logic, for the implementation

and specification of the underlying systems and, therefore, cannot be used to formally verify the functional properties of the systems. For example, integration and differentiation of generalized functions for modeling, analyzing and verifying various aspects of the power converters cannot be accomplished using first-order logic. `HOL Light`, an interactive theorem prover, has been used to formally verify the transfer function of pulse width modulation push-pull DC-DC converter and 1-boost cell DC-DC converter [12] using the signal flow graph and Mason's gain formalization to formally verify critical aspects of the systems, such as stability. However, the formal analysis is conducted for the frequency domain representation of the power converters and therefore cannot be used to formally verify the time-domain based characteristics of the systems.

Circuit components, i.e., resistor, capacitor and inductor, and circuit laws, i.e., Kirchoff's current and voltage laws, have been formally modeled and used in the formal analysis of analog circuits used in the design of embedded systems using `HOL Light` [81]. Similarly, differential equations have been formally modeled in `HOL4` for the formal verification of cyber-physical systems [71]. However, in thesis we have developed the framework for the formal complex domain analysis by using complex-valued functions as opposed to real-valued functions used in the formal analysis of analog circuits and cyber-physical systems. This fundamental difference results in more challenging task of formal verification of power electronics systems. Whereas, consideration of complex-valued functions is mandatory to incorporate the harmonics which are inevitable due to switching power electronics circuits. Moreover, formal modeling of non-homogeneous equations, non-ideal circuit components and switch have also been developed for the first time to analyze and design power electronics circuits.

Formal methods have also been employed to formalize the control systems due to their safety or mission-critical applications. The formalization

of Laplace transform [80] has been proposed to formally reason and verify the transformation properties, e.g., existence, linearity, frequency shifting and differentiation and integration in time domain. This formalization framework allows to verify the correspondence of the time domain representation of the system, i.e., linear differential equation, to the frequency domain representation of the system, i.e., transfer functions. This existing work can be used along with the formalization proposed in this paper to analyze the stability analysis of control systems, expressed in terms of their dynamical behaviors using differential equations.

Block diagrams formalization has been proposed [40] [1] to conduct steady-state error analysis, i.e., when  $s \rightarrow 0$ , for feedback and unity feedback control systems, in frequency domain. However, this formalization does not explicitly deal with the stability analysis of control systems. Formal stability analysis has also been proposed for some particular safety and mission-critical applications. The formal stability analysis of optical waveguides [75] has been performed by defining the stability condition in terms of the boundedness and orientation of a ray in a wave guide using multivariate theory in `HOL Light`. A logical framework for the formal verification of various strategies for the platoon vehicle controllers [69] is proposed and is then used for developing a run-time monitor which can be used for automatic monitoring of the vehicles for stability violation. Similarly, another comprehensive logical framework for the analysis of control systems [68] considers the system differential equations and obtains their corresponding transfer functions using Laplace transformation and it also provides a support for the block diagram analysis of the system in frequency domain. On the basis of this framework, formal analysis of active realizations of various controllers, Proportional Integral-Derivative (PID), Proportional-Integral (PI), Proportional-Derivative (PD), Proportional (P), Integral (I) and Derivative (D) and various active and passive compensators, such as lag, lead and lag-lead is conducted. However, the



aforementioned formalizations for the stability are application specific and do not provide a generic treatment of the stability of the control systems. The formally verified quadratic roots [71] have been used for the formal analysis of cyber-physical systems using the real number theory in the HOL4 theorem prover. However, this formalization of the quadratic formula in real number theory cannot be used to analyze the complex-domain of the control systems.

## 1.6 Problem Statement

Power electronics systems exhibit nonlinear behavior due to switching functionality and therefore pose serious challenges of modeling, analyzing and verification. Mathematically, differential, integral, generalized calculus, one-sided limits and stability theory are employed to design power electronics systems. Traditionally, paper-and-pencil and computer-based simulation methods are used to analyze and verify power electronics systems. However, these methods cannot guarantee a sound and complete analysis of the systems due to inherent limitations. Whereas, power electronics applications include many safety and mission-critical applications, such as medical equipment, electric vehicles, smart grids, and aerospace engineering, and a minor error can lead to a catastrophic event, including the loss of human lives. Therefore, traditional analysis techniques cannot be relied upon for the analysis and design of safety or mission-critical power processing applications.

## 1.7 Proposed Solution

The primary objective of this thesis is to develop a higher-order-logic framework for the accurate analysis and design of the power electronics systems within the sound core of the HOL `Light` theorem prover (as shown in Figure 1.5). The main contributions of this thesis are:

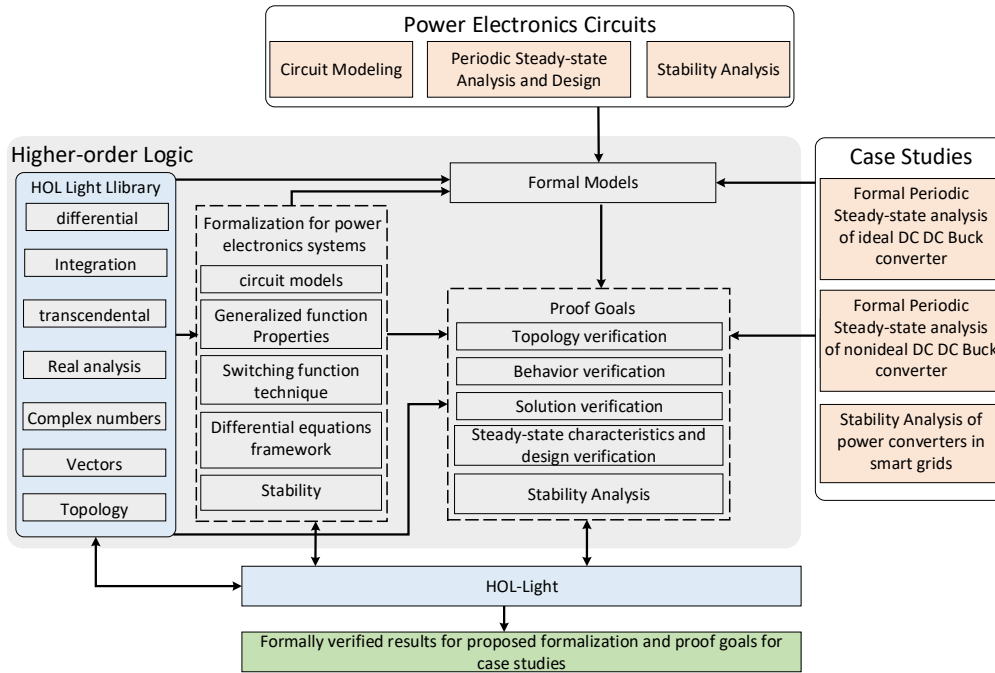


Figure 1.5: Proposed Methodology

- We develop higher-order-logic based formalization of basic circuit theory to formally analyze the topology of power electronics circuits. The formalization includes higher-order-logic models of ideal and non-ideal circuit components and switching function technique (Sections 3.1 and 3.2). This logical framework allows to formally analyze and verify the topologies of power electronics circuits. Moreover, the formalization also contains formally verified results for differential and integral properties of piecewise functions (Section 3.3) which are mandatory to conduct formal analysis of various aspects of power electronics systems.
- We also present formalization of differential equations to express the behavior of power electronics circuits and verify their circuit parameters. The formalization includes higher-order-logic modeling of differential equations and formally verified results for homogeneous and particular

solutions of the differential equations (Sections 4.1 and 4.2). Moreover, formal models of steady-state characteristics and design parameters are developed to formally specify and verify the power electronics circuit design and analysis within the sound of core of the `HOL Light` theorem prover (Section 4.3). To illustrate the usefulness of the proposed formalization, periodic steady-state analysis of an ideal DC-DC Buck converter is presented that includes topology, steady-state behavior and solution verification of the converter (Section 4.4).

- To analyze the stability of power electronics systems, we formally model the stability criterion in higher-order logic (Section 5.1) that utilizes the characteristic equation of the system which is obtained from the transfer function representation of the system. We also provide formally verified results for the stability analysis of characteristic equations upto the fourth-order (Section 5.3). These formally verified results are also supplemented by the formally verified factorization theorems for the characteristic equations upto the fourth-order (Section 5.2). We use the proposed stability formalization to conduct formal stability analysis of an  $H^\infty$  current,  $H^\infty$  voltage and  $H^\infty$  repetitive current controllers for wind turbines in smart grids using the proposed formalization (Section 5.4).
- Finally, we present formal time-domain periodic steady-state analysis of non-ideal DC-DC power converters to show the usefulness of the proposed formalization for the practical design of power electronics circuits (Chapter 6). Notably, a generic logical framework is presented to formally express and verify the periodic steady-state behavior of basic DC-DC power converter topologies using first-order linear differential equations (Section 6.1). The generic logical framework is then employed to formally verify the periodic steady-state analysis and design

of non-ideal DC-DC Buck converter (Section 6.3).

## 1.8 Thesis Organization

The rest of the thesis is organized as follows: In Chapter 2, we provide a brief introduction to the `HOL Light` theorem prover and an overview of Set and Multivariate theories in `HOL Light` library to familiarize the reader with notations and notions used in the proposed formalization presented in the rest of the thesis. Chapter 3 presents the basic circuit theory and library of circuit components formalization that enables us to formally specify power electronics circuits in the `HOL Light` theorem prover. Chapter 4 describes higher-order-logic framework to formally specify and verify the  $n$ -th order differential equation representation of power electronics systems in periodic steady-state. We demonstrate the utility of the proposed formalization, in Chapter 3 and 4, by formally verifying various aspects of an ideal DC-DC Buck power converter. In Chapter 5, we present stability formalization of control systems to formally analyze and verify the stability of systems represented by their transfer functions. As a case study, we formally verify the controllers for power converters of a wind turbine which are used in the smart grids to process intermittent energy generated from the wind. In Chapter 6, a formal analysis of a non-ideal DC-DC Buck converter is performed to illustrate the usefulness of the proposed formalizations for the design of real-world power electronics systems. Finally, Chapter 7 concludes the thesis and outlines some future research directions.

## 2

# Preliminaries

## 2.1 HOL Light Theorem Prover

HOL Light [38] is an interactive theorem prover that allows its users to develop new mechanized theories, proofs, and inference rules with the support of many automated tools and pre-proved mathematical theories, such as Multivariate set, differential and integration theories. It has been widely-used for some significant industrial-scale verification applications [32] [35].

A variant of the strongly typed functional programming language, i.e., Objective CAML (OCaml), is used to implement higher-order logic in the HOL Light theorem prover. HOL Light provides a secure and sound platform for the formal verification and specification of the systems. Sound theorem proving is ensured by the small core that consists of only 1500 lines, including 10 primitive inference rules, such as modus ponens and reflexivity, whereas soundness is ascertained due to the convergence of all the mechanized proofs to these inference rules. HOL Light supports backward and forward proof strategies. In the backward proof strategy, a theorem is formally verified using inference rules, whereas, in the forward proof strategy, the given theorem is broken down into subgoals using HOL Light

Table 2.1: Higher-order-logic (HOL) symbols and functions.

HOL Symbol	Standard Symbol	Meaning
$\wedge$	<i>and</i>	Logical <i>and</i>
$\vee$	<i>or</i>	Logical <i>or</i>
$\neg$	<i>not</i>	Logical <i>negation</i>
$\implies$	$\rightarrow$	Logical <i>conditional</i>
$\%$	$c \vec{d}$	Scalar multiplication of vectors
$\lambda x.t$	$\lambda x.t$	Function that maps $x$ to $t(x)$
<b>num</b>	$\{0, 1, 2, \dots\}$	Positive integers data type
<b>real</b>	All real numbers	Real data type
<b>complex</b>	All complex numbers	Complex data type
<b>SUC n</b>	$n + 1$	Successor of a <i>num</i>
<b>rpow x y</b>	$x^y$	Power with real exponent
<b>max (f(x), g(x))</b>	$max(g(x), f(x))$	Maximum among $f(x)$ and $g(x)$

tactics. A tactic is a special ML function used to divide the main goal into subgoals and perform simple decidable real, complex and vector arithmetics, such as `GEN_TAC`, `REPEAT_TAC`, `SIMP_TAC`, `REAL_ARITH_TAC` and `SIMPLE_COMPLEX_ARITH_TAC`. In the proposed formalization, we have used many such tactics to formally verify the power electronics circuits. More detail on tactics can be found here [38].

We used the `HOL Light` theorem prover for the proposed work as it is endowed with the library of the Multivariate set, differential and integration and topology theories to facilitate the higher-order logic modeling, analysis and verification of power electronics systems. `HOL Light` has been utilized, at intel, for the formal verification of the floating numbers [35]. `HOL Light` theorem prover has, also, been employed in the formal verification of the Kepler's conjunction [33]. One of the criteria for the efficiency and performance of any theorem prover is the number of formally verified theorems from the list of 100 theorems. `HOL Light` is on the top by formally verifying 86 theorems from the list [34]. Table 2.1 presents some of the frequently used `HOL Light` functions and symbols to facilitate the understanding of the formalization and verification in the rest of thesis.

## 2.2 Multivariate Theory in HOL Light

We present basic definitions and results from set, differential, integration and topology theories of HOL `Light` library that will be helpful in understanding the formalizations, presented in the next chapters of this thesis.

### 2.2.1 Set Theory

A set membership ( $\in$ ) operation is defined in the higher-order logic as:

**Definition 2.1:** *Set Membership*

$$\vdash \forall P x. \quad x \text{ IN } P = P x$$

An empty set is modeled as follows:

**Definition 2.2:** *Empty Set*

$$\vdash \{\} = (\lambda x. \quad F)$$

There are number of theorems, which are used to eliminate set abstraction. We present the basic one which has been used in our formalizations,

**Definition 2.3:** *Set Abstraction Elimination*

$$\vdash \forall p. \quad \text{GSPEC } p = p$$

Where  $P:A \rightarrow \text{bool}$  is a predicate modeling a set.

Finally, a non-empty set related theorem is as follows:

**Theorem 2.1:** *Non empty set*

$$\vdash \forall x. \quad \sim ( x \text{ IN } \{\} )$$

The above theorem ensures that empty set has no member.

## 2.2.2 Multivariate Theory

HOL `Light` is endowed with the Multivariate theory to formally reason about the topology, analysis and geometry in Euclidean space. HOL `Light` models an  $N$ -dimensional Euclidean space as  $R^N$  data type [37]. This allows to formally model an  $N$ -dimensional vector in Euclidean space using a higher-order-logic mapping function, `lambda`,

**Definition 2.4:** *Vector*

$\vdash \forall l. \text{ vector } l = (\text{lambda } i. \text{ EL } (i - 1) l)$

In above definition, `vector` is a higher-order-logic function, which accepts a list, `l`, and maps the elements to an  $R^N$  space. This ingenious approach allows to not only formally reason in finite  $N$ -dimensional space but also supports formal reasoning in subspaces, such as *real* and *complex*, by instantiating  $N=1$  and  $2$ , respectively.

There are HOL `Light` functions which allow to map *real*, *complex* and *vector* spaces. A term of type *complex* in HOL `Light` is defined using Definition 2.4 as:

**Definition 2.5:** *Complex Number*

$\vdash \forall x y. \text{ complex}(x, y) = \text{vector } [x; y]$

A term of type *real* can be mapped as a complex number using `Cx`,

**Definition 2.6:** *Real-to-Complex Mapping*

$\vdash \forall a. \text{ Cx } a = \text{complex}(a, \&0)$

A term of type *real*<sup>1</sup> can be mapped to a real type using `drop`,

**Definition 2.7:** *Vector-to-Real Mapping*

$\vdash \forall x. \text{ drop } x = x\$1$

Where `$` represents dimension index. A converse operation on term of real is achieved using the `lift` function,



**Definition 2.8:** *Real-to-Vector Mapping*

$\vdash \forall x. \text{ lift } x = (\text{lambda } i. \ x)$

The traditional Frechet derivative definition [87] in HOL Light is expressed as:

**Definition 2.9:** *Frechet Derivative*

$\vdash \forall f \ f' \ \text{net}.$

```
(f has_derivative f') net =
[A1] linear f' ^
((λy. inv (norm (y - netlimit net)))) %
(f y - (f (netlimit net) + f' (y - netlimit net))) →
vec 0
```

`has_derivative` is a higher-order-logic function, which accepts function  $f:R^M \rightarrow R^N$ , derivative of function  $f':R^M \rightarrow R^N$  and evaluation point or interval  $\text{net}:A$ . `net` has an arbitrary type,  $A$ , specified by the user. In Assumption A1, `linear` is another higher-order-logic predicate that ensures that the derivative function is a linear transformation. The conclusion of the above definition is a predicate ensuring that the limit of the derivative approaches zero.

Differentiability of a function is formally modeled in higher-order logic as,

**Definition 2.10:** *Differentiability within an interval*

$\vdash \forall f \ s.$

```
f differentiable_on s = ∀x. x IN s
==> f differentiable (at x within s)
```

In the above definition, `differentiable_on` accepts a function,  $f$ , and a real interval,  $s$ , to specify the differentiability of a given function within the interval.

Continuity of a function is formally defined in higher-order logic as,

**Definition 2.11:** *Continuity*

$$\begin{aligned} &\vdash \forall x. \ x \text{ IN } s \implies \\ &\quad f \text{ continuous\_on } s \implies \forall e. \ \&0 < e \\ &\quad \exists d. \ \&0 < d \wedge \\ &\quad \forall x'. \ x' \text{ IN } s \wedge \text{dist } (x', x) < d \\ &\quad \text{dist } (f(x'), f(x)) < e \end{aligned}$$

Above Definition formally specifies the continuity of a function using mathematical *epsilon-delta* definition of continuity. That is, a small change ( $d$ ) in the argument of the function leads to the function value ( $e$ ). Whereas, `dist` is a higher-order-logic function to model the small change in the argument and value of the given function.

The Henstock-Kurzweil integral [49] is defined in higher-order logic, as:

**Definition 2.12:** *Henstock-Kurzweil integral*

$$\begin{aligned} &(f \text{ has\_integral } y) \text{ (interval } [a, b]) = \\ &\quad (\forall e. \ \&0 < e \\ &\quad (\exists d. \ \text{gauge } d \wedge \\ &\quad \quad (\forall p. \ p \text{ tagged\_division\_of interval } [a, b] \wedge d \text{ fine } p \\ &\quad \quad \implies \text{norm } (\text{vsum } p \ (\lambda(x, k). \ \text{content } k \% f \ x) - y) < e))) \end{aligned}$$

In the above definition,  $e$  is a positive real number,  $d$  is Gauge function and  $p$  is the tagged division of the given interval  $[a, b]$  which are related using higher-order logic `tagged_division_of` and `fine` functions. Whereas, `norm`, `vsum` and `content` are higher-order-logic functions which are used to express the Henstock-Kurzweil condition on the integral  $y$ .

Finally, we present definition of the limit and theorems on limits from the topology theory in `HOL Light` library. The limit of a function  $f$  is formally modeled in the `HOL Light` theorem prover, as:

**Definition 2.13:** *Limit of a function*

$$\forall f. \ \text{lim net } f = @l. \ (f \rightarrow l) \text{ net}$$

In Definition 2.13, `lim` is higher-order-logic function which accepts `net`, of an arbitrary data-type `A`, and `f`, of data-type `A → ℝM`. The right-hand side of `lim` models the notion of function, `f`, approaching limit point `l`, of data-type `ℝM` for the specified `net`. Whereas, `@` is the Hilbert choice operator which is used as a binding operator. Hilbert choice operator facilitates quantified substitution in a formal deductive system, such as higher-order logic.

The formally verified right and left-hand side limits in topology theory are:

**Theorem 2.2:** *Right-hand Side Limit*

$\forall f\ l\ a.$

$(f \rightarrow l) \text{ (at } a \text{ within } \{x \mid x \text{ IN } s \wedge \text{drop } a \leq \text{drop } x\}) =$

$(f \rightarrow l) \text{ (at } a \text{ within } \{x \mid x \text{ IN } s \wedge \text{drop } a < \text{drop } x\})$

**Theorem 2.3:** *Left-hand Side Limit*

$\forall f\ l\ a.$

$(f \rightarrow l) \text{ (at } a \text{ within } \{x \mid x \text{ IN } s \wedge \text{drop } x \leq \text{drop } a\}) =$

$(f \rightarrow l) \text{ (at } a \text{ within } \{x \mid x \text{ IN } s \wedge \text{drop } x < \text{drop } a\})$

The above two theorems formally verify the equivalence of the limit of a given function, `f`, at a point, `a`, within the interval, `s`, and limit of the given function when it approaches the point, `a`, from right or left. The data-type of `net` in the above theorems is specified using `s:(real→bool)`.

# 3

## Formalization of Basic Circuit Theory

In this chapter, we describe the formalization of commonly used basic circuit theory concepts in the analysis and design of power electronics circuits. In order to formally specify the behavior of the circuit components, we present higher-order-logic models of circuit components, both ideal and non-ideal behaviors. Then, we present formal models of modified Kirchoff's voltage and current laws which are based on the switching function technique to enable the formal verification of the circuit topologies. Finally, we present formally verified results for the integration and differentiation of piecewise functions which provide formal mathematical machinery in the formal analysis and design of power electronics circuits.

### 3.1 Circuit Components Models

#### 3.1.1 Formal Modeling of Ideal Circuit Components

In power electronics circuits, semiconductor devices such as, diodes, BJTs (bipolar junction transistors), MOSFETs (metal oxide semiconductor field

effect transistors), IGBTs (insulated gate bipolar transistors) etc, are used for performing the switching operation. These semiconductor devices play a key role in the efficient power conversion [6]. Although, these devices differ in their physics and physical properties, however, as a switch, their function is to connect or disconnect a path or subcircuit, in a power electronics circuit, to achieve the desired conversion. Therefore, the functionality of an ideal semiconductor device as a switch can be modeled using the Heaviside function, i.e., Equation (1.6), in HOL Light:

**Definition 3.1:** *Switch Functionality*

$$\vdash \forall t. \text{ semi\_switch } t = \text{if } t < \&0 \text{ then } \&0 \text{ else} \\ (\text{if } t = \&0 \text{ then } \&1 / \&2 \text{ else } \&1)$$

Definition 3.1 models the functionality of a semiconductor switch as a real value 1, for connected status, and 0, for disconnected status, in higher-order logic. Whereas, at the switching instance  $t$ , it has value  $1/2$ . The  $\&$  is a typecasting operator in HOL Light that maps a number to a real number. In our formalization, we use switch status or switching function to refer connected or disconnected switch.

The mathematical expressions for ideal elements in Table 1.1 are formally defined in HOL Light as,

**Definition 3.2:** *Ideal Inductor Current*

$$\vdash \forall i_o L v. \text{ ideal\_ind\_curr } v L i_o = \\ (\lambda t. i_o + Cx (\&1 / L) * \text{integral } (\text{interval } [\&0, t]) v)$$

**Definition 3.3:** *Ideal Capacitor Current*

$$\vdash \forall C v. \text{ ideal\_cap\_curr } C v = \\ (\lambda t. Cx C * \text{vector\_derivative } v \text{ (at } t))$$

**Definition 3.4:** *Resistor Current*

$$\vdash \forall v R. \text{ res\_curr } R v = (\lambda t. v t * Cx (\&1 / R))$$

**Definition: 3.5** *Resistor Voltage*

$$\vdash \forall i R t. \text{resis\_volt } i R t = (i t) * Cx(R)$$

**Definition: 3.6** *Ideal Inductor Voltage*

$$\vdash \forall i R t. \text{ideal\_ind\_volt } i L t = Cx(L) * (\text{vector\_derivative } i (\text{at } t))$$

**Definition: 3.7** *Ideal Inductor Voltage*

$$\vdash \forall v_0 i R t. \text{ideal\_cap\_volt } v_0 i R t = \\ v_0 + Cx(1/C) * (\text{integral } (\text{lift}[0, t]) i)$$

The function `ideal_resis_volt` accepts current  $i : (\text{real} \rightarrow \text{complex})$ , through a resistor and resistance value,  $R : (\text{real})$ , to express the voltage across the resistor. Similarly, the function `ideal_ind_volt` accepts the current value through an inductor,  $i : (\text{real} \rightarrow \text{complex})$ , and inductance,  $L : (\text{real})$  to express the voltage across the inductor. Finally, the function `ideal_cap_volt` models the voltage across a capacitor by using initial voltage,  $v_0 : (\text{real})$ , capacitance,  $C : (\text{real})$ , and the current through capacitor,  $i : (\text{real} \rightarrow \text{complex})$ . Whereas, `vector_derivative` and `integral` are higher-order-logic functions that model the mathematical derivative and integral, respectively, in HOL Light.

### 3.1.2 Formal Modeling of Non-ideal Circuit Components

Based on the formally defined models of the ideal inductor, capacitor and resistor relationships, i.e., Definition 3.2-3.7, we formally model the voltage and current relationships of non-ideal components, described in Table 1.2, in higher-order logic, as:

**Definition: 3.8** *Non-ideal Inductor Voltage*

$$\vdash \forall i L \text{ESR } t. \text{non\_ideal\_ind\_volt } i L \text{ESR } t = \text{ideal\_ind\_volt } i L t + \\ \text{resis\_volt } i \text{ESR } t$$

**Definition: 3.9** *Ideal Inductor Voltage*

$$\vdash \forall V_0 L \text{ ESR } v \ t. \text{ non\_ideal\_ind\_curr } V_0 L \text{ ESR } v \ t = \text{ ideal\_ind\_curr } V_0 L \\ v \ t + \text{ resis\_curr } v \ \text{ ESR } \ t$$

The function `non_ideal_ind_volt` takes arguments of inductor current,  $i : (\text{real} \rightarrow \text{complex})$ , inductance,  $L : (\text{real})$ , inductor ESR,  $\text{ESR} : (\text{real})$ , and time,  $t : (\text{real})$ , to express the voltage across the inductor. Whereas, the function `non_ideal_ind_curr` accepts the initial voltage,  $V_0 : (\text{real})$ , inductance,  $L : (\text{real})$ , inductor ESR,  $\text{ESR} : (\text{real})$ , and time,  $t : (\text{real})$ , to find the current through the inductor.

**Definition: 3.10** *Non-ideal Capacitor Voltage*

$$\vdash \forall i_0 i \ C \ \text{ ESR } \ t. \text{ non\_ideal\_cap\_volt } i_0 i \ C \ \text{ ESR } \ t = \text{ ideal\_cap\_volt } i_0 i \\ C \ t + \text{ resis\_volt } i \ \text{ ESR } \ t$$

**Definition: 3.11** *Non-ideal Capacitor Current*

$$\vdash \forall v \ C \ \text{ ESR } \ t. \text{ non\_ideal\_cap\_curr } v \ C \ \text{ ESR } \ t = \text{ ideal\_cap\_curr } v \ C \ t + \\ \text{ resis\_curr } v \ \text{ ESR } \ t$$

The function `non_ideal_cap_volt` accepts the initial current,  $i_0 : (\text{real})$ , capacitor current,  $i : (\text{real} \rightarrow \text{complex})$ , capacitance,  $C : (\text{real})$ , capacitor ESR,  $\text{ESR} : (\text{real})$ , and time,  $t : (\text{real})$ , and returns the voltage across the capacitor. Similarly, the function `non_ideal_cap_curr` accepts the capacitor voltage,  $v : (\text{real} \rightarrow \text{complex})$ , capacitance,  $C : (\text{real})$ , capacitor ESR,  $\text{ESR} : (\text{real})$ , and time,  $t : (\text{real})$ , to model the current through the capacitor.

**Definition: 3.12** *Semiconductor on-resistance Voltage*

$$\vdash \forall i \ R_{\text{on}} \ t. \text{ semi\_resis\_model\_volt } i \ R_{\text{on}} \ t = \\ \text{ resis\_volt } i \ R_{\text{on}} \ t$$

**Definition: 3.13** *Semiconductor on-resistance Current*

$$\vdash \forall v \ R_{\text{on}} \ t. \text{ semi\_resis\_model\_curr } v \ R_{\text{on}} \ t = \\ \text{ resis\_curr } v \ R_{\text{on}} \ t$$

The function `semi_resis_model_volt` accepts the current,  $i : (\text{real} \rightarrow \text{complex})$ , on-resistance,  $R_{\text{on}} : (\text{real})$ , and time,  $t : (\text{real})$ , to model the voltage across the on-resistance of the semiconductor device. Whereas, `semi_resis_model_curr` accepts the voltage across a capacitor,  $v : (\text{real} \rightarrow \text{complex})$ , on-resistance,  $R_{\text{on}} : (\text{real})$ , and time,  $t : (\text{real})$ , to determine the current through the on-resistance of the semiconductor device.

**Definition 3.14** *Semiconductor Forward-voltage Drop Model*

$\vdash \forall V_F i R_D t. \text{semi\_volt\_rises\_model\_volt } V_F i R_D t = C V_F + \text{rises\_volt } i R_D t$

The function `semi_volt_resis_model_volt` accepts the forward voltage drop,  $V_F : (\text{real})$ , current,  $i : (\text{real} \rightarrow \text{complex})$ , through on-resistances,  $R_{\text{on}} : (\text{real})$ , and time,  $t : (\text{real})$ , to model the voltage across the semiconductor device.

Definitions 3.1-3.14, enable us to formally specify and reason about the implementation behavior of given converter circuits in higher-order logic.

To accomplish the formal modeling of the basic circuit theory notions, we also formalize the Kirchoff's voltage and current laws:

**Definition 3.15:** *Kirchoff's Voltage Law (KVL)*

$\vdash \forall \text{vol\_lst } t. \text{kvl } \text{vol\_lst } t = \text{vsum } (0.. \text{LENGTH } \text{vol\_lst} - 1) (\lambda n. \text{EL } n \text{ vol\_lst } t) = Cx \ (\&0)$

**Definition 3.16:** *Kirchoff's Current Law (KCL)*

$\vdash \forall \text{cur\_lst } t. \text{kcl } \text{cur\_lst } t = \text{vsum } (0.. \text{LENGTH } \text{cur\_lst} - 1) (\lambda n. \text{EL } n \text{ cur\_lst } t) = Cx \ (\&0)$

The `kvl` and `kcl` functions accept lists of type  $(\mathbb{R} \rightarrow \mathbb{C})$ , to express the behavior of the time dependent voltages and currents in the given power converter circuit and a time variable  $t$ . They return the predicates that guarantee that the sum of the voltages in a loop or sum of the currents at a node are zero for all the time instants.



## 3.2 Switching Function Technique

Voltages and currents at the switching junction in higher-order logic are defined, as:

**Definition 3.17:** *Modified KVL*

$$\vdash \forall \text{ mod\_lst volt\_lst } t. \text{ switch\_volt mod\_lst volt\_lst } t = \\ \text{vsum } (0..\text{LENGTH mod\_lst} - 1) (\lambda n. \text{EL } n \text{ volt\_lst } t * \text{Cx } (\text{EL } n \\ \text{mod\_lst}))$$

The function `switch_volt` describes the voltage at the switch junction using Equation 1.1(a). It accepts a list, `volt_lst`, which contains all the possible voltage drops at the switching junction, a list of modes, `mod_lst`, which contains the switch status or switching function for each mode, and `t` is the time, which indicates that this function is time dependent. Whereas, `EL` is a HOL `Light` function, which accepts a list `volt_lst` and index of list element `n` and returns the corresponding list member.

**Definition 3.18:** *Modified KCL*

$$\vdash \forall \text{ mod\_lst curr } t. \text{ switch\_current mod\_lst curr } t = \\ \text{curr } t * \text{vsum } (0..\text{LENGTH mod\_lst} - 1) (\lambda n. \text{Cx } (\text{EL } n \\ \text{mod\_lst}))$$

Definition 3 formally models the current at the switching junction using Equation 1.1(b). It accepts an argument `curr`, which represents the total supplied current to the switch junction, a list of modes, `mod_lst`, which contains the switch status or switching function for each mode, and `t`, which represents time.

## 3.3 Properties of Generalized Function

The voltages and currents in power electronics circuits are piecewise functions due to the switching action. We formally verify the integration and differen-

tiation properties of functions expressed using Heaviside function (Equation 1.6).

**Theorem 3.1:** *Integration of Piecewise Function*

$\vdash \forall f a b c x.$

$$\begin{aligned} & [A1] (\forall t. (\lambda x. f(x)) \text{differentiable\_on } s) \wedge \\ & [A2] \sim(\text{real\_interval } [a,b] = \{\}) \wedge [A3] c \in [a, b] \\ & \Rightarrow \int_a^b (\lambda x. \text{semi\_switch } x c) * f(x) = \int_c^b (\lambda x. f(x)) \end{aligned}$$

In above theorem,  $f : (\text{real} \rightarrow \text{complex})$  is a complex valued function and `semi_switch` is the Heaviside function that models switching functionality. Assumption A1 imposes condition on the differentiability of the given function,  $f$ . Assumptions A2-A3 ensure that a given real interval is a valid interval with upper and lower bounds, i.e.,  $a$  and  $b$ . Whereas,  $c \in [a, b]$  is the switching instance of the semiconductor switch.

Theorem 3.1 formally verifies the generalized property of step function that changes the integral limits of the given function  $f$ .

**Theorem 3.2:** *Derivative of a Heaviside Function*

$\vdash \forall x. [A1] \sim(x = 0) \Rightarrow$

$$\text{vector\_derivative } (\text{lift} \circ (\lambda x. \text{semi\_switch } x) \circ \text{drop}) \text{ at } (\text{lift } x) = (\text{lift } 0)$$

In above theorem, Assumption A1 ensures that the singularity point is excluded from the domain of the given function. In case of power electronics circuits, this singularity corresponds to the switching instance. Whereas, `vector_derivative` is the higher-order-logic definition of the partial derivative in multivariate differentiation theory of HOL Light.

Theorem 3.2 allows to formally reason and verify the differentiation of circuit parameters in the analysis and design of the power electronics circuits.

## 3.4 Summary and Discussions

In this chapter, we described the formal basic circuit theory concepts to formally specify and verify the power electronics circuits. We provide higher-order-logic models of ideal and non-ideal power electronics circuit components and modified Kirchoff's voltage and current laws at the switching junction in a circuit. Moreover, to formally reason about the piecewise nature of the circuit variables, we formally verify results of integration and differentiation of piecewise functions described using Heaviside function.

The formal models developed in this chapter enable us to formally specify and reason about the topologies of power electronics circuits. The ideal and non-ideal equivalent circuit models are widely used to analyze the functionality and specify the design parameters of the power electronics systems [24]. On the other hand, the switching function technique allows to leverage upon the modified Kirchoff's current and voltage laws to specify the circuit parameters as a single expression which is the core objective of the analysis techniques in power electronics systems [44]. Finally, the formally verified results of Section 3.3, i.e., Theorems 3.1 and 3.2, provide mandatory support for the formal analysis and verification of the power electronics systems within the sound core of the HOL `Light` theorem prover. In power electronics systems, formal verification of topology, steady-state behavior and design specifications require integration and differentiation operations and hence these results are direly needed to perform the formal analysis and verification of involved piecewise functions . The mechanized results of Theorem 3.1 and 3.2 are generic in nature and can provide formal reasoning support for large class of systems that use piecewise functions to capture the underlying phenomenon [19].

# 4

## Formalization of Periodic Steady-state Analysis

In this chapter, we present the formalization required for the time-domain periodic steady-state analysis of the power electronics circuits. To formally describe the behavior of the circuits in steady-state for each mode, we formally model the  $n$ -th order differential equations in the HOL Light theorem prover. In steady-state, the variables of interest in power electronics circuits are deduced as the solution of the corresponding  $n$ -th order differential equations. Therefore, we provide generic results for the formal verification of the solution of the  $n$ -th order differential equations. This framework enables us to formally verify the mathematical expression of the variables of the given circuit which are in practice used to analyze and design the circuits. Finally, we provide formal models of steady-state characteristics and design specifications using the circuit variables. The proposed formalization is then used to formally verify the topology, steady-state behavior and expression for the steady-state output of a DC-DC Buck converter.

## 4.1 Differential Equation Representation

We formalized the  $n^{\text{th}}$ -order derivative function in higher-order logic as follows:

**Definition 4.1:** *n-th Order Derivative*

$$\begin{aligned} \vdash \forall n f t. \quad & (\text{n\_vec\_deri } 0 f t = f t) \quad \wedge \\ & (\forall n. \quad \text{n\_vec\_deri } (\text{SUC } n) f t = \\ & \quad \text{n\_vec\_deri } n (\lambda t. \quad \text{vector\_derivative } f \text{ at } t) t) \end{aligned}$$

The function `n_vec_der` accepts a positive integer `n` that represents the order of the derivative, the function `f:( $\mathbb{R} \rightarrow \mathbb{C}$ )` that represents the complex-valued function that needs to be differentiated, and the variable `t:( $\mathbb{R}$ )` that is the variable with respect to which we want to differentiate the function `f`. It returns the  $n^{\text{th}}$ -order derivative of `f` with respect to `t`. Now, based on this definition, we can formalize the left-hand side (LHS) and right-hand side (RHS) of Equation (1.3) in HOL Light as the following definitions:

**Definition 4.2:** *LHS of a Differential Equation*

$$\begin{aligned} \vdash \forall P y t. \quad & \text{diff\_eq\_lhs } A f t = \\ & \text{vsum } (0..\text{LENGTH } A) (\lambda n. \quad \text{Cx } (\text{EL } n A t) * \text{n\_vec\_deri } n f t) \end{aligned}$$

**Definition 4.3:** *RHS of a Differential Equation*

$$\begin{aligned} \vdash \forall L y t. \quad & \text{diff\_eq\_rhs } L p t = \\ & \text{vsum } (0..\text{LENGTH } L) (\lambda n. \quad \text{Cx } (\text{EL } n L) * \text{EL } n p t) \end{aligned}$$

In the above definitions, `A` and `L` are the coefficient's lists, `f:( $\mathbb{R} \rightarrow \mathbb{C}$ )` and `p(t):( $\mathbb{R} \rightarrow \mathbb{C}$ )` are complex-valued functions, and `t:( $\mathbb{R}$ )` is the time variable to formally model the linear ordinary differential equation.

We formally model the  $n$ -th order differentiability of list of functions in higher-order logic as,

**Definition 4.4:** *differentiability of functions*

$$\begin{aligned} \vdash \forall n. \quad & \text{n\_differentiable\_fn } f \ n = \\ & \text{n\_differentiable\_fn } [] \ n = T \wedge \\ & \text{n\_differentiable\_fn } (\text{CONS } f \ t) \ n = \\ & \forall m. \quad (m \leq n) \implies (\lambda x. \text{ n\_vec\_deri } m \ f \ t) \text{ differentiable } (\text{at } x) \\ & \wedge \text{n\_differentiable\_fn } t \ n \end{aligned}$$

In the above definition, `n_differentiable_fn` is recursively defined and accepts a list of functions, `f`, and the order of the differentiability, `n`. First conjunction defines base case for empty list and assigns it boolean truth value `T`. In second conjunction, `CONS` is a higher-order-logic function in `HOL Light` for list manipulation and returns head element of the given list (`f`) and rest of the list (`t`). The order of the derivative of the function, `m`, is specified using Definition 4.1. Finally, third conjunction calls the differentiability function for the function list `t`.

We formally specify the solution of homogeneous differential equation in `verb|HOL Light|` as,

**Definition 4.5:** *Homogeneous Solution*

$$\begin{aligned} \vdash \forall Yh \ L \ t. \quad & \text{n\_homo\_sln } Yh \ L \ t = \text{n\_homo\_sln } [] \ L \ t = T \wedge \\ & \text{n\_homo\_sln } (\text{CONS } yh \ x) \ t = \text{diff\_eq\_lhs } yh \ L \ t = C \ (&0) \wedge \\ & \wedge \text{diff\_eq\_lhs } x \ L \ t \end{aligned}$$

The higher-order-logic function, `n_homo_sln`, accepts a list of solution of a homogeneous differential equation, `Yh`, list of coefficients of the differential equation and independent time variable, `t`. The first conjunct defines the base case of the recursive definition and assigns true boolean value (`T`) for an empty list. The second conjunct formally specifies the condition for the solution, i.e., the solution satisfies the differential equation. Finally, third conjunct calls the function for the rest of the solutions in the list.

We formally specify the solution of non-homogeneous differential equation in `HOL Light` as,

**Definition 4.6:** *Non-homogeneous Solution*

$$\vdash \forall A L y p g t. \quad \text{n\_order\_homo\_sln } A L y g t = \\ \text{diff\_eq\_lhs } A y p t = \text{diff\_eq\_rhs } L g t$$

The higher-order-logic function `n_order_homo_soln` accepts lists of coefficients, `A` and `L`, for right- and left-hand sides of a differential equation, lists of particular solution and function, `yp` and `g`, and independent variable, i.e., time (`t`). The formal definition formally specifies the condition for the valid solution, i.e., solution verifies the differential equation.

We formally define a linear combination of the solutions of a differential equation in higher-order logic as,

**Definition 4.7:** *Solution of a Differential Equation*

$$\vdash \forall C y h t. \quad \text{linear\_solution } C y t = \\ \text{linear\_solution } C [] t = Cx (&0) \wedge \\ \text{linear\_solution } C (\text{CONS } h x) t = \\ Cx (\text{EL } (\text{LENGTH } C - \text{LENGTH } (\text{CONS } h x)) ) * (h t) + \\ \text{linear\_solution } C x t$$

The function `linear_sol` models the linear solution combination of fundamental solutions, i.e.,  $\sum_{i=1}^n c_i y_i(t)$ , using the lists of solution functions `Yh` and arbitrary constants `C`.

Definition 4.1 is used to formally define the steady-state condition of the power electronics circuits as:

**Definition 4.6:** *Steady-state Conditions*

$$\vdash \forall n. \quad ( \text{steady\_state } 0 f T_p = \\ (\text{n\_vec\_deri } 0 f (&0) = \text{n\_vec\_deri } 0 f T_p) ) \wedge \\ ( \text{steady\_state } (\text{SUC } n) f T_p = \\ (\text{n\_vec\_deri } (\text{SUC } n) f (&0) = \text{n\_vec\_deri } (\text{SUC } n) f T_p) )$$

The above definition is higher-order logic equivalent of steady-state conditions described in Problem (1.3). In the above definition, the first conjunct

defines the base case which represents the steady-state conditions for the functions values at the initial time,  $t = 0$  and final time,  $t = T_p$ , whereas, the second conjunct accounts for steady-state conditions for the higher order function derivatives at initial and final time values.

The above generic formalization allows to formally model the dynamic behavior of systems represented by differential equations. We have utilized this formalization to formally specify and reason the periodic steady-state behavior of power converters, described in Equation 1.3.

## 4.2 Solution Verification of Differential Equations

The linearity property of the derivatives (Equation 1.7) is formally verified for the complex-valued functions as:

**Theorem 4.1:** *Linearity of  $n$ -th Order Derivative*

$\vdash \forall n f h t.$

[A1]  $(\lambda m t. m \leq n \Rightarrow (\lambda t. n\_vec\_deri m f t) \text{ differentiable at } t) \wedge$

[A2]  $(\lambda m t. m \leq n \Rightarrow (\lambda t. n\_vec\_deri m h t) \text{ differentiable at } t) \Rightarrow n\_vec\_deri n (\lambda t. Cx a * f t + Cx b * h t) t = Cx a * n\_vec\_deri (\lambda t. f t) t + Cx b * n\_vec\_deri (\lambda t. g t) t$

Theorem 4.1 formally verifies linearity property of the  $n$ -th order derivative operator, i.e.,  $\frac{d^n}{dx^n}$ . The formal verification is accomplished by induction on the order of the derivative,  $n$  in HOL Light theorem prover and using Definitions 2.10 and 4.1.

Now we formally verify solution of homogeneous differential equation solution in HOL Light as,



**Theorem 4.2:** *Solution of a Homogeneous Differential Equation*

$\vdash \forall Y_h C L t.$

[A1]  $(n\_homo\_soln L Y_h t) \wedge$

[A2]  $(n\_differentiable\_fn Y_h (LENGTH L)) \wedge$

$\Rightarrow diff\_eq\_lhs L (\lambda t. linear\_sol C Y_h t = Cx \ \&0)$

Assumption [A1] formally specifies the solutions of the differential equation using Definition 4.5. The differentiability of these solutions is formally specified using Definition 4.4. Whereas, conclusion formally verifies the linear combination of the differential equation solutions (formally specified using Definition 4.7) for the specified solution list  $Y_h$ .

We formally verified the solution of a linear differential equation, represented by Equation (1.4), in the HOL `Light` theorem prover as follows:

**Theorem 4.2:** *Solution of a Differential Equation*

$\vdash \forall Y_h C Y_p A L p t.$

[A1]  $(n\_differentiable\_fn Y_h (LENGTH A)) \wedge$

[A2]  $(n\_differentiable\_fn Y_p (LENGTH L)) \wedge$

[A3]  $(n\_homo\_soln A Y_h t) \wedge$  [A4]  $(n\_nonhomo\_soln L Y_h Y_p t)$

$\Rightarrow diff\_eq\_lhs A (\lambda t. linear\_sol C Y_h t + Y_p t) =$

$diff\_equ\_rhs L p t$

In Theorem 4.2, Assumptions A1 and A2 ensure the  $n^{\text{th}}$ -order differentiability of the fundamental solutions, given as a list  $Y_h$ , and particular solution, provided as a list  $Y_p$ , respectively. The predicate in the Assumption A3, i.e., `n_order_homo_eq_soln_list`, ensures that each element of the list  $Y_h$  is a solution of the given differential equation, when  $p(t) = 0$  in Equation (1.3), where  $L$  is the list of coefficients. Similarly, the predicate in Assumption A4, i.e., `n_order_nonhomo_eq_soln_list`, ensures that the particular solution,  $Y_p$ , satisfies the differential Equation (1.3). The formal verification of Theorem 4.2 is based on Theorem 4.1 and the formally verified lemma about solution of homogeneous differential equation, i.e., when  $p(t) = 0$  in Equation

(1.3). More details about the modeling and verification steps can be found in our proof script [2].

## 4.3 Modeling of Steady-state Characteristics and Design Specifications

In this section, we formally define the periodic steady-state characteristics and converter specifications described in Table 1.3.

The average value of a circuit variable, such as voltage or current, is defined in higher-order logic as:

**Definition: 4.7** *Average Value of a Function*

$$\vdash \forall s f. \text{average\_ac } s f = \frac{1}{\text{interval\_upperbound } s - \text{interval\_lowerbound } s} * (\text{integral } s f)$$

Where the function `average_ac` accepts a real interval,  $s : (\text{real} \rightarrow \text{bool})$ , and a variable,  $f : (\text{real} \rightarrow \text{complex})$ , that can be used to represent the circuit voltage or current, and returns its average value. The functions `interval_upperbound` and `interval_lowerbound` return upper and lower bounds, respectively, of the given real interval.

**Definition: 4.8** *Ripple Quantity*

$$\vdash \forall f t_p t_v. \text{ripple } f t_p t_v = f t_p - f t_v$$

The function `ripple` accepts a function  $f : (\text{real} \rightarrow \text{complex})$ , representing the circuit voltage or current, and time instances,  $t_p$  and  $t_v$ , where the function is maximum and minimum, respectively, to return the ripple (or maximum change) in the given variable.

**Definition: 4.9** *RMS of a Ripple Quantity*

$$\vdash \forall f t_p t_v. \text{rms\_ripple } f t_p t_v = \frac{\text{ripple } f t_p t_v}{2 * \text{csqrt } Cx (3)}$$

The function `rms_ripple` accepts the ripple value of the circuit variable, `fr`, and returns the root mean square (RMS) value of the ripple voltage or current.

**Definition: 4.10** *RMS of a AC Quantity*

$$\vdash \forall s f t_p f_v. \text{rms\_ac } s f t_p f_v = \text{csqrt} \left( (\text{average\_ac } s f) \text{ pow } 2 \right) + (\text{rms\_ripple } f t_p t_v \text{ pow } 2)$$

The function `rms_ac` accepts the average (`average_ac`) and ripple RMS (`ripple_rms`) values of a circuit variable, `f : (real → complex)`, to return the RMS value of the given variable.

**Definition: 4.11** *Power Dissipation*

$$\vdash \forall s f t_p t_v r. \text{pow\_ac } s f t_p t_v r = (\text{rms\_ac } s f t_p t_v) \text{ pow } 2 * \text{Cx } (r)$$

The function `pow_ac` accepts the RMS value of the current through a resistance, `r`, and returns the power dissipation due to the given resistance.

## 4.4 Case study: Periodic Steady-state Analysis of Ideal DC-DC Buck Converter

The DC-DC buck converter is a commonly used power converter that steps down a given input to a desired output level. In a DC-DC Buck converter, operating in a continuous conduction mode, a switch controls the flow of energy from the raw source,  $V_s$ , to the output by periodically switching between Positions 1 and 2, as shown in Fig 6.1a. The energy is stored in the inductor when the switch is at Position 1, and is dissipated to the output circuitry, when the switch is at Position 2. The circuit has two modes, i.e.,  $n = 2$ , defined by the switching instances,  $t_0$ ,  $t_{on}$ , and  $t_{off}$ . In periodic steady-state the circuit will repeat its behavior periodically over the time period  $T_p$ . Moreover, due to periodic steady-state the dependence on  $t_0$  can be dropped and therefore have assigned  $t_0 = 0$  in our analysis. Applying Kirchoff's current

and voltage laws in switch Positions 1 and 2, gives the following differential equations for the respective modes:

$$\begin{aligned}
 i_L &= i_C + i_R \\
 \frac{d^2}{dt^2} V_{out}^1(t) + \frac{1}{RC} \frac{d}{dt} V_{out}^1(t) + \frac{1}{LC} V_{out}^1(t) &= \frac{V_s}{LC} \\
 V_{out}^1(t) &= c_1 e^{s_1 t} + c_2 e^{s_2 t} + V_s
 \end{aligned} \tag{4.1}$$

$$\begin{aligned}
 i_L &= -i_c - i_R \\
 \frac{d^2}{dt^2} V_{out}^2(t) + \frac{1}{RC} \frac{d}{dt} V_{out}^2(t) + \frac{1}{LC} V_{out}^2(t) &= 0 \\
 V_{out}^2(t) &= c_3 e^{s_3 t} + c_4 e^{s_4 t}
 \end{aligned} \tag{4.2}$$

Where,  $V_{out}$  is the output voltage of the converter, as shown in the Figure 6.1a, and  $s_1, s_2, s_3$  and  $s_4$  are the roots of the characteristic equation of the converter in two modes. Moreover,  $s_1 = s_3$  and  $s_2 = s_4$  due to the identical characteristic equations. The solution of Equations (4.1-4.2), over the time period  $T_p$ , can be written using the Heaviside step function as

$$V_{out}(t) = u(t - t_{on}) V_{out}^1(t) + (1 - u(t - t_{on})) V_{out}^2(t) \tag{4.3}$$

In the periodic steady-state, the voltage of the DC-DC buck converter satisfies the following conditions

$$V_{out}(0) = V_{out}(T), \quad \frac{d}{dt} V_{out}(0) = \frac{d}{dt} V_{out}(T) \tag{4.4}$$

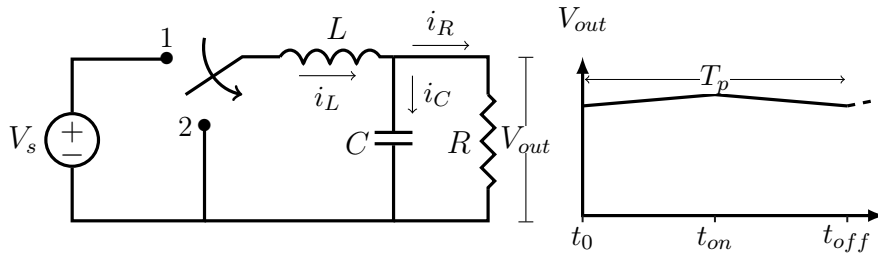


Figure 4.1: DC-DC buck Converter

The steady-state conditions provide two algebraic equations, however, there are four constants involved in the solution. Two more algebraic equations can be obtained from the continuity of the voltage, i.e.,  $V_{out}$ , due to continuous conduction mode of the circuit, i.e.,

$$V_{out}^1(t_{on}) = V_{out}^2(t_{on}), \quad \frac{d}{dt}V_{out}^1(t_{on}) = \frac{d}{dt}V_{out}^2(t_{on}) \quad (4.5)$$

Equations (4.4-4.5) are used to specify the periodic steady-state voltage that allows finding the minimum and peak conduction currents in steady-state. These currents can then be used to determine ripple currents, which are essentially crucial in specifying the components in the design of the power electronics circuits.

#### 4.4.1 Topology

The first step, in the formalization of the DC-DC Buck converter consists of using the switching function technique to write the switch junction voltages. Now, using Definitions 3.2, 3.3, 3.4, 3.15, 3.16, and 3.17, we can formalize the implementation of DC-DC Buck converter as:

**Definition 4.12:** *Implementation*

```

⊢ ∀ i_o L C R V_s V_out V_L t_on t.
  buck_ckt_impl i_o L C R V_s V_out V_L t_on t =
    (Vl = switch_volt [λt. Cx V_s - V_out t; (λt. -V_out t)]
      [&1 - semi_switch (t - t_on); semi_switch (t - t_on] t)
    ∧ (∀t. ~ (t = t_on) ⇒
      kcl [ind_curr (λt. V_L t) L i_o; cap_curr C (λt. -V_out t);
          res_curr R (λt. -V_out t)] t )

```

In the above definition,  $V_s$  is the supply voltage,  $V_{out}$  is the voltage drop at the junction of all these components, with respect to the ground, and  $V_L$  is the voltage drop across the inductor. However, due to the the presence of the

switching junction, we model the inductor voltage, in the first conjunct, using the `switch_volt` function, which is provided with two lists; one for all the possible voltage drops, and the other with all the corresponding switching functions for every mode, and an independent variable `t`. Where, `ton`, is the exact switching instant. This voltage is then used to apply the conventional Kirchoff's current law, using the function `kcl`, which accepts a list of currents, and an independent variable, i.e., `t`.

This implementation model results in the ordinary linear differential equations of the system, which can be described using Definitions 4.2 and 4.3 as:

**Definition 4.13:** *Behavior Specification*

$$\begin{aligned} &\vdash \forall i_o V_s V_{out} L C R t_{on} t. \\ &\text{buck\_diff\_equ } i_o V_s V_{out} L C R t_{on} t = \\ &\text{if } (t < t_{on}) \text{ then diff\_eq\_lhs } \left[ \frac{1}{L * C}; \frac{1}{R * C}; 1 \right] (V_{out}(t)) t = \\ &\quad \text{diff\_eq\_rhs } \left[ \frac{V_s}{L * C} \right] [1] t \\ &\text{else diff\_eq\_lhs } \left[ \frac{1}{L * C}; \frac{1}{R * C}; 1 \right] (V_{out}(t)) t = \text{diff\_eq\_rhs } [0] [0] t \end{aligned}$$

According to the proposed methodology, as a first step, we formally verify the implementation and behavior of the Buck converter using the formal model of switching function technique and linear order differential equations as:

**Theorem 4.3:** *Implementation and Behavior*

$$\begin{aligned} &\vdash \forall i_o V_s V_L V_{out} L C R t_{on} T_p t. \\ &[A1] (\forall t. V_L \text{ continuous\_on } [0, t]) \wedge \\ &[A2] \sim (C = 0) \wedge \\ &[A3] (t \in (0, T_p)) \wedge \\ &[A4] \sim(t = t_{on}) \wedge [A5] (t_{on} \in (0, T_p)) \wedge \\ &[A6] (\forall t. \text{differentiable\_n\_vec\_deri } 1 V_{out} t) \wedge \\ &[A7] \text{buck\_ckt\_impl } i_o L C R V_s V_{out} V_L t_{on} t \\ &\quad \Rightarrow \text{buck\_diff\_equ } i_o V_s V_{out} L C R t_{on} t \end{aligned}$$

Assumption A1 ensures that the converter is operating in the continuous conduction mode. Assumption A2 prevents a division by zero case in the formal analysis. Assumptions A3-A4 ensure that the time is over one time period of the system and does not include the singularities, at  $t_0 = 0$ ,  $t = t_{on}$  and  $t = T_p$ , due to switching action. Whereas, Assumptions A5 specifies that the switching time,  $t = t_{on}$ , lies within the open interval defined by the single time period of the circuit. Assumption A6 formally specifies the differentiability of the function,  $V_{out}$ , and its first derivative. The predicate `differentiable_n_vec_der1` accepts a number,  $n$ , and function,  $f$ , and specifies the differentiability of the function upto its  $n^{\text{th}}$ -derivative. Finally, Assumption A7 specifies the formal implementation of the power converter circuit using Definition 4.12. The formal proof of Theorem 4.3 involves taking derivative of Assumption A7, which consists of piecewise functions, by employing Theorems 3.1 and 3.2.

#### 4.4.2 Solution of Differential Equations

Following the proposed methodology, the next task is to formally verify the correctness of the solution of the ordinary linear differential equations of the Buck converter in HOL Light. Therefore, we define the piecewise solution, i.e., Equation (4.3), of the Buck converter in higher-order logic as:

**Definition 4.14:** *Solution*

```

⊢ ∀ c1 c2 c3 c4 s1 s2 ton t.
  solution Vs c1 c2 c3 c4 s1 s2 ton t =
  linear_sol [c1; c2] (cexp_list [s1; s2]) t *
    Cx (semi_switch (t - ton)) +
  linear_sol [c3; c4] (cexp_list [s1; s2]) t *
    Cx (&1 - semi_switch (t - ton))

```

Where  $c_1$ ,  $c_2$ ,  $c_3$  and  $c_4$  are arbitrary constants,  $s_1$  and  $s_2$  are the roots of homogeneous differential equations corresponding to Equations (7)

and (8), respectively. Whereas, the `cexp_list` function is a higher-order-logic function to express the exponential form of the solution for real and distinct roots, i.e.,  $s_1$  and  $s_2$ , of the circuit. It is defined as:

**Definition 4.15:** *Exponential Solution*

$$\vdash \forall x. (\text{cexp\_list } [] = []) \wedge \\ \text{cexp\_list } (\text{CONS } s \ t) = \text{CONS } (\lambda x. \text{cexp } (s * Cx \ (x))) \ (\text{cexp\_list } t)$$

Next, using Definition 4.14, we formally verify the correctness of the solution of the differential equations, in each mode of the converter, in HOL `Light` as:

**Theorem 4.4:** *Solution Verification*

$$\vdash \forall i_0 \ V_s \ V_{\text{out}} \ L \ C \ R \ c_1 \ c_2 \ c_3 \ c_4 \ s_1 \ s_2 \ t_{\text{on}} \ T_p \ t . \\ \text{[A1]} \ (\forall t. \sim(t = t_{\text{on}}) \Rightarrow V_{\text{out}} = \text{solution } c_1 \ c_2 \ c_3 \ c_4 \ s_1 \ s_2 \ t_{\text{on}} \ t) \wedge \\ \text{[A2]} \ (s_1 = -\frac{1}{2RC} + \frac{1}{2} \sqrt{\frac{1}{(RC)^2} - \frac{4}{LC}}) \wedge \\ \text{[A3]} \ (s_2 = -\frac{1}{2RC} - \frac{1}{2} \sqrt{\frac{1}{(RC)^2} - \frac{4}{LC}}) \wedge \\ \text{[A4]} \ (4 \ R^2 \ C \leq L) \wedge \\ \text{[A5]} \ (0 < L) \wedge \\ \text{[A6]} \ (0 < R) \wedge \\ \text{[A7]} \ (0 < C) \wedge \\ \text{[A8]} \ (t \in (0, T_p)) \wedge \\ \text{[A9]} \ \sim(t = t_{\text{on}}) \wedge \\ \text{[A10]} \ (t_{\text{on}} \in (0, T_p)) \\ \Rightarrow \text{buck\_diff\_equ } i_0 \ V_s \ V_{\text{out}} \ L \ C \ R \ t_{\text{on}} \ t$$

Assumption **A1** formally defines the output voltage  $V_{\text{out}}$  as a piecewise function, over the time period,  $T_p$ , of the converter circuit. Assumptions **A2-A3** formally specify the roots of the equation. Assumption **A4** formally specifies the condition on the circuit parameters for real and distinct roots. Assumptions **A5-A7**, ensure the positive values of inductance, resistance and capacitance of the circuit. Assumptions **A8-A9** ensure that the time is over one time period



of the system and does not include the singularities, at  $t_0 = 0$ ,  $t = t_{on}$  and  $t = T_p$ , due to switching action. Whereas, Assumptions A10 specifies that the switching time,  $t = t_{on}$ , lies within the open interval defined by the single time period of the circuit.

The formal verification of Theorem 4.4 utilized the formally verified results of Theorems 3.1, 3.2 and 4.2.

### 4.4.3 Steady-state Expressions for Output Voltage

Finally, we present the formally verified results of periodic steady-state voltage of the DC-DC Buck converter as:

**Theorem 4.5:** *Steady-state Output*

$\vdash \forall V_s V_{out} c_1 c_2 c_3 c_4 s_1 s_2 t_{on} t T_p.$

[A1]  $(t \in (0, T_p)) \wedge$

[A2]  $\sim(t = t_{on}) \wedge$

[A3]  $(t_{on} \in (0, T_p)) \wedge$

[A4]  $(\forall t. \sim(t = t_{on}) \Rightarrow V_{out} = \text{solution } V_s c_1 c_2 c_3 c_4 s_1 s_2 t_{on} t)$

$\wedge$

[A5]  $(\forall t. \text{n\_vec\_deri } 1 (\lambda t. V_{out} t) \text{ continuous at } t) \wedge$

[A6]  $\sim(s_2 - s_1 = 0) \wedge$

[A7]  $\text{steady\_state } 1 V_{out} t \Rightarrow$

$$\begin{aligned} & \left( V_{out}(0) = \left( \frac{s_2}{s_2 - s_1} \right) \left[ \left( V_{out}(0) + \frac{1}{s_2} \frac{d}{dt} V_{out}(0) - V_s \right) e^{-t_{on}s_1} + V_s \right] e^{-T_p s_1} \right. \\ & + \left. \left( \frac{s_1}{s_2 - s_1} \right) \left[ \left( -V_{out}(0) - \frac{1}{s_1} \frac{d}{dt} V_{out}(0) + V_s \right) e^{-t_{on}s_1} - V_s \right] e^{-T_p s_2} \right) \wedge \\ & \left( -\frac{d}{dt} V_{out}(0) = \left( \frac{s_1 s_2}{s_2 - s_1} \right) \left[ \left( V_{out}(0) + \frac{1}{s_2} \frac{d}{dt} V_{out}(0) - V_s \right) e^{-t_{on}s_1} + V_s \right] \right. \\ & \quad \left. e^{-T_p s_1} + \left( \frac{s_1 s_2}{s_2 - s_1} \right) \left[ \left( -V_{out}(0) - \frac{1}{s_1} \frac{d}{dt} V_{out}(0) + V_s \right) e^{-t_{on}s_1} - V_s \right] \right. \\ & \quad \left. e^{-T_p s_2} \right) \end{aligned}$$

Assumptions A1 and A2 formally specify the analysis over one time period with singularities, at  $t = 0$ ,  $t = t_{on}$  and  $t = T_p$ , excluded. Whereas, Assumptions A3 specifies that the switching time,  $t = t_{on}$ , lies within the open

interval defined by the single time period of the circuit. Assumption **A4** formally defines the output voltage  $V_{\text{out}}$  as a piecewise function, over the time period,  $T_p$ , of the converter circuit. Assumption **A5** formally specifies the continuity of the function and its derivative, to ensure the continuous conduction mode. Assumption **A6** prevents the division by zero case in the analysis, and finally, Assumption **A7** defines the steady-state of the buck converter.

The formal proof of Theorem 4.5 essentially consists of finding the values of the function and its derivative at  $t = 0$  and  $t = T_p$ , in limit sense, and the values of arbitrary constants  $c_1$ ,  $c_2$ ,  $c_3$  and  $c_4$  by utilizing the continuity assumption **A5** and the one-sided limits concepts (Theorems 2.2 and 2.3) due to singularities at  $t = 0$ ,  $t = t_{\text{on}}$  and  $t = T_p$ , due to switching action. More details about the proof can be found at [2].

## 4.5 Summary and Discussions

In this chapter, we developed a formal model of linear differential equations to formally specify the behavior of the power electronics circuits. We also formally verified the correctness of the solution of differential equations representing the behavior of circuits, and also the steady-state behavior of quantities of interests, such as voltages and currents. To enable the formal specification and verification of the steady-state parameters, we presented the formal modeling of the steady-state characteristics and design parameters. Finally, we conduct formal periodic steady-state analysis of an ideal DC-DC Buck converter which includes topology and steady-state behavior of the circuits.

The formalization, presented in Sections 4.1-4.3, is generic and provides sufficient support to formally model and reason about different aspects of a power electronics circuit including implementation and behavior, specification, correctness of the solution of differential equations representing the

behavior of circuits, and also the steady-state behavior of quantities of interests, such as voltages and currents. The corresponding proof script, which is available for download at [2], has 3000 lines of `HOL Light` code and requires about 350 man hours of development time.

The proposed logical framework, in conjunction with formalization from Chapter 3, allowed us to formally specify and verify the nonlinear behavior of the DC-DC Buck converters in a very straightforward manner. Theorem 4.3 verifies that the implementation and behavior of the Buck converter by explicitly specifying the conditions on the piecewise functions, e.g., voltages in the case of DC-DC Buck converter, in the continuous conduction operating mode of the converter. The formally verified result is very helpful in the topology selection of the converter, which is usually the first step in the design procedure and, in practice, consists of an intuitive selection of topology for a given design specification. Moreover, Theorem 4.4 formally verifies the correction of the solution of the linear order differential equations representing the power converter behavior. This result plays a vital role in the performance evaluation. Once the implementation and behavior (Theorem 4.3), and the solution (Theorem 4.4) of the DC-DC Buck converter is formally verified, then Theorem 4.5 formally verifies the relationship among different parameters of the circuit, such as voltage and circuit components, in periodic steady-state. This result is instrumental in formal verification of the design objectives, such as desired voltage levels and component values, of the circuit. However, unlike traditional techniques these formally verified results give exact conditions in terms of the parameters of the Buck converter as they have been formally verified using a sound theorem prover. Moreover, these results are generic in terms of universally quantified variables and contain an exhaustive set of assumptions required for the validity of the results.

# 5

## Formalization of Stability Theory

In this chapter, we present formal stability theory analysis of control systems using their frequency or complex-domain representations, as described in Section 1.4. We formally model the stability criterion in the HOL Light theorem prover. Next, we provide formal results for the factorization of the characteristic equations (Equation 1.10) upto the fourth order. The formal stability criterion and factorization results are used to exhaustively verify the stability conditions for the control systems which have characteristic equations upto the fourth order. Finally, we present formal stability analysis of power controllers which are used to process the energy generated from wind turbines in smart grids.

### 5.1 Stability Model

The stability of a root is defined, as a higher-order-logic function, as:

**Definition 5.1:** *Stability Criterion*

$$\vdash \forall f. \text{ stable } f = \sim(\{ x \mid f \ x = Cx \ (0) \wedge \text{Re } (x) < 0 \} = \text{EMPTY } )$$

In Definition 5.1,  $f : R^2 \rightarrow R^2$  represents a complex function, which is a polynomial in our case,  $x : R^2$  is a complex variable, which in our case is the

root of the given polynomial, and  $Cx$  and  $Re$  are HOL `Light` functions, which are used to convert a real number into a complex number and to retrieve the real part of a given complex number, respectively.

The predicate  $stable:(R^2 \rightarrow R^2) \rightarrow bool$  accepts a polynomial and returns a *boolean* output, which is true for a stable root of the polynomial of the considered system and false otherwise. Definition 5.1 formally models two conditions for the stability of a root of the given complex polynomial, i.e.,  $f\ x = Cx\ (0)$  and  $Re\ (x) < 0$ . These conditions ensure that a complex-variable,  $x$ , is a root of the given polynomial and its real part lies in the left-half of the complex-plane. Furthermore, these roots are formally defined as the member of a set which should not be empty if the polynomial has any stable root. To ensure that all roots of a given polynomial are the members of this set, however, requires us to find all the roots of the given polynomial. Therefore, in the next section, we formally verify the roots of a polynomial.

## 5.2 Factorization of Polynomials upto the Fourth Order

To formally analyze the stability of the quadratic polynomial, we formally verify the famous quadratic formula in HOL `Light` theorem prover as:

**Theorem 5.1:** *Quadratic Roots*

$\vdash \forall a\ b\ c\ x .$

[A1]  $a \neq 0$

$$\begin{aligned} \Rightarrow & ( Cx\ a * x\ pow\ 2 + Cx\ b * x + Cx\ c = Cx\ 0 ) = \\ & ( x = \frac{-Cx\ b + \sqrt{Cx\ b\ pow\ 2 - Cx\ 4 * Cx\ a * Cx\ c}}{Cx\ 2 * Cx\ a} \vee \\ & x = \frac{-Cx\ b - \sqrt{Cx\ b\ pow\ 2 - Cx\ 4 * Cx\ a * Cx\ c}}{Cx\ 2 * Cx\ a} ) \end{aligned}$$

In the above theorem,  $a$ ,  $b$  and  $c$  are real numbers, whereas,  $x$  is a complex variable. Assumption A1 ensures that the polynomial is quadratic. The

theorem is a formally verified result that a quadratic polynomial has two roots, using the sound core of the HOL `Light` theorem prover.

To formally analyze the stability of the cubic polynomial, we formally verify the factor decomposition of a cubic into its linear and quadratic factors in HOL `Light` as follows:

**Theorem 5.2:** *Cubic Factors*

$\vdash \forall a\ b1\ c1\ d1\ r\ x .$

$$[A1] \quad Cx\ b = Cx\ b1 + Cx\ a * Cx\ r \wedge$$

$$[A2] \quad Cx\ c = Cx\ c1 + Cx\ b1 * Cx\ r$$

$$[A3] \quad Cx\ d = Cx\ c1 * Cx\ r \wedge$$

$$\Rightarrow Cx\ a * x\ pow\ 3 + Cx\ b * xpow\ 2 + Cx\ c * x + Cx\ d = \\ (x + Cx\ r) * (Cx\ a * x\ pow\ 2 + Cx\ b1 * x + Cx\ c1)$$

In the above theorem,  $a$ ,  $b1$ ,  $c1$ ,  $d1$  and  $r$  are real numbers which represent coefficients of the cubic factors. Whereas,  $x$  is a complex variable. Assumptions A1-A3 formally represent the factor decompositions of the cubic polynomial.

Next, we present formally verified roots of the cubic polynomial using Definition 5.1, Theorems 5.1 and 5.2 in HOL `Light` as:

**Theorem 5.3:** *Cubic Roots*

$\vdash \forall a\ b1\ c1\ d1\ r\ x .$

$$[A1] \quad a \neq 0 \wedge$$

$$[A2] \quad Cx\ b = Cx\ b1 + Cx\ a * Cx\ r \wedge$$

$$[A3] \quad Cx\ c = Cx\ c1 + Cx\ b1 * Cx\ r \wedge$$

$$[A4] \quad Cx\ d = Cx\ c1 * Cx\ r$$

$$\Rightarrow (Cx\ a * x\ pow\ 3 + Cx\ b * xpow\ 2 + Cx\ c * x + Cx\ d = Cx\ 0) \\ = ( \quad x = Cx\ r \vee x = \frac{-Cx\ b1 + \sqrt{Cx\ b1\ pow\ 2 - Cx\ 4 * Cx\ a * Cx\ c1}}{Cx\ 2 * Cx\ a} \vee \\ \quad x = \frac{-Cx\ b1 - \sqrt{Cx\ b1\ pow\ 2 - Cx\ 4 * Cx\ a * Cx\ c1}}{Cx\ 2 * Cx\ a} )$$

In the above theorem, Assumption **A1** ensures that the leading coefficient of the polynomial is not zero, i.e., the given polynomial is cubic. Assumptions **A2-A4** provide the factor decomposition of the given polynomial. Based on these assumptions, Theorem 5.3 formally verifies that the cubic polynomial has three roots.

To formally analyze the stability of the quartic polynomial, we formally verify the factor decomposition of a quartic into its two quadratic factors in `HOL Light` as:

**Theorem 5.4:** *Quartic Factors*

$\vdash \forall a1\ b1\ c1\ a2\ b2\ c2\ x .$

$$\begin{aligned}
& [A1] \ Cx\ a = Cx\ a1 * Cx\ a2 \wedge \\
& [A2] \ Cx\ b = Cx\ a1 * Cx\ b2 + Cx\ a2 * Cx\ b1 \wedge \\
& [A3] \ Cx\ c = Cx\ a1 * Cx\ c2 + Cx\ b1 * Cx\ b2 + Cx\ a2 * Cx\ c1 \wedge \\
& [A4] \ Cx\ d = Cx\ b1 * Cx\ c2 + Cx\ b2 * Cx\ c1 \wedge \\
& [A5] \ Cx\ e = Cx\ c1 * Cx\ c2 \\
\Rightarrow & (Cx\ a * x^{pow4} + Cx\ b * x^{pow3} + Cx\ c * x^{pow2} + Cx\ d * x \\
& + Cx\ e = Cx\ 0) = \\
& ( (Cx\ a1 * x^{pow2} + Cx\ b1 * x + Cx\ c1) * \\
& (Cx\ a2 * x^{pow2} + Cx\ b2 * x + Cx\ c2) )
\end{aligned}$$

In the above theorem,  $a1$ ,  $b1$ ,  $c1$ ,  $a2$ ,  $b2$  and  $c2$  are real-valued variables, which represent coefficients of the quadratic factors of a given quartic polynomial. Whereas,  $x$  is a complex variable. Theorem 5.4 formally verifies the factor decomposition of the quartic polynomial given the Assumptions **A1-A5**.

Next, we present formally verified roots of the quartic polynomial using Theorem 5.1 and 5.4 in `HOL Light` as:

**Theorem 5.5:** *Quartic Roots*

$\vdash \forall a1\ b1\ c1\ a2\ b2\ c2\ x .$

$$\begin{aligned}
& [A1] \ a \neq 0 \wedge [A2] \ Cx\ a = Cx\ a1 * Cx\ a2 \wedge \\
& [A3] \ Cx\ b = Cx\ a1 * Cx\ b2 + Cx\ a2 * Cx\ b1 \wedge
\end{aligned}$$





**Lemma 5.2** *Real Root Case 1*

$\vdash \forall a b c x .$

$$[A1] \ a \neq 0 \wedge$$

$$[A2] \ b^2 - 4 * a * c = 0 \wedge$$

$$[A3] \ 0 < \frac{b}{a}$$

$$\Rightarrow \text{stable } (\lambda x. Cx a * x^2 + Cx b * x + Cx c)$$

**Lemma 5.3** *Real Root Case 2*

$\vdash \forall a b c x .$

$$[A1] \ a < 0 \wedge$$

$$[A2] \ 0 < b^2 - 4 * a * c$$

$$[A3] \ b < \sqrt{b^2 - 4 * a * c}$$

$$\Rightarrow \text{stable } (\lambda x. Cx a * x^2 + Cx b * x + Cx c)$$

**Lemma 5.4:** *Real Root Case 3*

$\vdash \forall a b c x .$

$$[A1] \ a < 0 \wedge$$

$$[A2] \ b^2 - 4 * a * c < 0 \wedge$$

$$[A3] \ \sqrt{b^2 - 4 * a * c} < -b$$

$$\Rightarrow \text{stable } (\lambda x. Cx a * x^2 + Cx b * x + Cx c)$$

**Lemma 5.5:** *Real Root Case 4*

$\vdash \forall a b c x .$

$$[A1] \ 0 < a \wedge$$

$$[A2] \ 0 < b^2 - 4 * a * c \wedge$$

$$[A3] \ \sqrt{b^2 - 4 * a * c} < b$$

$$\Rightarrow \text{stable } (\lambda x. Cx a * x^2 + Cx b * x + Cx c)$$

**Lemma 5.6:** *Real Root Case 5*

$\vdash \forall a b c x .$

$$[A1] \ 0 < a \wedge$$

$$[A2] \ 0 < b^2 - 4 * a * c \wedge$$

$$\begin{aligned}
& \text{[A3]} \quad -b < \sqrt{b^2 - 4ac} \\
& \Rightarrow \text{stable } (\lambda x. Cx a * x^2 + Cx b * x + Cx c)
\end{aligned}$$

Lemmas 5.1-5.6 are formally verified using the multivariate complex, real analysis and transcendental theories available in the library of the HOL Light theorem prover. The above formally verified results cover all possible conditions on coefficients, of the second order polynomial, and on the discriminant of the quadratic formula for the stability of roots, as shown in Figure 5.1.

Now, Lemmas 1-6 are used to formally assert the stability of a quadratic polynomial as:

**Theorem 5.6:** *Quadratic Stability*

$\vdash \forall a b c x .$

$$\text{[A1]} \quad a \neq 0 \wedge$$

$$\text{[A2]} \quad 0 < \frac{b}{a} \wedge ( b^2 - 4ac < 0 \vee b^2 - 4ac = 0 ) \vee$$

$$\begin{aligned}
& 0 < b^2 - 4ac \wedge \\
& \quad ( a < 0 \wedge ( b < \sqrt{b^2 - 4ac} \vee \\
& \quad \quad \quad \sqrt{b^2 - 4ac} < -b ) \vee \\
& \quad ( 0 < a \wedge ( \sqrt{b^2 - 4ac} < b \vee \\
& \quad \quad \quad -b < \sqrt{b^2 - 4ac} ) ) \\
& \Rightarrow \text{stable } (\lambda x. Cx a * x^2 + Cx b * x + Cx c)
\end{aligned}$$

Theorem 5.6 provides a formally verified comprehensive result for the stability of the quadratic polynomial under all possible cases that may arise due to the nature of the discriminant, nature of real coefficients of the polynomial using HOL Light. The formalization of the quadratic polynomial plays a key role in the formal stability analysis of cubic and quartic polynomials as will be observed in the next two subsections.

Finally, the above formalization is used to formally verify the stability of a cubic polynomial as:

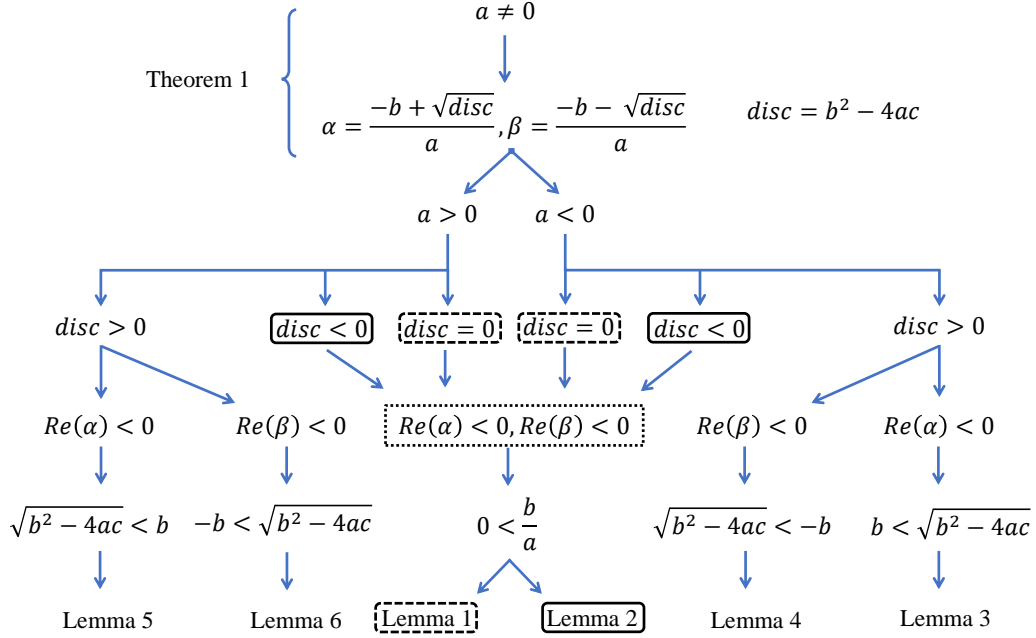


Figure 5.1: Stability of Quadratic Polynomial

**Theorem 5.7: Cubic Stability**

$\vdash \forall a \ b1 \ c1 \ d1 \ r \ x .$

[A1]  $a \neq 0 \wedge$  [A2]  $Cx \ b = Cx \ b1 + Cx \ a * Cx \ r \wedge$

[A3]  $Cx \ c = Cx \ c1 + Cx \ b1 * Cx \ r \wedge$  [A4]  $Cx \ d = Cx \ c1 * Cx \ r$

[A5]  $0 < r \vee$

$( ( 0 < \frac{b1}{a} \wedge ( \ b1 \text{ pow } 2 - 4 * a * c1 < 0 \vee$   
 $\qquad \qquad \qquad b1 \text{ pow } 2 - 4 * a * c1 = 0 ) ) \vee$

$( 0 < b1 \text{ pow } 2 - 4 * a * c1 \wedge$   
 $\qquad ( a < 0 \wedge ( b1 \sqrt{b1 \text{ pow } 2 - 4 * a * c1} \vee$   
 $\qquad \qquad \qquad \sqrt{b1 \text{ pow } 2 - 4 * a * c1} < -b1 ) \vee$

$( 0 < a \wedge ( \sqrt{b1 \text{ pow } 2 - 4 * a * c1} < b1 \vee$   
 $\qquad \qquad \qquad -b < \sqrt{b1 \text{ pow } 2 - 4 * a * c1} ) ) )$

$\Rightarrow \text{stable} (\lambda x. Cx \ a * x \text{ pow } 3 + Cx \ b * x \text{ pow } 2 + Cx \ c * x + Cx \ d)$

Theorem 5.7 provides a formally verified result for the stability of the cubic

polynomial under all possible values of real coefficients of the cubic polynomial, and explicitly states the relationship among them for satisfying stability conditions.

Finally, the above formalization is used to formally verify the stability of a quartic polynomial as:

**Theorem 5.8:** *Quartic Stability*

$\vdash \forall a_1 b_1 c_1 a_2 b_2 c_2 x .$

$$\begin{aligned}
& [A1] \ a \neq 0 \wedge [A2] \ Cx\ a = Cx\ a_1 * Cx\ a_2 \wedge \\
& [A3] \ Cx\ b = Cx\ a_1 * Cx\ b_2 + Cx\ a_2 * Cx\ b_1 \wedge \\
& [A4] \ Cx\ c = Cx\ a_1 * Cx\ c_2 + Cx\ b_1 * Cx\ b_2 + Cx\ a_2 * Cx\ c_1 \wedge \\
& [A5] \ Cx\ d = Cx\ b_1 * Cx\ c_2 + Cx\ b_2 * Cx\ c_1 \wedge \\
& [A6] \ Cx\ e = Cx\ c_1 * Cx\ c_2 \wedge \\
& [A7] \ ( 0 < \frac{b_1}{a_1} \wedge ( b_1 \text{ pow } 2 - 4 * a_1 * c_1 < 0 \vee \\
& \qquad \qquad \qquad b_1 \text{ pow } 2 - 4 * a_1 * c_1 = 0 ) ) \vee \\
& ( b_1 \text{ pow } 2 - 4 * a_1 * c_1 < 0 \wedge \\
& \qquad ( a_1 < 0 \wedge ( b_1 < \sqrt{b_1 \text{ pow } 2 - 4 * a_1 * c_1} \vee \\
& \qquad \qquad \qquad \sqrt{b_1 \text{ pow } 2 - 4 * a_1 * c_1} < -b_1 ) \vee \\
& \qquad ( 0 < a_1 \wedge ( \sqrt{b_1 \text{ pow } 2 - 4 * a_1 * c_1} < b_1 \vee \\
& \qquad \qquad \qquad -b_1 < \sqrt{b_1 \text{ pow } 2 - 4 * a_1 * c_1} ) ) \vee \\
& ( 0 < \frac{b_2}{a_2} \wedge ( 0 < b_2 \text{ pow } 2 - 4 * a_2 * c_2 \vee \\
& \qquad \qquad \qquad b_2 \text{ pow } 2 - 4 * a_2 * c_2 = 0 ) ) \vee \\
& ( b_2 \text{ pow } 2 - 4 * a_2 * c_2 < 0 \wedge \\
& \qquad ( a_2 < 0 \wedge ( b_2 < \sqrt{b_2 \text{ pow } 2 - 4 * a_2 * c_2} \vee \\
& \qquad \qquad \qquad \sqrt{b_2 \text{ pow } 2 - 4 * a_2 * c_2} < -b_2 ) \vee \\
& \qquad ( 0 < a_2 \wedge ( \sqrt{b_2 \text{ pow } 2 - 4 * a_2 * c_2} < b_2 \vee \\
& \qquad \qquad \qquad -b_2 < \sqrt{b_2 \text{ pow } 2 - 4 * a_2 * c_2} ) ) \\
& \Rightarrow \text{stable} (\lambda x. (Cx\ a * x^{\text{pow}4} + Cx\ b * x^{\text{pow}3} + Cx\ c * x^{\text{pow}2} \\
& \qquad \qquad \qquad + Cx\ d * x + Cx\ e)
\end{aligned}$$

Theorem 5.8 provides an exhaustive set of conditions for the stability of the

quartic polynomial using the HOL `Light` theorem prover.

## 5.4 Case Study: Current and Voltage Controllers in Smart Grids

Smart grids are networks with intelligent nodes to produce, consume and share the energy efficiently by leveraging upon the advances in the fields of communication, electronics and computation [62]. There has been an enormous increase in the usage of smart grid technology over the world in the last decade or so [30]. Thus, an insecure and unreliable smart grid can even lead to disastrous consequences [4].

Among many other challenges, energy harvesting from unconventional sources, such as wind turbines and solar panels, and processing of this energy is one of the key challenges in smart grids due to the intermittent nature of the produced energy [89]. To achieve a steady flow from these sources, power converters are designed to alleviate the problem. This objective is usually achieved by designing efficient current and voltage controllers for these power converters so that a smooth supply of power can be ensured, as shown in Figure 5.2.

We formally verify the stability of an  $H^\infty$  current,  $H^\infty$  voltage and  $H^\infty$  repetitive current controllers designed for the power converters to enhance the efficiency of smart grids [89].  $H^\infty$  [78] and repetitive control [45] are control methods, which are used for designing suboptimal controllers and controllers, which enable the power converters to inject a clean power into the grid system and thus resulting in more reliable and secure grid operations.

The transfer function of an  $H^\infty$  current controller is given [89] as:

$$[TF]_i = \frac{1.7998 * 10^9 (s + 300)}{s^2 + 4.33403 * 10^8 s + 1.10517 * 10^{12}} \quad (5.1)$$

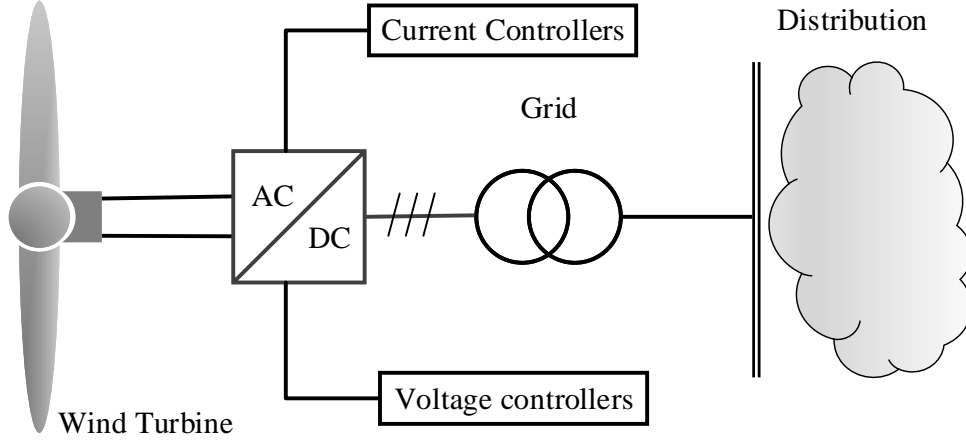


Figure 5.2: Efficient energy harvesting using Power converter controllers in smart grids

The characteristic equation of above transfer function is of second order therefore we utilize Theorem 5.2 to formally verify the stability in higher-order logic as:

**Theorem 5.9:**  $H^\infty$  Current Controller

$\vdash \forall a b c s .$

$\text{stable } (\lambda x. Cx 1 * s \text{ pow } 2 + Cx 4.3340 * 10^8 * x +$   
 $Cx 1.10517 * 10^{12})$

The transfer function of an  $H^\infty$  voltage controller is given [89] as:

$$[TF]_v = \frac{748.649(s^2 + 6954s + 3.026 * 10^8)}{s^3 + 10519s^2 + 3.246 * 10^8s + 7.7596 * 10^7} \quad (5.2)$$

The characteristic equation of this transfer function is of third order therefore we utilize Theorem 5.7 to formally verify the stability in higher-order logic as:

**Theorem 5.10:**  $H^\infty$  Voltage Controller

$\vdash \forall a \ b1 \ c1 \ d1 \ r \ s .$

[A1]  $a = 1 \wedge$  [A2]  $b1 = 79669 \wedge$  [A3]  $c1 = 3.043 * 10^8 \wedge$  [A4]  $r =$   
2550

$\Rightarrow$  stable  $(\lambda x. Cx \ 1 * s \ \text{pow} \ 3 + Cx \ 10519 * s \ \text{pow} \ 2 + Cx \ 3.246 * 10^8$   
 $* \ s$   
 $+ Cx \ 7.7596 * 10^7)$

The transfer function of an  $H^\infty$  repetitive current controller is given [89] as:

$$[TF]_{vr} = \frac{8.63 * 10^8 (s + 10^4)(s + 1000)(s + 80)}{s^4 + 1.55 * 10^8 s^3 + 1.83 * 10^{13} s^2 + 1.43 * 10^{17} s + 1.08 * 10^{19}} \quad (5.3)$$

The characteristic equation of above transfer function is of fourth order therefore we utilize Theorem 5.8 to formally verify the overall stability in higher-order logic as:

**Theorem 5.11:**  $H^\infty$  Repetitive Current Controller

$\vdash \forall a1 \ b1 \ c1 \ a2 \ b2 \ c2 \ s .$

[A1]  $a1 = 1 \wedge$  [A2]  $b1 = 1.557 * 10^7 \wedge$  [A3]  $c1 = 1.70538 * 10^3 \wedge$

[A4]  $a2 = 1 \wedge$  [A5]  $b2 = 8.403 * 10^3 \wedge$  [A6]  $c2 = 6.375 * 10^5$

$\Rightarrow$  stable  $(\lambda x. Cx \ 1 * s \ \text{pow} \ 4 + Cx \ 1.55 * 10^8 * s \ \text{pow} \ 3 +$   
 $Cx \ 1.83 * 10^{13} * s \ \text{pow} \ 2 + 1.43 * 10^{17} * s + Cx \ 1.08 * 10^{19})$

## 5.5 Summary and Discussions

This chapter presents a formalization for the stability analysis of control systems, which is a safety-critical system specification. We provided a formal definition of stability in higher-order logic and also formally verified the roots of *characteristic* equations, upto the fourth order, that are used for representing the control systems in the complex-domain. Our formalization

is based on the multivariate complex, real and transcendental theories available in `HOL Light` theorem prover and allows us to conduct the stability analysis of wide range of control systems almost automatically. For illustration, we also presented the analysis of voltage and current controllers of the power converters which are used to ensure the efficient and reliable smart grid operations.

Theorems 5.9-5.11 formally verify the correctness of the power converter controllers for a smart grid and the reasoning process was very straightforward, i.e., only a few lines of code and almost automatic based on simple real arithmetic. The main distinguishing feature of these theorems, compared to the corresponding results obtained through the traditional methods, is the explicit availability of all the assumptions required for the results to hold. As can be noted from Theorems 5.9-5.11 many of these assumptions specify very important design constraints. If these constraints are not met then we may get an unstable controller, which can be very dangerous, given the safety-critical nature of smart grids.



# 6

## Case Study: Non-ideal Power Converters

There are three basic non-isolated DC-DC converter topologies, namely, Buck, Boost and Buck-Boost, as shown in Figure 6.1. Buck and Boost converters step down and up, respectively, the input DC level, whereas, Buck-Boost can produce an output DC level that can be greater than or less than the input DC level.

Power converters are usually modeled using ideal circuit components, as shown in the Figure 6.1, which allow to easily analyze the functionality of these circuits. However, this kind of modeling does not allow incorporating power losses due to non-ideal behavior of the storage components and semiconductor devices [24]. Therefore, non-ideal circuit converter modeling (using Table 1.2) is mandatory for the design of the real-world power converters. In order to obtain the impact of these non-ideal behaviors, time domain based periodic steady-state analysis is conducted. The steady-state parameters are then used to characterize most of the converter design specifications [24]. We develop a logical framework for the first-order differential equation representation of the non-ideal power converters which implicitly

implies the assumption of the negligible capacitor ESR. The assumption allows to analyze the output ripple voltage or current that plays a vital in design of power converters [24] [23].

Mathematically, the converter behavior in each mode can be represented as a first-order linear differential equation:

$$\begin{aligned} \frac{d}{dt}y_n(t) &= a_n y_n(t) + b_n \\ y_n(t_n) &= y_{n-1}(t_{n-1}) \\ y(t'_0) &= y(t'_0 + T_p) \end{aligned} \quad (6.1)$$

Where

$$t \in T_p, T_p \in \bigcup_{i=1}^l [t'_{i-1}, t'_i], T_p = t'_{max(i)} - t'_0, n, l, k \in \mathbb{N}$$

In Equation (6.1),  $y_n$  is the function of an independent variable  $t$  and,  $a_n$  and  $b_n$  are real constants in an  $n$ -th mode.

In power converters, the time is considered as an independent variable, whereas, the voltage or current of the energy storage components is considered as a dependent variable. The constant  $b_n$  determines if the linear differential equation is homogeneous or non-homogeneous. The term is non-zero when energy source is included in the corresponding configuration. For every mode, the value of the dependent variable at switching instance serves

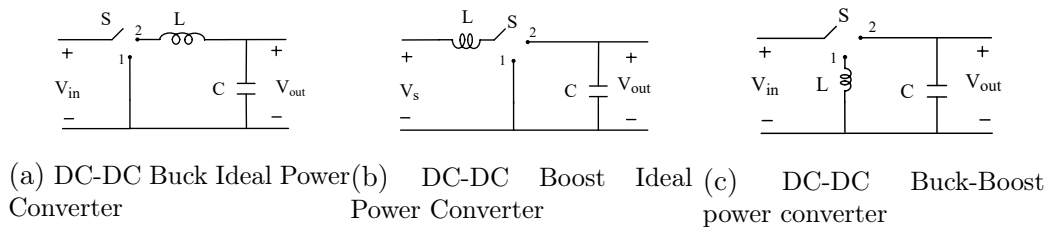


Figure 6.1: DC-DC power converters and equivalent ideal converter circuit models.

as the initial condition for the next mode, i.e.,  $y_n(t_n) = y_{n-1}(t_{n-1})$ , when switching instance occurs. Whereas,  $y(t'_0) = y(t'_0 + T_p)$  refers to the steady-state condition of the circuit using reference time instance,  $t_0$ , and  $t_{max(i)}$ , which also define the time period,  $T_p$ , of the converter circuit.

The solution to any first-order linear differential equation, represented by Equation (6.1), in each mode is:

$$y_n = -\frac{b_n}{a_n} + c_n e^{-a_n t} \quad t \in T, \quad 0 < n \leq l \quad (6.2)$$

Where  $c_n$  is an arbitrary constant, which is determined using the steady-state conditions for specific converter topology. Generally, for a given converter, the solution for the dependent variable is a piecewise function (1.6) and is represented using Heaviside function.

$$y(t) = \sum_{i=0}^l y_i(t) u(t - t_i) \quad t \in T \quad (6.3)$$

The solution, i.e., Equation (6.3), represents the behavior of the circuit variable, either current or voltage, over one time period of the circuit. In this chapter, we present a formalization which enables the formal verification of periodic steady-state behavior and design of non-ideal power converters based on the framework encompassed by Equations (6.1)–(6.3). To accomplish this task, the first challenge is to develop a formal library of non-ideal models of the circuit components and steady-state characteristics and specifications to formally specify the converter circuits in higher-order logic. In this regard, we utilize higher-order-logic models of circuit components and steady-state characteristics and specification developed in Chapters 3 and 4. The second challenge is to formalize the mathematical framework, such as differential theory and operation calculus, to formally verify the behavior of the non-ideal converters, operating in steady-state. We tackle this challenge

by exploiting, the existence of, the common mathematical formulation, as described by Equations (6.1)–(6.3), to develop a unified logical framework, in the `HOL Light` theorem prover, for the time-domain based steady-state analysis of non-ideal power converters. We utilize formally verified properties of generalized functions (Section 3.2) to conduct the formal analysis and design of power converters. Moreover, we consider CCM operation of the power converters which, further, allows us to account for only two modes, i.e.,  $l = 2$ , when a converter is in steady-state. These considerations simplify the formal analysis to one time period,  $T_P$ , of the given converter topology without compromising the effectiveness of the time-domain based steady-state analysis of power converters. In many safety or mission-critical applications, converters are desired to be operated in the CCM, therefore, the formalization can be employed to a large spectrum of the power processing applications.

## 6.1 Steady-state Behavior and Specification of Converters

The steady-state behavior of a given converter circuit topology is formally specified in `HOL Light`, using Definitions 4.2 and 4.3, as:

**Definition: 6.1** *Behavior Specification*

$$\begin{aligned} &\vdash \forall a_1 a_2 b_1 b_2 y t_{on} t. \text{nideal\_power\_conv\_diff\_equ } a_1 a_2 b_1 b_2 y t_{on} t = \\ &\text{if } (t < t_{on}) \text{ then diff\_eq\_lhs } [a_1; 1] (y(t)) t = \text{diff\_eq\_rhs } [b_1] [1] t \\ &\text{else diff\_eq\_lhs } [a_2; 1] (y(t)) t = \text{diff\_eq\_rhs } [b_2] [1] t \end{aligned}$$

In the above definition,  $a_1$ ,  $a_2$ ,  $b_1$ , and  $b_2$  are real coefficients representing the coefficients of the corresponding system of first-order differential equations of the converter. The circuit variable of interest, such as voltage or current, is modeled using a real to complex function  $y(t)$ . Conditional (`if...else`) is used to model two modes constituting the time period,  $T_P$ , of

the given circuit.

Now, we formally specify the solution of the differential equations, expressed as Equation (6.3), to formally analyze the behavior of the circuit variables in HOL Light, as:

**Definition: 6.2** *Solution Specification*

$$\begin{aligned} & \vdash \forall c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{on} t. \\ & \text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{on} t = [\text{linear\_sol\_comb } [c_1] (\text{cexp\_lst } [s_1]) t \\ & + s_{p_1}] * Cx (\text{semi\_switch } (t - t_{on})) + [\text{linear\_sol\_comb } [c_2] (\text{cexp\_lst } \\ & [s_2]) t + s_{p_2}] * Cx (1 - \text{semi\_switch } (t - t_{on})) \end{aligned}$$

In the above definition,  $s_1$  and  $s_2$  represent general solution, and,  $s_{p_1}$  and  $s_{p_2}$  represent particular solutions of the given differential equations. The `linear_sol_comb` is a higher-order-logic function which models the general solution of given differential equation. It accepts a list of coefficients, corresponding list of exponential functions, as `cexp_list`, and time variable,  $t \in (t_0, t_0 + T_p)$ . Whereas, `semi_switch`, having switching instance specified at  $t_{on}$ , is used to model the piecewise nature of the solution over the time period,  $T_p$ , of the converter circuit.

We use above formalization to formally verify the steady-state behavior of the given converter circuit, in higher-order logic, as:

**Theorem: 6.1** *Behavior Verification*

$$\begin{aligned} & \vdash \forall a_1 a_2 b_1 b_2 c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{on} T_p t. \\ & [A1] \sim(a_1 = 0) \wedge [A2] \sim(a_2 = 0) \wedge \\ & [A3] (s_1 = -a_1) \wedge [A4] (s_2 = -a_2) \wedge \\ & [A5] (s_{p_1} = -\frac{b_1}{a_1}) \wedge [A6] (s_{p_2} = -\frac{b_2}{a_2}) \wedge \\ & [A7] (\sim(t = t_{on}) \wedge [A8] (\sim(t_{on} \in (0, T_p))) \wedge \\ & [A9] y t = \text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{on} t \\ & \Rightarrow \text{nideal\_power\_conv\_diff\_equ } a_1 a_2 b_1 b_2 t_{on} t \end{aligned}$$

In the above theorem, Assumption A1-A2 ensure that the order of the differential equation is not reduced. Assumptions A3-A6 specify the general

and particular solution in terms of the circuit parameters, i.e.,  $a_1$ ,  $a_2$ ,  $b_1$  and  $b_2$ . Assumption A7 ensures that the switching instance is excluded. Similarly, Assumption A8 specifies the time period of the converter as an open interval to exclude the switching instances at the upper and lower bounds of the time period. Assumption A9 formally specifies the solution of the differential equations using Definition 6.2. Finally, based on these assumptions the steady-state behavior of a converter circuit, as differential equations, is formally verified in the conclusion.

Once the generic solution for the differential equations for power converters is formally verified, then, we formally verify the coefficients to specify the solution w.r.t the given initial condition in HOL Light as:

**Theorem: 6.2** *Coefficients of a Solution*

$\vdash \forall a_1 a_2 b_1 b_2 c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{on} T_p t.$

[A1]  $(\forall t. \text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{on} t \text{ continuous\_on at } t) \Rightarrow$

$c_1 = (\text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} 0 t - s_{p_1}) \wedge$

$c_2 = ((\text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} 0 t - s_{p_1}) * \text{cexp } (s_1 * t_{on} + s_{p_1} - s_{p_2}))$

In the above theorem, formal expression for the  $c_1$  is formally verified by simply using function value at  $t = 0$ . Whereas,  $c_2$  is formally verified using one-sided limits at switching instance,  $t_{on}$ , along with the continuity assumption, i.e., A2. Both expressions are formally verified in terms of the initial condition, general and particular solution.

The formalization, in this section, provides higher-order logic framework for the formal verification of the non-ideal power converters basic topologies which are modeled using first-order differential equations.

## 6.2 Steady-state Characteristics

Now, we formally verify a result based on the steady-state principle, i.e., Equation (1.8), in HOL Light, as,

**Theorem: 6.3** *Steady-state Principle*

$\vdash \forall a_1 a_2 b_1 b_2 c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{on} T_p t.$

[A1]  $(\forall t. \text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{on} t \text{ continuous\_on at } t) \wedge$

[A2]  $(\text{steady\_state } 0 (\forall t. \text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{on} t) 0 =$   
 $\text{steady\_state } 0 (\forall t. \text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{on} t) T_p) \wedge$

[A3]  $\text{average\_ac } (0, T_p) (\forall t. \text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{on} t) = 0$

$\Rightarrow \frac{b_1}{a_1} - \frac{b_2}{a_2} = ((\text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} 0 t - s_{p_1}) * \text{cexp } (s_1 * t_{on}) + s_{p_1}$   
 $- s_{p_2}) * \text{cexp } (-a_2 * T_p) -$   
 $((\text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} 0 t) - s_{p_1}))$

In Theorem 6.3, Assumption A1 ensures the continuity of the `solution` function. Whereas, Assumption A2-A3 ensure that the converter is operating in the steady-state. The conclusion of the above theorem is formally verified using steady-state conditions in terms of the coefficients of differential equations representing power converters.

Theorem 6.3 is formally verified using the steady-state conditions, i.e., Assumptions A2-A3 . Whereas, Theorem 3.1 is used to treat the integral involved in formally verifying the expression using Assumption A3 and A21.

Finally, we formally verify the ripple quantity of interest, such as voltage or current, in HOL Light, as,

**Theorem: 6.4** *Ripple Quantity*

$\vdash \forall c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{on} T_p t.$

[A1]  $(\forall t. y(t) = \text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{on} t) \wedge$

[A2]  $\sim ((1 - \text{cexp } (s_1 Cx t_{on} + s_2 * Cx (T_p - t_{on})) = Cx 0)$

$\Rightarrow \text{ripple } y t_{on} 0 = \frac{(\text{cexp } s_1 * t_{on}) - 1}{1 - (\text{cexp } (s_1 * t_{on} + s_2 * (T - t_{on})))} [s_{p_1} * (\text{cexp } s_2 * (T_p -$   
 $t_{on}) - \text{cexp } ((s_1 * t_{on}) + s_2 * (T_p - t_{on})) + s_{p_2} * (1 - \text{cexp } s_2 * (T_p -$   
 $t_{on}))] + s_{p_1} * (1 - \text{cexp } (s_1 * t_{on}))$

In the above theorem, we utilize Definition 4.8 to formally verify the ripple in the variable of the interest. The solution of the converter is passed as a function  $y(t)$ , in Assumption A1, which is evaluated at time instance 0 and

$t_{\text{on}}$ . Whereas, Assumption A2 arises from the algebraic manipulation of the expression to avoid the divide by zero case.

The formalization, presented in this section, along with the formalization described in Chapter 3, allows us to formally analyze and verify the steady-state behavior of the non-ideal power converters, including circuit implementation and specification behavior, periodic steady-state characteristics and design specifications.

### 6.3 Periodic Steady-state Analysis of Non-ideal DC-DC Buck Converter

DC-DC Buck converter circuits [24], also called step down converter or chopper, steps down an input energy level to a desired output energy level. This basic topology is widely used for power processing in many mission or safety critical applications, such as earth-orbiting spacecrafts and electric vehicles [24]. In such applications, non-ideal models of power converter circuits are used to analyze and verify the design specifications to achieve high efficiency and performance.

A simple DC-DC Buck converter circuit is shown in Figure 6.2a. Under the continuous switching action of MOSFET (Q) and diode (D), the circuit exhibits various configurations, termed as modes of the circuit, to achieve the desired power conversion. However, in steady-state, the behavior of the system becomes repetitive over time period,  $T_p$ . The time period is determined by the switching instances  $t_{\text{on}}$  and  $t_{\text{off}}$  of Q and D, respectively, i.e.,  $T_p = t_{\text{on}} + t_{\text{off}}$ . Figure 6.2b shows the equivalent non-ideal model of the converter that is commonly used to analyze the ripple in the inductor current, which can significantly affect the efficiency, performance and size of the Buck converters [24]. The first step in the analysis of converter circuits involves identification of the modes of the given circuit. As shown in Figure 6.2b,



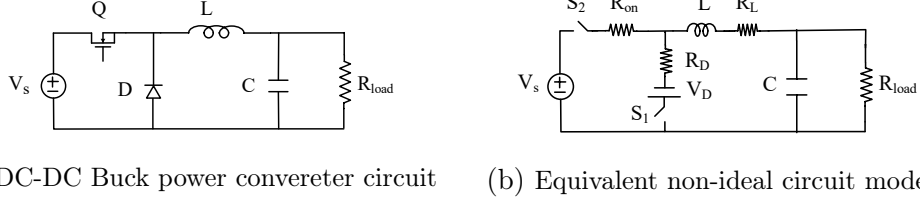


Figure 6.2: DC-DC Buck power converter and equivalent non-ideal converter circuit model.

when  $S_2$  is connected, and  $S_1$  is disconnected then the Buck converter operates in Mode-1, and the circuit behavior can be obtained using Kirchoff's voltage law, according to which the algebraic sum of all the voltages within the network loop must be equal to zero [20], as:

$$\begin{aligned} V_s &= v_Q^1(t) + v_L^1(t) + v_{R_L}^1(t) + v_C^1(t) \\ v_C^1(t) &= v_{load}^1(t) = v_{out}^1 = I_1^1(t)R_{load} \end{aligned} \quad (6.4)$$

Where  $V_s$  is a voltage source, and,  $v_Q^1(t)$ ,  $v_L^1(t)$ ,  $v_{R_L}^1(t)$  and  $v_C^1(t)$  are voltage drops across  $R_{on}$ ,  $L$ ,  $R_L$  and  $C$  or  $R_{load}$ , respectively, in Mode-1.

Similarly, when  $S_1$  is connected and  $S_2$  is disconnected then the Buck converter operates in Mode-2, in Figure 6.2b, and the behavior can be obtained using Kirchoff's voltage law, as:

$$\begin{aligned} V_D + v_{R_D}(t) + v_L^2 + v_{R_L}^2 + v_C^2 &= 0 \\ v_C^2(t) &= v_{load}^2(t) = v_{out}^2 = I_1^2(t)R_{load} \end{aligned} \quad (6.5)$$

Where  $V_D$  is the forward voltage drop of diode, and,  $v_{R_D}(t)$ ,  $v_L^2$ ,  $v_{R_L}^2$  and  $v_C^2$  are the voltage drops across  $R_D$ ,  $L$ ,  $R_L$  and  $C$  or  $R_{load}$ , respectively, in Mode-2.

Due to negligible capacitor ESR assumption, Equation 6.4 and 6.5 can be reduced to:

$$\begin{aligned} \frac{d}{dt}I_1^1(t) + \left(\frac{R_{on} + R_L + R_{load}}{L}\right)I_1^1(t) &= \frac{V_s}{L} \\ \frac{d}{dt}I_1^2(t) + \left(\frac{R_D + R_L + R_{load}}{L}\right)I_1^2(t) &= -\frac{V_D}{L} \end{aligned} \quad (6.6)$$

The solutions to the above non-homogeneous first-order differential equations

are:

$$\begin{aligned} I_1^1(t) &= \left( \frac{V_s}{R_{on} + R_L + R_{load}} \right) + c_1 \exp^{-\left( \frac{R_{on} + R_L + R_{load}}{L} \right) t} \\ I_1^2(t) &= -\left( \frac{V_D}{R_D + R_L + R_{load}} \right) + c_2 \exp^{-\left( \frac{R_D + R_L + R_{load}}{L} \right) t} \end{aligned} \quad (6.7)$$

A unified single expression, representing the solution in two modes, can be expressed using the Heaviside function [19], as:

$$I(t) = I_1^1(t)u(t - t_{on}) + I_1^2(t)(1 - u(t - t_{on})) \quad (6.8)$$

Once the periodic steady-state circuit variables are available from the implementation and specification of the Buck converter, then, periodic steady-state characteristics and converter specifications can be obtained by using the mathematical expressions of Table 1.3.

### 6.3.1 Topology

The implementation of the non-ideal DC-DC Buck converter, i.e., 6.4 and 6.5, is defined in higher-order logic, as:

**Definition: 6.3** *Implementation*

```

⊢ ∀ i0 I1 I2 L C Rload RD RL RC Ron Vout Vs VD Vsw ton t.
non_ideal_buck_ckt_impl i0 I1 I2 L C Rload RD RL RC Ron Vout Vs VD Vsw ton t
=
( ∀t. (0 < t) ∧ ∼(t = ton) ⇒ ( Vsw t = switch_volt [ (λt. --Cx Vs +
semi_resis_model_volt Ron I1 t); (λt. semi_volt_resis_model_volt VD
I1 RD t)] [1 - semi_switch_(t - ton); semi_switch_(t - ton)] t ) ∧
(kvl [Vsw; non_ideal_ind_volt I1 L RL; non_ideal_cap_volt i0 (λt. I1 -
I2 C RC] t) ∧ (Vout t = ideal_resis_volt I1 Rload t) )

```

In the above definition, the first conjunction formally models the switch junction voltage, i.e.,  $V_{sw}$ , using Definitions 3.1, 3.17, 3.12 and 3.14. The second conjunction formally models the implementation of the circuit using Kirchhoff's voltage law, i.e., Definition 3.15, along with the voltages and

currents of inductor and capacitors, i.e., Definition 3.8 and 3.10. The assumption in the second conjunction ensures that the circuit behavior is not specified at the singularity point, i.e.,  $t_{on}$ .

The correspondence between the implementation and specification of the given non-ideal Buck converter is formally verified, in `HOL Light`, as:

**Theorem: 6.5** *Implementation and Behavior*

$\vdash \forall i_0 V_s a_1 a_2 b_1 b_2 I_1 I_2 V_D L C R_{load} R_L R_C R_D R_{on} t_{on} T_p t .$

[A1]  $(\forall t. I_1(t) = I_2(t)) \wedge$  [A2]  $(R_C = 0) \wedge$

[A3]  $\sim (L = 0) \wedge$  [A4]  $a_1 = \frac{R_{on} + R_L + R_{load}}{L} \wedge$

[A5]  $a_2 = \frac{R_D + R_L + R_{load}}{L} \wedge$  [A6]  $b_1 = -\frac{V_s}{L} \wedge$  [A7]  $b_2 = -\frac{V_D}{L} \wedge$

[A8]  $(t \in (0, T_p)) \wedge$  [A9]  $\sim(t = t_{on}) \wedge$

[A10] `non_ideal_buck_ckt_impl`  $i_0 I_1 I_2 L C R_D R_{load} R_L R_C R_{on} V_s t_{on} t$   
 $\Rightarrow$  `nideal_power_conv_diff_equ`  $a_1 a_2 b_1 b_2 y t_{on} t$

Assumptions A1 and A2 formally specify that the capacitor current is zero, which in turn implies that the inductor current is supplied to the resistor in both the modes. Assumption A3 ensures that the inductance,  $L$ , of the inductor is not zero to avoid the undefined divide by zero case in the formal analysis. Assumptions A6-A8 ensure that the circuit behavior is specified over one time period of the converter circuit with singularities excluded at  $t = 0$ ,  $t = t_{on}$  and  $t = T_p$ . Finally, Assumption A10 and conclusion predicates formally specify the implementation and behavior of the converter using Definition 6.2 and 6.3, respectively. The formal verification of the above theorem is conducted by using Definitions 3.1-3.18, along with some complex arithmetic reasoning.

Next, we formally verify the correctness of the solution of the given piecewise differential equations, representing BUCK converter behavior, using Theorem 6.1 and 6.2, in `HOL Light` as:

**Theorem: 6.6** *Behavior Verification*

$\vdash \forall i_0 V_s a_1 a_2 b_1 b_2 I_1 I_2 V_D L C R_{load} R_L R_C R_D R_{on} t_{on} T_p t .$   
 [A1]  $\sim(R_{on} = 0) \wedge$  [A2]  $\sim(R_L = 0) \wedge$  [A3]  $\sim(R_{load} = 0) \wedge$   
 [A4]  $\sim(R_D = 0) \wedge$  [A5]  $\sim(V_D = 0) \wedge$  [A6]  $\sim(V_s = 0) \wedge$   
 [A7]  $a_1 = \frac{R_{on}+R_L+R_{load}}{V_s} \wedge$  [A8]  $a_2 = \frac{R_D+R_L+R_{load}}{V_D} \wedge$   
 [A9]  $b_1 = -\frac{V_s}{L} \wedge$  [A10]  $b_2 = -\frac{V_D}{L} \wedge$   
 [A11]  $s_1 = -(\frac{R_{on}+R_L+R_{load}}{L}) \wedge$  [A12]  $s_2 = -(\frac{R_D+R_L+R_{load}}{L}) \wedge$   
 [A13]  $(s_{p1} = \frac{-V_s}{R_{on}+R_L+R_{load}}) \wedge$  [A14]  $(s_{p2} = \frac{-V_D}{R_D+R_L+R_{load}}) \wedge$  [A15]  $\sim(t = t_{on}) \wedge$   
 [A16]  $(t_{on} \in (0, T_p)) \wedge$   
 [A17]  $(\forall t. y t = \text{solution } c_1 c_2 s_1 s_2 s_{p1} s_{p2} t_{on} t \text{ continuous at}) \Rightarrow$   
 nideal\_power\_conv\_diff\_equ  $a_1 a_2 b_1 b_2 y t_{on} t$

Then above theorem formally verifies the steady-state behavior of the DC-DC Buck converter circuit for  $a_1$ ,  $b_1$ ,  $a_2$ ,  $b_2$ ,  $s_1$ ,  $s_2$ ,  $s_{p1}$ ,  $s_{p2}$ ,  $c_1$  and  $c_2$ , which are formally specified in Assumption A7-A14, within the circuit time period, i.e.,  $(0, T_p)$ .

### 6.3.2 Steady-state Principle

Next, we formally verify the steady-state principle for the output of the non-ideal DC-DC Buck converter in HOL Light as:

**Theorem: 6.7** *Steady-state Principle*

$\vdash \forall c_1 c_2 s_1 s_2 s_{p1} s_{p2} t_{on} T_p t .$   
 [A1]  $\sim(R_{on} = 0) \wedge$  [A2]  $\sim(R_L = 0) \wedge$  [A3]  $\sim(R_{load} = 0) \wedge$   
 [A4]  $\sim(R_D = 0) \wedge$  [A5]  $\sim(V_D = 0) \wedge$  [A6]  $\sim(V_s = 0) \wedge$   
 [A7]  $a_1 = \frac{R_{on}+R_L+R_{load}}{V_s} \wedge$  [A8]  $a_2 = \frac{R_D+R_L+R_{load}}{V_D} \wedge$   
 [A9]  $b_1 = -\frac{V_s}{L} \wedge$  [A10]  $b_2 = -\frac{V_D}{L} \wedge$   
 [A11]  $(s_1 = -(\frac{R_{on}+R_L+R_{load}}{L})) \wedge$  [A12]  $(s_2 = -(\frac{R_D+R_L+R_{load}}{L})) \wedge$   
 [A13]  $(s_{p1} = \frac{V_s}{R_{on}+R_L+R_{load}}) \wedge$  [A14]  $(s_{p2} = \frac{V_D}{R_D+R_L+R_{load}})$   
 [A15]  $(\text{steady\_state } 0 (\lambda t. \text{solution } c_1 c_2 s_1 s_2 s_{p1} s_{p2} t_{on} t) 0 =$   
      $\text{steady\_state } 0 (\lambda t. \text{solution } c_1 c_2 s_1 s_2 s_{p1} s_{p2} t_{on} t) T_p \wedge$

$$\begin{aligned}
& \text{[A16] } \text{average\_ac}(0, T_p) (\lambda t. \text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t) = 0 \quad \wedge \\
& \text{[A17] } (\forall t. \text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{\text{on}} t \text{ continuous at } t) \Rightarrow \\
& \quad \frac{R_{\text{on}} + R_L + R_{\text{load}}}{V_s} + \frac{R_D + R_L + R_{\text{load}}}{V_D} = \left( \left( \text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{\text{on}} 0 - \right. \right. \\
& \quad \left. \left. \frac{V_s}{R_{\text{on}} + R_L + R_{\text{load}}} \right) \right) * \text{cexp} \left( -\left( \frac{R_D + R_L + R_{\text{load}}}{L} \right) * t_{\text{on}} \right) + \frac{V_s}{R_{\text{on}} + R_L + R_{\text{load}}} + \frac{V_D}{R_D + R_L + R_{\text{load}}} \quad * \\
& \quad \text{cexp} \left( -\left( \frac{R_D + R_L + R_{\text{load}}}{V_D} * T_p \right) - \right. \\
& \quad \left. \left( \left( \text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{\text{on}} 0 \right) - \frac{V_s}{R_{\text{on}} + R_L + R_{\text{load}}} \right) \right)
\end{aligned}$$

Assumptions A1-A6 ensure that  $a_1$  and  $a_2$  are not zero. Assumptions A7-A14 formally specify the coefficients of the first-order differential equations, i.e.,  $a_1$  and  $a_2$ , and general,  $s_1$  and  $s_2$ , and specific solutions,  $s_{p_1}$  and  $s_{p_2}$ , of the given differential equations. Whereas, A15-A17 formally specifies the initial, steady-state and continuity conditions, respectively, on the output current of the given circuit, i.e.,  $\text{solution}$ .

### 6.3.3 Steady-state Characteristics and Design Specifications

Finally, we proceed to formally verify the periodic steady-state characteristics and specifications of a non-ideal DC-DC Buck converter in higher-order logic as:

**Theorem: 6.8** *Design and Specifications*

$$\begin{aligned}
& \vdash \forall i_0 V_s V_D V_{\text{in}} I L C R_{\text{load}} R_L R_C R_{\text{on}} c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{\text{on}} T_p C_{\text{eff}} C_{\text{ratio}} t. \\
& \text{[A1] } (\forall t. I t = \text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t_{\text{on}} t) \wedge \\
& \text{[A2] } (s_1 = -\left( \frac{R_{\text{on}} + R_L + R_{\text{load}}}{L} \right)) \wedge \text{[A3] } (s_2 = -\left( \frac{R_D + R_L + R_{\text{load}}}{L} \right)) \wedge \\
& \text{[A4] } (s_{p_1} = \frac{V_s}{R_{\text{on}} + R_L + R_{\text{load}}}) \quad \wedge \quad \text{[A5] } (s_{p_2} = \frac{-V_D}{R_D + R_L + R_{\text{load}}}) \quad \wedge \\
& \text{[A6] } \sim \left[ \left( 1 - \text{cexp} \left( -\left( \frac{R_{\text{on}} + R_L + R_{\text{load}}}{L} \right) * Cx t_{\text{on}} - \right. \right. \right. \\
& \quad \left. \left. \left( \frac{R_D + R_L + R_{\text{load}}}{L} \right) * Cx (T_p - t_{\text{on}}) \right) = Cx \ \& \ 0 \right] \\
& \text{[A7] } \text{average\_ac}(0, T_p) (\lambda t. \text{solution } c_1 c_2 s_1 s_2 s_{p_1} s_{p_2} t) = 0 \\
& \text{[A8] } C_{\text{ratio}} = \frac{\text{ideal\_resis\_volt}(\text{rms\_ac}(0, T_p) I t_{\text{on}} 0) R_{\text{load}} t}{V_s} \wedge \\
& \text{[A9] } C_{\text{eff}} = \\
& \quad \frac{\text{power\_ac}(0, T_p) I t_{\text{on}} 0 R_{\text{load}}}{\text{power\_ac}(0, T_p) I t_{\text{on}} 0 R_{\text{load}} + \text{power\_ac}(0, T_p) I t_{\text{on}} 0 (R_{\text{load}} + R_D + R_{\text{on}} + R_L)} \Rightarrow
\end{aligned}$$

$$\begin{aligned}
& [\text{CONJ1 :}] \text{ripple I } t_{\text{on}} 0 = \\
& \frac{(\text{cexp}(-\frac{R_{\text{on}}+R_{\text{L}}+R_{\text{load}}}{L}) * t_{\text{on}}) - 1}{1 - (\text{cexp}(-\frac{R_{\text{on}}+R_{\text{L}}+R_{\text{load}}}{L}) * t_{\text{on}} - (\frac{R_{\text{D}}+R_{\text{L}}+R_{\text{load}}}{L}) * (T-t_{\text{on}}))} \\
& \left[ \frac{V_{\text{s}}}{R_{\text{on}}+R_{\text{L}}+R_{\text{load}}} * (\text{cexp}(-\frac{R_{\text{D}}+R_{\text{L}}+R_{\text{load}}}{L}) * (T_{\text{P}} - t_{\text{on}})) - \text{cexp}(-\frac{R_{\text{on}}+R_{\text{L}}+R_{\text{load}}}{L}) * t_{\text{on}} \right. \\
& \quad \left. - (\frac{R_{\text{D}}+R_{\text{L}}+R_{\text{load}}}{L}) * (T_{\text{P}} - t_{\text{on}}) \right] + \\
& \frac{-V_{\text{D}}}{R_{\text{D}}+R_{\text{L}}+R_{\text{load}}} * (1 - \text{cexp}(-\frac{R_{\text{D}}+R_{\text{L}}+R_{\text{load}}}{L}) * (T_{\text{P}} - t_{\text{on}})) \\
& + \frac{V_{\text{s}}}{R_{\text{on}}+R_{\text{L}}+R_{\text{load}}} * (1 - \text{cexp}(-\frac{R_{\text{on}}+R_{\text{L}}+R_{\text{load}}}{L}) * t_{\text{on}}) \wedge \\
& [\text{CONJ2 :}] \text{rms\_ac}(\text{average\_ac}(0, T_{\text{P}}) \text{I})(\text{ripple I } t_{\text{on}} 0) = \\
& \quad \frac{1}{2\text{csqrt}(3)} (\text{ripple I } t_{\text{on}} 0) \wedge \\
& [\text{CONJ3 :}] \text{C\_ratio} = \frac{R_{\text{load}}}{2V_{\text{s}}\text{csqrt}(3)} (\text{ripple I } t_{\text{on}} 0) \wedge \\
& [\text{CONJ4 :}] \text{C\_eff} = \frac{R_{\text{load}}}{R_{\text{load}}+R_{\text{on}}+R_{\text{D}}+R_{\text{L}}}
\end{aligned}$$

In the above theorem, CONJ1 is formally verified using Theorem 6.4, along with the Assumption A1-A7. Whereas, CONJ2 is a formally verified result for the RMS value of the current using Definitions 4.7-4.11. Finally, Assumption A8-A9 are used to formally specify the converter ratio and efficiency, respectively, utilizing definitions of voltage across output load resistor, i.e., Definition 3.4, and power loss, i.e., Definition 4.11, due to the non-ideal behavior of components of the Buck converter. Formally verified results of CONJ1 – 2 are also employed to formally verify the BUCK converter ratio and efficiency in CONJ3 – 4.

## 6.4 Summary and Discussions

This chapter presents an approach for the formal time-domain based steady-state analysis and design of the non-ideal power converter circuits, which are used in many safety-critical applications, using interactive higher-order logic theorem proving. Primarily, a logical framework for first-order differential equations for basic power converter topologies is developed which leverages upon the formalization of basic circuit theory and differential equations (in Chapter 3 and 4, respectively) to formally verify the design specifications of

the real-world power converters. The formally verified results provide sufficient conditions on the circuit variables and parameters due to mathematical rigor involved in verifying the corresponding closed form expressions within the sound core of `HOL Light` theorem prover. Based on the proposed formalization, we conducted the formal time-domain based steady-state analysis and design of a non-ideal DC-DC Buck converter.

The proposed formalization provides a comprehensive logical framework to formally analyze and verify the behavior and design specifications of non-ideal power converters in periodic steady-state. Formal models of non-ideal components of the converter circuits, in Section 3.1, and switching function technique, in Table 1.2, allow us to formally verify the behavior of the current or voltage quantities of the circuit components based upon their connections in the given circuit. Such an analysis is used for the topology selection which is usually the first step in the circuit analysis [61]. We employed the aforementioned formalization to formally verify the implementation behavior of DC-DC Buck converter as Theorem 6.5 in `HOL Light`. Formally verified results in Section ??, i.e., Theorems 6.1 and 6.2, allow us to formally express and verify the time-domain based steady-state behavior of the Buck converter as Theorem 6.6. Finally, Theorems 6.7 and 6.8 provide formally verified results for the steady-state characteristics and specifications of BUCK converter, such as ripple, power loss, efficiency and converter ratio, mainly using Theorems 6.3 and 6.4. In practice, steady-state condition is employed to specify the values of circuit components, such as inductor and capacitor, for the given design requirements [24]. Whereas, ripple in the current or voltage quantities is essential to derive the analytical expression for power losses, and thus, plays a vital role in designing power converters with desired efficiency and performance. Unlike traditional analysis techniques [51] [23] [24], the formal verification within the sound core of `HOL Light` theorem prover allowed us to obtain an exhaustive set of assumptions explicitly stating constraints on

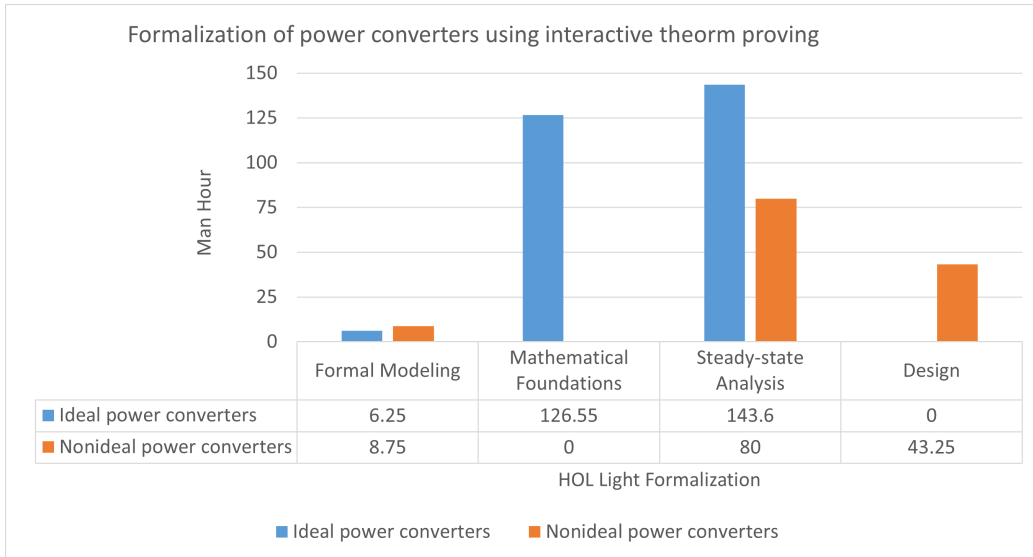


Figure 6.3: Quantification and comparison of formal verification of ideal and non-ideal power converters

the circuit variables. The real challenge in the proposed formalization was to account for the singularities due to highly non-linear switching operation in the converter circuits. Therefore, the proposed formalization ensures secure and reliable time-domain based periodic steady-state analysis and design of the power converter circuits for the safety or mission-critical applications. Moreover, the formal time-domain based periodic steady-state analysis of other interesting converter topologies, i.e., non-ideal Boost and Buck-Boost converters [24], can readily be conducted by just instantiating the variables with the parameter values of the given converter circuit. The `HOL Light` code for the proposed formalization and case study is available for download at [3].

Figure 6.3 shows the comparison of the verification effort involved in producing the mechanized proofs for ideal and non-ideal power converters using the `HOL Light` theorem prover. The overall effort has been divided into four major challenges, i.e., formal modeling, mathematical foundations, steady-state and design analysis. The formal modeling choice directly affects the



amount of the formalization of the mathematical notions needed to conduct the formal analysis of the given system, and, therefore can be regarded as the most difficult and time consuming phase of the formal verification of power converters. Given the extensive formal modeling background of the user, the difficulty level for this part of the proposed formalization was substantially reduced, as shown in the Figure 6.3. Whereas, the formal periodic steady-state analysis and design challenges, for the non-ideal power converters, were of a moderate difficulty level due to the requirement of intensive guidance from the user to mechanize the proofs. In the formal periodic steady-state analysis and design of the non-ideal power converters, the multivariate transcendental, differential and integral theories of `HOL Light` were utilized to exhaustively specify and verify the systems. Usually, interactive theorem proving is considered quite expensive in terms of the time and effort required to accomplish the formal verification task, but this comparison reveals interesting trend of decreasing time and effort required in the presence of reusable formal libraries. Whereas, resulting formalization of the non-ideal power converters is valuable as it allows to use interactive theorem proving technique for designing real-world power converters for safety or mission-critical applications.

# 7

## Conclusions and Future Work

### 7.1 Conclusions

In this thesis, we have proposed to use higher-order-logic theorem proving for the analysis and design of power electronics circuits as a complementary approach to the state-of-the-art simulation and paper-pencil techniques. Power electronics circuits are characterized as hybrid systems, i.e., the systems that exhibit continuous behavior driven by discrete switching events, and thus pose serious challenges of modeling, analyzing and verification using traditional techniques. The main motivation for developing a theorem proving based analysis and design framework for power electronics systems is to leverage upon the high-expressiveness of higher-order logic and soundness of theorem provers to ensure an accurate and exhaustive analysis and design of power electronics circuits. Thus, the proposed solution can prove to very useful for the analysis and design of safety and mission-critical power processing applications.

The primary objective is to develop a comprehensive logical framework in higher-order logic to facilitate the formal specification and verification of power electronics systems in both time-domain and frequency domain. The

proposed formalization, mainly, facilitates the periodic steady-state analysis, in time-domain and stability analysis, in frequency domain, of power electronics circuits. In time-domain analysis, notable feature of the proposed formalization is that it caters for the hybrid behavior of power electronics circuits using higher-order-logic theorem proving. In this regard, a formal library of power electronics circuit components is developed which is accompanied by the formalization of basic circuit theory notions and formally verified properties of piecewise functions. To enable the formal time-domain based steady-state analysis of power electronics, we also present formalization of differential equations that includes formal verification of the circuit parameters, formal library of important steady-state characteristics and design parameters. The above formalization framework enables to formally specify and reason about various crucial aspects of power electronics circuits in time-domain, including, topology, behavior and parameter verification. The major advantage of the time-domain formalization is that it caters for the hybrid behavior of the systems by incorporating singularities which are inevitable due to switching operation in the modeling and analysis of the power electronics systems. Moreover, the logical framework is based on the real-valued complex functions and hence capable of formally specifying and verifying almost all type of the power electronics systems, such as AC-AC, DC-AC or AC-DC circuits. The proposed formalization is employed to formally verify the periodic steady-state analysis and design of the ideal and non-ideal DC-DC Buck converters. The formal verification included topology, behavior and design specification of the circuits.

In this thesis, we have also presented a formalization of the stability theory in complex domain. We formally model the stability definition in higher-order logic using characteristic equation which is the denominator of the transfer function of the system. To enable the formal reasoning about the stability criterion, we also produced mechanized proofs for the factorization of

the characteristic equations upto the fourth order. Next, we formally verified the stability criterion for the characteristic equations within the sound core of the `HOL Light` theorem prover. The main advantage of the proposed formal stability analysis is that the formal results are generic and can be readily used to formally verify all engineering system that have characteristic equations upto the fourth order. We utilize the proposed formalization to formally verify the stability of the power converter controllers which are direly needed to smooth the intermittent energy flow from the wind turbines in a smart grid. The formal verification in the `HOL Light` theorem prover resulted in the exhaustive set of assumptions in terms of coefficients of the characteristic equations.

## 7.2 Future Work

The formalization and verification results, presented in this thesis, open new avenues in using theorem proving for the precise analysis of power electronics systems as a complement to the simulation and model checking techniques. The proposed theorem proving logical framework for power electronics systems can be further equipped and strengthened by adding new features. Some of the future extensions are outlined below.

- Dynamic behavior of power electronics circuits is vital to the performance evaluation. In this regard, a hybrid approach leveraging upon the strengths of two formal methods techniques, i.e., theorem proving and model checking, can be very useful. For example, the formally verified results presented , in Section 4.4 and Chapter 6 can be used to formally specify the automaton representing power converters to evaluate the dynamic behavior of the power converters, which are traditionally derived using paper-and-pencil analysis.

- The proposed formalization of steady-state behavior and design of power electronics circuits can be easily extended to incorporate the switching losses of circuits [47], which are also an important consideration in many safety and mission-critical power processing applications.
- The formalization framework of stability can be easily extended to incorporate the formal verification of marginally stable and unstable roots of the presented polynomials, which are also important for the design of many interesting control system designs in power electronics systems.
- Incorporating formally verified results of this thesis into the conventional computer based tools by linking the `HOL Light` with these external tools [38], such as MathWorks Simulink/Stateflow [57] and Maxima [58], which will allow users (other than formal methods practitioners) to generate formal proofs of the power electronics systems.
- The proposed formalization allows to formally verify power electronics circuits as a single-input single-output system (SISO). However, complicated analysis and design of power electronics systems involves modeling the systems as multi-input multi-output systems (MIMO) [64]. The state space representations largely depends upon linear algebra techniques, such as eigen-value analysis [31], to analyze and design power electronics systems. In this regard, the proposed formalization of stability in Chapter 5 can be used to perform runtime verification [50] of eigenvalues for a system represented and analyzed using state space representation.

# Bibliography

- [1] Muhammad Ahmad and Osman Hasan. Formal verification of steady-state errors in unity-feedback control systems. In *International Workshop on Formal Methods for Industrial Critical Systems*, pages 1–15. Springer, 2014.
- [2] Asad Ahmed. Formal Periodic Steady-state Analysis of Power Converters in Time-domain, <http://save.seecs.nust.edu.pk/projects/fpssapc/>, 2019. Online; accessed May-2021.
- [3] Asad Ahmed. Formal Steady-state Analysis of Non-ideal Power Converters using Interactive Theorem Proving, <https://github.com/a150285a/npcf/>, 2021. Online; accessed May-2021.
- [4] S. Massoud Amin and B. F. Wollenberg. Toward a smart grid: power delivery for the 21st century. *IEEE Power and Energy Magazine*, 3(5):34–41, Sept 2005.
- [5] Stanley Bak and Parasara Sridhar Duggirala. Hylaa: A tool for computing simulation-equivalent reachability for linear systems. In *Proceedings of the 20th International Conference on Hybrid Systems: Computation and Control*, pages 173–178, 2017.
- [6] B Jayant Baliga. *Fundamentals of power semiconductor devices*. Springer Science & Business Media, 2010.

- [7] Robert J Barker, Neville C Luhmann, John H Booske, and Gregory S Nusinovich. *Modern microwave and millimeter-wave power electronics*. 2005.
- [8] Issa Batarseh and Ahmad Harb. *Power Electronics*. Springer, 2018.
- [9] Omar Ali Beg, Houssam Abbas, Taylor T Johnson, and Ali Davoudi. Model validation of pwm dc–dc converters. *IEEE Transactions on Industrial Electronics*, 64(9):7049–7059, 2017.
- [10] Omar Ali Beg, Luan Nguyen, Ali Davoudi, and Taylor T Johnson. Computer-aided formal verification of power electronics circuits. In *FAC 2017; Frontiers in Analog CAD*, pages 1–6. VDE, 2017.
- [11] Gerd Behrmann, Alexandre David, and Kim G Larsen. A tutorial on uppaal 4.0. *Department of computer science, Aalborg university*, 2006.
- [12] Sidi Mohamed Beillahi, Umair Siddique, and Sofiène Tahar. Formal analysis of power electronic systems. In *The 17th International Conference on Formal Engineering Methods, ICFEM2015, Paris*, pages 270–286. Springer, 2015. DOI: 10.1007/978-3-319-25423-4\_17.
- [13] K Bimal. *Modern power electronics and AC drives*. Prentice-Hall, 2001.
- [14] William E Boyce, Richard C DiPrima, and Douglas B Meade. *Elementary differential equations and boundary value problems*. John Wiley & Sons, 2021.
- [15] Ching Chuen Chan and KT Chau. An overview of power electronics in electric vehicles. *IEEE transactions on Industrial Electronics*, 44(1):3–13, 1997.
- [16] Edmund M Clarke, Thomas A Henzinger, Helmut Veith, and Roderick Bloem. *Handbook of model checking*, volume 10. Springer, 2018.

- [17] Edmund M Clarke, William Klieber, Miloš Nováček, and Paolo Zuliani. Model checking and the state explosion problem. In *LASER Summer School on Software Engineering*, pages 1–30. Springer, 2011.
- [18] Philip J Davis and Philip Rabinowitz. *Methods of numerical integration*. Courier Corporation, 2007.
- [19] LMBC de Costa Campos. *Generalized calculus with applications to matter and forces*. CRC Press, Boca Raton, Florida, United States, 2014. DOI: 10.1007/BF02745840.
- [20] Charles A Desoer. *Basic circuit theory*. Tata McGraw-Hill Education, India, 2010.
- [21] Phil PG Dyke. *An introduction to Laplace transforms and Fourier series*. Springer, 2014.
- [22] K Emadi and MJIA Ehsani. Aircraft power systems: technology, state of the art, and future trends. *IEEE Aerospace and Electronic Systems Magazine*, 15(1):28–32, 2000. DOI: 10.1109/62.821660.
- [23] Juan Manuel Enrique, Antonio Javier Barragán, Eladio Durán, and José Manuel Andújar. Theoretical assessment of dc/dc power converter-  
sâĀŻ basic topologies. a common static model. *Applied Sciences*, 8(1):19, 2018.
- [24] Robert W Erickson and Dragan Maksimovic. *Fundamentals of power electronics*. Springer Science & Business Media, Germany, Berlin, 2007. DOI: 10.1007/b100747.
- [25] FDA. <https://www.fda.gov/medical-devices/medical-device-recalls/medtronic-inc-recalls-instructions-use-and-patient-manual-heartware-hvad-system-update-information>. [Online; accessed June-2021].



- [26] FDA. <https://www.fda.gov/medical-devices/medical-device-recalls/edwards-lifesciences-llc-recalls-ev1000-clinical-platforms-due-electrical-short-circuit-which-may>. [Online; accessed June-2021].
- [27] FDA. <https://www.fda.gov/medical-devices/medical-device-recalls/philips-medical-systems-cleveland-recalls-for-te-gamma-camera-system-due-potential-detector-drop>. [Online; accessed June-2021].
- [28] Goran Frehse. Phaver: algorithmic verification of hybrid systems past hytech. *International Journal on Software Tools for Technology Transfer*, 10(3):263–279, 2008.
- [29] Goran Frehse, Colas Le Guernic, Alexandre Donzé, et al. SpaceEx: Scalable verification of hybrid systems. In Shaz Qadeer Ganesh Gopalakrishnan, editor, *Proc. 23rd International Conference on Computer Aided Verification (CAV)*, LNCS. Springer, 2011.
- [30] Vincenzo Giordano, Flavia Gangale, Gianluca Fulli, Manuel Sánchez Jiménez, Ijeoma Onyeji, Alexandru Colta, Ioulia Papaioannou, Anna Mengolini, Corina Alecu, Tauno Ojala, et al. Smart grid projects in Europe. *JRC Ref Rep Sy*, 8, 2011.
- [31] Leonard L Grigsby. *Power system stability and control*. CRC press, 2007.
- [32] Thomas Hales, Mark Adams, Gertrud Bauer, Tat Dat Dang, John Harrison, Hoang Le Truong, Cezary Kaliszyk, Victor Magron, Sean McLaughlin, Tat Thang Nguyen, et al. A formal proof of the kepler conjecture. In *Forum of Mathematics, Pi*, volume 5. Cambridge University Press, 2017.

- [33] Tom Hales. flyspeck. <https://code.google.com/archive/p/flyspeck/>. [Online; accessed 29-July-2020].
- [34] John Harrison. Formalizing 100 theorems. <http://www.cs.ru.nl/~freek/100/>. [Online; accessed 29-July-2020].
- [35] John Harrison. Floating point verification in hol light: the exponential function. In *International Conference on Algebraic Methodology and Software Technology*, pages 246–260. Springer, 1997.
- [36] John Harrison. A short survey of automated reasoning. In *International Conference on Algebraic Biology*, pages 334–349. Springer, 2007.
- [37] John Harrison. The HOL light theory of euclidean space. *Journal of Automated Reasoning*, 50(2):173–190, 2013.
- [38] John Harrison. Hol light tutorial, <https://www.cl.cam.ac.uk/~jrh13/hol-light/tutorial.pdf>, 2017. Online; accessed May-2021.
- [39] John Harrison, Josef Urban, and Freek Wiedijk. History of interactive theorem proving. In *Computational Logic*, volume 9, pages 135–214, 2014.
- [40] Osman Hasan and Muhammad Ahmad. Formal analysis of steady state errors in feedback control systems using hol-light. In *Proceedings of the Conference on Design, Automation and Test in Europe*, pages 1423–1426. EDA Consortium, 2013.
- [41] Osman Hasan and Sofiene Tahar. Formal verification methods. In *Encyclopedia of Information Science and Technology, Third Edition*, pages 7162–7170. IGI Global, 2015.
- [42] Thomas A Henzinger, Pei-Hsin Ho, and Howard Wong-Toi. Hytech: A model checker for hybrid systems. *International Journal on Software Tools for Technology Transfer*, 1(1-2):110–122, 1997.

- [43] Donald W Hight. *A concept of limits*. Courier Corporation, 2012.
- [44] Richard G Hoft and Jordan B Casteel. Power electronic circuit analysis techniques. *IFAC Proceedings Volumes*, 10(10):987–1024, 1977.
- [45] Tomas Hornik and Qing-Chang Zhong. A current-control strategy for voltage-source inverters in microgrids based on  $H^\infty$  and repetitive control. *IEEE Trans. Power Electron*, 26(3):943–952, 2011.
- [46] Thomas M Jahns and Vladimir Blasko. Recent advances in power electronics technology for industrial and traction machine drives. *Proceedings of the IEEE*, 89(6):963–975, 2001.
- [47] David Jauregui, Bo Wang, and Rengang Chen. Power loss calculation with common source inductance consideration for synchronous buck converters, <https://www.ti.com/lit/an/slpa009a/slpa009a.pdf>, 2011. Online; accessed March-2021.
- [48] Philip T Krein, Joseph Bentsman, Richard M Bass, and Bernard L Lesieutre. On the use of averaging for the analysis of power electronic systems. *IEEE Transactions on Power Electronics*, 5(2):182–190, 1990. DOI: 10.1109/63.53155.
- [49] Tuo Yeong Lee. *Henstock-Kurzweil integration on Euclidean spaces*, volume 12. World Scientific, 2011.
- [50] Martin Leucker and Christian Schallhart. A brief account of runtime verification. *The Journal of Logic and Algebraic Programming*, 78(5):293–303, 2009.
- [51] Dragan. Maksimovic. Automated steady-state analysis of switching power converters using a general-purpose simulation tool. In *Record 28th Annual IEEE Power Electronics Specialists Conference, PESC97*,

- June 1997, St. Louis, MO, USA*, volume 2, pages 1352–1358. IEEE, 1997. DOI: 10.1109/pesc.1997.616944.
- [52] Zohar Manna and Amir Pnueli. *The temporal logic of reactive and concurrent systems: Specification*. Springer Science & Business Media, 2012.
- [53] H Alan Mantooth and Martin Vlach. Beyond spice with saber and mast. In *[Proceedings] 1992 IEEE International Symposium on Circuits and Systems*, volume 1, pages 77–80. IEEE, 1992.
- [54] Filip Maric. A survey of interactive theorem proving. *Zbornik radova*, 18(26):173–223, 2015.
- [55] C. C. Marouchos. *The Switching Function: Analysis of Power Electronic Circuits*, volume 17. IET, United Kingdom, 2006. DOI: 10.1049/pbcs017e.
- [56] MathWorks. <https://www.mathworks.com/solutions/power-electronics-control.html>.
- [57] MathWorks. stateflow, <https://www.mathworks.com/products/stateflow.html>. Online; accessed May-2021.
- [58] Maxima. <https://maxima.sourceforge.io/>. Online; accessed May-2021.
- [59] RD Middlebrook and Slobodan Cuk. A general unified approach to modelling switching-converter power stages. In *Power Electronics Specialists Conference, 1976 IEEE*, pages 18–34. IEEE, 1976.
- [60] Marcia Verônica Costa Miranda and Antônio Marcus Nogueira Lima. Formal verification and controller redesign of power electronic converters. In *Industrial Electronics, IEEE International Symposium on Industrial Electronics, Ajaccio, France*, volume 2, pages 907–912. IEEE, 2004. DOI: 10.1109/ISIE.2004.1571934.

- [61] Ned Mohan, William P Robbins, Tore M Undeland, Robert Nilssen, and Olve Mo. Simulation of power electronic and motion control systems-an overview. *Proceedings of the IEEE*, 82(8):1287–1302, 1994.
- [62] James A Momoh. *Smart grid: fundamentals of design and analysis*, volume 63. John Wiley & Sons, 2012.
- [63] Toyota Motor Corporation. Defect information report (nhtsa recall 14v-053). <https://static.nhtsa.gov/odi/rc1/2018/RMISC-18V684-8461.pdf>. [Online; accessed June-2021].
- [64] Norman S Nise. *Control Systems Engineering*. John Wiley & Sons, 2007.
- [65] U.S. Department of Energy (DOE). The Smart Grid: An Introduction. [https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE\\_SG\\_Book\\_Single\\_Pages%281%29.pdf](https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf). [Online; accessed June-2021].
- [66] André Platzer and Yong Kiam Tan. Differential equation axiomatization: The impressive power of differential ghosts. In Anuj Dawar and Erich Grädel, editors, *LICS*, pages 819–828, New York, 2018. ACM.
- [67] Junaid Qadir and Osman Hasan. Applying formal methods to networking: theory, techniques, and applications. *IEEE Communications Surveys & Tutorials*, 17(1):256–291, 2014.
- [68] Adnan Rashid and Osman Hasan. Formal analysis of linear control systems using theorem proving. In *International Conference on Formal Engineering Methods*, pages 345–361. Springer, 2017.
- [69] Adnan Rashid, Umair Siddique, and Osman Hasan. Formal verification of platoon control strategies. In *International Conference on Software Engineering and Formal Methods*, pages 223–238. Springer, 2018.

- [70] Muhammad H Rashid. *Spice for power electronics and electric power*. CRC press, 2012.
- [71] Muhammad Usman Sanwal and Osman Hasan. Formally analyzing continuous aspects of cyber-physical systems modeled by homogeneous linear differential equations. In *International Workshop on Design, Modeling, and Evaluation of Cyber Physical Systems*, pages 132–146. Springer, 2015.
- [72] ROHM Semiconductor. Switching regulator ic series «efficiency of buck converter», 15, 2016.
- [73] Matthew Senesky, Gabriel Eirea, and T John Koo. Hybrid modelling and control of power electronics. In *Maler O., Pnueli A. (eds) Hybrid Systems: Computation and Control, HSCC 2003, Lecture Notes in Computer Science*,, volume 2623. Springer, Berlin, Heidelberg, 2003. DOI: 10.1007/3-540-36580-x\_33.
- [74] Arman Shehabi, Sarah Smith, Dale Sartor, Richard Brown, Magnus Herlin, Jonathan Koomey, Eric Masanet, Nathaniel Horner, Inês Azevedo, and William Lintner. United states data center energy usage report. 2016.
- [75] Umair Siddique, Vincent Aravantinos, and Sofiene Tahar. Formal stability analysis of optical resonators. In *NASA Formal Methods Symposium. LNCS*, volume 7871, pages 368–382. Springer, Berlin, Heidelberg, 2013.
- [76] Sigurd Skogestad and Ian Postlethwaite. *Multivariable feedback control: analysis and design*, volume 2. Wiley New York, 2007.
- [77] SpaceX. Are spaceEx results formally sound? Are they useless if they're not?, <http://spaceex.imag.fr/documentation/user->

- documentation/frequently-asked-questions-21, 2021. Online; accessed May-2021.
- [78] Anton A Stoorvogel. *The  $H_\infty$  Control Problem: A State Space Approach*. Citeseer, 1992.
- [79] David R Stoutemyer. Crimes and misdemeanors in the computer algebra trade. *Notices of the American Mathematical Society*, 38(7):778–785, 1991.
- [80] Syeda Hira Taqdees and Osman Hasan. Formalization of Laplace transform using the multivariable calculus theory of HOL-light. In *International Conference on Logic for Programming Artificial Intelligence and Reasoning*, pages 744–758. Springer, 2013.
- [81] Syeda Hira Taqdees and Osman Hasan. Formally verifying transfer functions of linear analog circuits. *IEEE Design & Test*, 34(5):30–37, 2017.
- [82] Richard PE Tymerski. *Topology and analysis in power conversion and inversion*. PhD thesis, Virginia Polytechnic Institute and State University, 1988.
- [83] A Walker, Emily Cox, J Loughhead, and J Roberts. Counting the cost: the economic and social costs of electricity shortfalls in the uk-a report for the council for science and technology. 2014.
- [84] Heqiang Wang. Reachability analysis of power electronic converters. 2019.
- [85] Wolfram. Mathematica, <https://www.wolfram.com/mathematica/>. Online; accessed May-2021.
- [86] Yin Xu, Chen-Ching Liu, Kevin P Schneider, Francis K Tuffner, and Dan T Ton. Microgrids for service restoration to critical load in a re-

- silient distribution system. *IEEE Transactions on Smart Grid*, 9(1):426–437, 2016.
- [87] Sadayuki Yamamuro. *Differential calculus in topological linear spaces*, volume 374. Springer, 2006.
- [88] Yanlin Yang, Yin-E Chen, and Zhizhong Liu. Energy constraints and china’s economic development. *Journal of Economic Policy Reform*, 10(4):343–354, 2007.
- [89] Qing-Chang Zhong and Tomas Hornik. *Control of power inverters in renewable energy and smart grid integration*, volume 97. John Wiley & Sons, 2012.



# Publications

## Refereed Journals <sup>1</sup>

**Bio-Jr-1** A. Ahmad, O. Hasan, F. Awwad and N. Bastaki, ‘Formalization of Cost and Utility in Microeconomics’, *Energies*, Multidisciplinary Digital Publishing Institute, 2020.

**Bio-Jr-2** A. Ahmed, O. Hasan and A. Hasan, “Formal Periodic Steady-State Analysis of Power Converters in Time-Domain”, *IfCoLog Journal of Logics and their Applications*, College Publications, 6(3), pp. 447-468, 2019.

**Bio-Jr-3** A. Ahmed, O. Hasan, F. Awwad, S. R. Hasan and N. Bastaki, “Formal Asymptotic Analysis of Online Scheduling Algorithms for Plug-In Electric Vehicles’s Charging”, *Energies*, Multidisciplinary Digital Publishing Institute, 12(1), pp. 1-20, 2018.

## Peer Review Conferences <sup>2</sup>

**Bio-Cf-1** A. Ahmed, O. Hasan and F. Awwad, “Formal Stability Analysis of Control Systems,” In *International Workshop on Formal Techniques*

---

<sup>1</sup>Bio:Jr refers to a journal paper.

<sup>2</sup>Bio:Cf refers to a conference paper.

*for Safety-Critical Systems (FTSC-2018)*, Springer, Cham, Gold Coast, Australia, pp. 3-17.

**Bio-Cf-2** A. Ahmed, O. Hasan, S. Tahar and A. Mohamed, “Formal verification of energy consumption for an EEG monitoring wireless body area sensor network,” *10th International Conference on Open Source Systems & Technologies (ICOSST-2016)*, IEEE, Lahore, Pakistan, pp. 18-22.

**Bio-Cf-3** A. Ahmed, A. Rashid and S. Iqbal, “Analysis of weather forecasting model in PRISM,” *12th International Conference on Frontiers of Information Technology (FIT-2014)*, IEEE, Islamabad, Pakistan, pp. 355-360.