Formal Stability Analysis of Control Systems

Asad Ahmed, Osman Hasan and Falah Awwad[1]

School of Electrical Engineering and Computer Science (SEECS)
National University of Sciences and Technology (NUST)
Islamabad, Pakistan
[1]College of Engineering, United Arab Emirates University, Al-Ain, UAE
{asad.ahmed,osman.hasan}@seecs.nust.edu.pk
f_awwad@uaeu.ac.ae

Abstract. Stability of a control system ensures that its output is under control and thus is the most important characteristic of control systems. Stability is characterized by the roots of the characteristic equation of the given control system in the complex-domain. Traditionally, paper-and-pencil proof methods and computer-based tools are used to analyze the stability of control systems. However, paper-and-pencil proof methods are error prone due to the human involvement. Whereas, computer based tools cannot model the continuous behavior in its true form due to the involvement of computer arithmetic and the associated truncation errors. Therefore, these techniques do not provide an accurate and complete analysis, which is unfortunate given the safety-critical nature of control system applications. In this paper, we propose to overcome these limitations by using higher-order-logic theorem proving for the stability analysis of control systems. For this purpose, we present a higher-order-logic based formalization of stability and the roots of the quadratic, cubic and quartic complex polynomials. The proposed formalization is based on the complex number theory of the HOL-Light theorem prover. A distinguishing feature of this work is the automatic nature of the formal stability analysis, which makes it quite useful for the control engineers working in the industry who have very little expertise about formal methods. For illustration purposes, we present the stability analysis of power converter controllers used in smart grids.

Keywords: Stability, Control systems, Polynomials, HOL-Light

1 Introduction

Stability [15] is the most important design requirement of a linear time-invariant control system. 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 [15] is done in the frequency domain. The main idea is to convert a differential equation representation of the system into its frequency domain representation using

a transform method, like Laplace or Fourier [4]. 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,

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

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 equation 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 [20] 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), 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:

$$b_n s^n + b_{n-1} s^{n-1} ... b_0 = 0 \tag{2}$$

Equation (2) is also referred to as a *characteristic* equation of the system. The system is categorized as *stable*, *unstable* and *marginally stable* based on the location of the roots of Equation (2) in the complex-plane. 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.

Traditionally, paper-and-pencil proof methods and computer based tools are used to perform the stability analysis of control systems. The stability analysis using paper-and-pencil proof methods is based on the quadratic formula for the second order polynomial (quadratic), Cardano's method, Vieta's method and Lagrange's method for the third order polynomial (cubic), and Ferrari's solution, Descartes' solution and Euler's solution for the fourth order polynomial (quartic). Whereas, to the best of our knowledge, there does not exist any closed form solution to find the root for higher than fourth order polynomials. Routh-Hurwitz criterion [15] is another paper-and-pencil proof method, which is used for the stability analysis of control systems. It consists of building a table using the coefficients of the given polynomial following certain rules. This table can be used to find if the given system is stable or unstable on the basis of patterns

exhibited by the rows and columns of the table [15]. The manual analytical analysis involved in these methods make them prone to human error. Moreover, these risks significantly increase with an increase in the system complexity.

Many computer-aided design tools based on the principles of numerical methods and simulation have also been introduced for the modeling and analysis of linear time-invariant control systems. For example, MathWorks Simulink [13] and MathWorks Control System Toolbox [12] facilitate finding the poles and zeros of the system and are thus frequently used in the design and analysis of control systems. They provide a scalable option to handle large and complex systems as well. However, these computer based techniques cannot capture the continuous aspects of the system in their true form and are based on the discrete frequency models. The completeness of the model is thus lost while dealing with the continuous time behavior. Moreover, the numerical values of roots computed using computer based arithmetic, like floating or fixed point numbers, are subject to truncation errors, and hence may not be accurate. Another alternative for analyzing the stability of control systems is computer algebra systems, such as Mathematica [26], Maple [10] and Maxima [21]. These methods are very efficient for computing the roots of a system, symbolically, but they are not reliable as well [8] due to the presence of unverified huge symbolic manipulation algorithms in their core, which are quite likely to contain bugs. Thus, given the above-mentioned inaccuracies, these traditional techniques should not be relied upon for the stability analysis of control systems used in safety-critical applications, such as nuclear plants, electric vehicles or auto-pilot systems, where an inaccurate or erroneous analysis could result in unfortunate catastrophic events that may even lead to the loss of human lives.

The main motivation of this paper is to develop a formalization for the stability analysis of linear time-invariant control systems, represented by characteristic equations of order upto four, with minimal dependence on conventional analysis techniques. We consider complex polynomials with real coefficients, for the purpose of formal analysis in higher-order logic, which allow us to express the cubic and quartic complex polynomials in terms of the quadratic polynomials. However, this choice does not limit the scope of the applicability of our formalization as these coefficients are usually real numbers as they represent the different parameters of the system, e.g., resistance in electrical and electronics systems. The formally verified roots, which are poles of the system, are then formally analyzed to check for the stability condition, i.e., if they lie in the left-half of the complex-plane, in the sound core of the higher-order-logic theorem prover HOL-Light [7]. The main motivation of this choice is the extensive reasoning support available in HOL-Light about multivariate complex, real and transcendental theories, which are required for the formalization of stability analysis of control systems.

The rest of the paper is organized as follows: In Section 2, we present a review of the related work. This is followed by the description of the proposed methodology about stability analysis in Section 3. The formalization of the quadratic, cubic and quartic characteristic polynomials is described in Section 4. We utilize

this formalization to formally verify voltage and current controllers designed for the power converters for reliable and efficient smart grid operation in Section 5. Finally, Section 6 concludes the paper.

2 Related Work

The formalization of Laplace transform [24] 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 [9] [2] 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 [19] 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 [17] is proposed and is then used for developing a runtime 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 [16] 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 [18] 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. Whereas, our formalization directly incorporates the transfer function of a control system, as a complex polynomial, for the stability analysis of a control system and thus provides the flexibility to be applied on any control system. A distinguishing aspect of our formal analysis is the explicit availability of an exhaustive list of side assumptions besides every theorem which is not pos-

sible in the informal analysis methods, which can be quite useful for the analysis of safety-critical application designers.

3 Proposed Methodology

We propose to use higher-order-logic theorem proving, as shown in Fig. 1, to formally verify the stability of linear time-invariant control systems. The analysis is primarily based on the characteristic equation of the system, of the fourth order at most, in the complex-domain. The first step in the proposed methodology is to formally verify the roots of the complex quadratic, cubic and quartic polynomials, which represent poles of a given control system. Therefore, these polynomials are described as higher-order-logic functions and the formal verification of their roots are performed using the multivariate complex, real and transcendental theories available in the library of HOL-Light theorem prover, interactively, as shown in Fig. 1. In the next step, the stability condition is formally modeled in higher-order logic to formally verify the stability of these roots, as higher-order-logic theorems, using the formally verified results from the first step, as shown in Fig. 1. Finally, the above-mentioned formalization can be utilized to formally analyze the stability of any control system almost automatically.

4 Stability Formalization

This section provides a formal definition of stability of a root of a polynomial, formally verified results for the close form solutions or roots of polynomilas upto

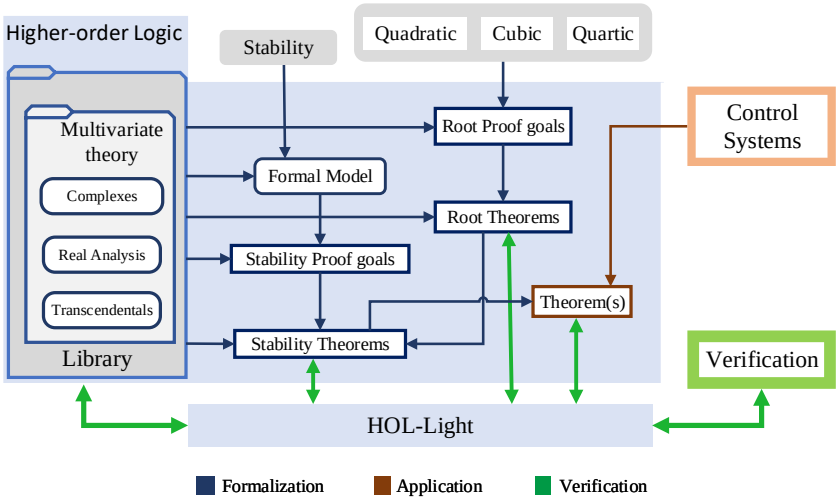

Fig. 1. Proposed methodology for stability analysis in HOL-Light

fourth order and formally verified results on the stability of these polynomials in the HOL-Light theorem prover. The stability of a root is defined, as a higher-order logic function, as:

Definition 1: *Stability*

```
⊢ ∀ f. stable f = ∼({ x | f x = Cx (0) ∧ Re (x) < 0 }= EMPTY )
```

In Definition 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 system and false otherwise. Definition 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.

4.1 Quadratic Polynomial

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

Theorem 1: *Quadratic Roots*

$$\begin{aligned}
&\vdash \forall\ \texttt{a b c x}\ .\\
&\quad \texttt{A1: a} \neq \texttt{0}\\
&\qquad \Rightarrow \texttt{Cx a} * \texttt{x pow 2} + \texttt{Cx b} * \texttt{x} + \texttt{Cx c} = \texttt{Cx 0}\\
&\qquad\quad \texttt{x} = \frac{-\texttt{Cx b} + \sqrt{\texttt{Cx b pow 2} - \texttt{Cx 4} * \texttt{Cx a} * \texttt{Cx c}}}{\texttt{Cx 2} * \texttt{Cx a}} \vee\\
&\qquad\quad \texttt{x} = \frac{-\texttt{Cx b} - \sqrt{\texttt{Cx b pow 2} - \texttt{Cx 4} * \texttt{Cx a} * \texttt{Cx c}}}{\texttt{Cx 2} * \texttt{Cx a}}
\end{aligned}$$

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.

Theorem 1 allows us to formally verify the stability conditions for the case of two roots, using Definition 1, as:

Lemma 1: *Complex Root Case*

$$\begin{aligned}
&\vdash \forall\ \texttt{a b c x}\ .\\
&\quad \texttt{A1: a} \neq \texttt{0} \wedge\\
&\quad \texttt{A2: b pow 2 - 4} * \texttt{a} * \texttt{c} < \texttt{0} \wedge\\
&\quad \texttt{A3: 0} < \tfrac{\texttt{b}}{\texttt{a}}\\
&\quad \Rightarrow \texttt{stable}\ (\lambda \texttt{x.}\ \texttt{Cx a} * \texttt{x pow 2} + \texttt{Cx b} * \texttt{x} + \texttt{Cx c})
\end{aligned}$$

Lemma 2 *Real Root Case 1*

$$\begin{aligned}&\vdash \forall\ \mathtt{a\ b\ c\ x}\ .\\ &\quad \mathtt{A1:\ a} \neq \mathtt{0} \wedge\\ &\quad \mathtt{A2:\ b\ pow\ 2\ -\ 4} * \mathtt{a} * \mathtt{c} = \mathtt{0} \wedge\\ &\quad \mathtt{A3:}\ 0 < \tfrac{b}{a}\\ &\quad \Rightarrow \mathtt{stable}\ (\lambda \mathtt{x.\ Cx\ a} * \ \mathtt{x\ pow\ 2} + \ \mathtt{Cx\ b} * \ \mathtt{x} + \ \mathtt{Cx\ c})\end{aligned}$$

Lemma 3 *Real Root Case 2*

$$\begin{aligned}&\vdash \forall\ \mathtt{a\ b\ c\ x}\ .\\ &\quad \mathtt{A1:\ a} < \mathtt{0} \wedge\\ &\quad \mathtt{A2:}\ 0 < \mathtt{b\ pow\ 2\ -\ 4} * \mathtt{a} * \mathtt{c}\\ &\quad \mathtt{A3:\ b} < \sqrt{\mathtt{b\ pow\ 2\ -\ 4} * \mathtt{a} * \mathtt{c}}\\ &\quad \Rightarrow \mathtt{stable}\ (\lambda \mathtt{x.\ Cx\ a} * \ \mathtt{x\ pow\ 2} + \ \mathtt{Cx\ b} * \ \mathtt{x} + \ \mathtt{Cx\ c})\end{aligned}$$

Lemma 4: *Real Root Case 3*

$$\begin{aligned}&\vdash \forall\ \mathtt{a\ b\ c\ x}\ .\\ &\quad \mathtt{A1:\ a} < \mathtt{0} \wedge\\ &\quad \mathtt{A2:\ b\ pow\ 2\ -\ 4} * \mathtt{a} * \mathtt{c} < \mathtt{0} \wedge\\ &\quad \mathtt{A3:}\ \sqrt{\mathtt{b\ pow\ 2\ -\ 4} * \mathtt{a} * \mathtt{c}} < \mathtt{-\ b}\\ &\quad \Rightarrow \mathtt{stable}\ (\lambda \mathtt{x.\ Cx\ a} * \ \mathtt{x\ pow\ 2} + \ \mathtt{Cx\ b} * \ \mathtt{x} + \ \mathtt{Cx\ c})\end{aligned}$$

Lemma 5: *Real Root Case 4*

$$\begin{aligned}&\vdash \forall\ \mathtt{a\ b\ c\ x}\ .\\ &\quad \mathtt{A1:}\ 0 < \mathtt{a} \wedge\\ &\quad \mathtt{A2:}\ 0 < \mathtt{b\ pow\ 2\ -\ 4} * \mathtt{a} * \mathtt{c} \wedge\\ &\quad \mathtt{A3:}\ \sqrt{\mathtt{b\ pow\ 2\ -\ 4} * \mathtt{a} * \mathtt{c}} < \mathtt{b}\\ &\quad \Rightarrow \mathtt{stable}\ (\lambda \mathtt{x.\ Cx\ a} * \ \mathtt{x\ pow\ 2} + \ \mathtt{Cx\ b} * \ \mathtt{x} + \ \mathtt{Cx\ c})\end{aligned}$$

Lemma 6: *Real Root Case 5*

$$\begin{aligned}&\vdash \forall\ \mathtt{a\ b\ c\ x}\ .\\ &\quad \mathtt{A1:}\ 0 < \mathtt{a} \wedge\\ &\quad \mathtt{A2:}\ 0 < \mathtt{b\ pow\ 2\ -\ 4} * \mathtt{a} * \mathtt{c} \wedge\\ &\quad \mathtt{A3:\ -\ b} < \sqrt{\mathtt{b\ pow\ 2\ -\ 4} * \mathtt{a} * \mathtt{c}}\\ &\quad \Rightarrow \mathtt{stable}\ (\lambda \mathtt{x.\ Cx\ a} * \ \mathtt{x\ pow\ 2} + \ \mathtt{Cx\ b} * \ \mathtt{x} + \ \mathtt{Cx\ c})\end{aligned}$$

Lemmas 1-6 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 Fig.2.

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

Theorem 2: *Quadratic Stability*

$$\begin{aligned}&\vdash \forall\ \mathtt{a\ b\ c\ x}\ .\\ &\quad \mathtt{A1:\ a} \neq \mathtt{0} \wedge\\ &\quad \mathtt{A2:}\ \ 0 < \tfrac{b}{a} \wedge (\ \mathtt{b\ pow\ 2\ -\ 4} * \mathtt{a} * \mathtt{c} < \mathtt{0} \vee\ \ \mathtt{b\ pow\ 2\ -\ 4} * \mathtt{a} * \mathtt{c} = \mathtt{0}\ )\\ &\vee\\ &\qquad 0 < \mathtt{b\ pow\ 2\ -\ 4} * \mathtt{a} * \mathtt{c} \wedge\end{aligned}$$

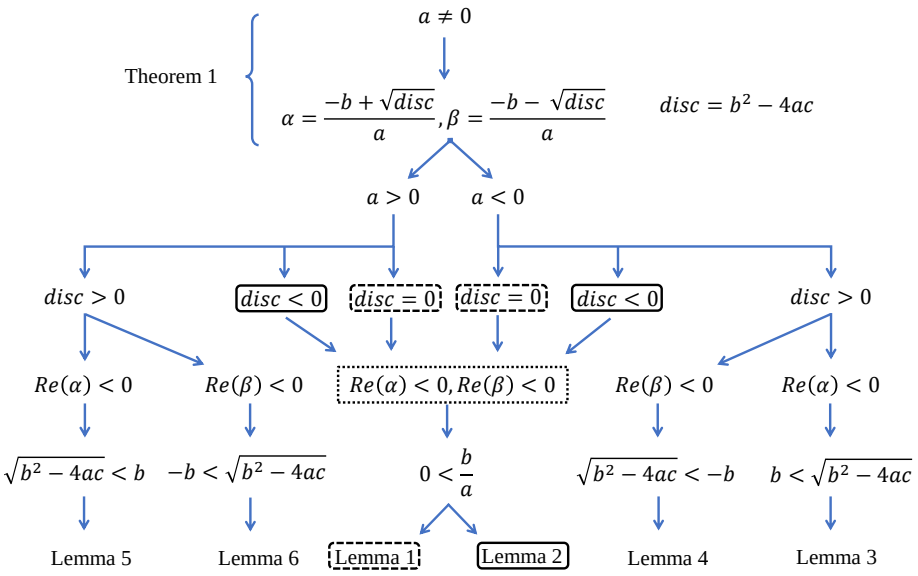

Fig. 2. Stability of Quadratic Polynomial

```
( a < 0 ∧ ( b < √(b pow 2 − 4 * a * c) ∨
            √(b pow 2 − 4 * a * c) < - b ) ∨
  ( 0 < a ∧ ( √(b pow 2 − 4 * a * c) < b ∨
            - b < √(b pow 2 − 4 * a * c) )
⇒ stable (λx. Cx a * x pow 2 + Cx b * x + Cx c)
```

Theorem 2 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 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.

4.2 Cubic Polynomial

In this section, we provide the formally verified results for the roots of a cubic polynomial, and their stability, using Definition 1 and Lemmas 1-6. 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 3: *Cubic Factors*

$$\begin{aligned}&\vdash \forall\ \texttt{a b1 c1 d1 r x}\ .\\ &\quad \texttt{A1: Cx b} = \texttt{Cx b1} + \texttt{Cx a} * \texttt{Cx r} \wedge\\ &\quad \texttt{A2: Cx c} = \texttt{Cx c1} + \texttt{Cx b1} * \texttt{Cx r} \wedge\\ &\quad \texttt{A3: Cx d} = \texttt{Cx c1} * \texttt{Cx r} \wedge\\ &\qquad \Rightarrow \texttt{Cx a} * \texttt{x pow 3} + \texttt{Cx b} * \texttt{xpow 2} + \texttt{Cx c} * \texttt{x} + \texttt{Cx d} =\\ &\qquad\quad (\texttt{x} + \texttt{Cx r}) * (\texttt{Cx a} * \texttt{x pow 2} + \texttt{Cx b1} * \texttt{x} + \texttt{Cx c1})\end{aligned}$$

In the above theorem, `a`, `b1`, `c1`, `d1` and `r` are real-valued random variables, 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 1, Lemmas 1-6 and Theorem 3 in HOL-Light as:

Theorem 4: *Cubic Roots*

$$\begin{aligned}&\vdash \forall\ \texttt{a b1 c1 d1 r x}\ .\\ &\quad \texttt{A1: a} \neq \texttt{0} \wedge\\ &\quad \texttt{A2: Cx b} = \texttt{Cx b1} + \texttt{Cx a} * \texttt{Cx r} \wedge\\ &\quad \texttt{A3: Cx c} = \texttt{Cx c1} + \texttt{Cx b1} * \texttt{Cx r} \wedge\\ &\quad \texttt{A4: Cx d} = \texttt{Cx c1} * \texttt{Cx r}\\ &\quad \Rightarrow (\texttt{Cx a} * \texttt{x pow 3} + \texttt{Cx b} * \texttt{xpow 2} + \texttt{Cx c} * \texttt{x} + \texttt{Cx d} = \texttt{Cx 0})\\ &\qquad = (\ \texttt{x} = \texttt{Cx r} \vee \texttt{x} = \frac{-\texttt{Cx b1} + \sqrt{\texttt{Cx b1 pow 2} - \texttt{Cx 4} * \texttt{Cx a} * \texttt{Cx c1}}}{\texttt{Cx 2} * \texttt{Cx a}} \vee\\ &\qquad\qquad\qquad \texttt{x} = \frac{-\texttt{Cx b1} - \sqrt{\texttt{Cx b1 pow 2} - \texttt{Cx 4} * \texttt{Cx a} * \texttt{Cx c1}}}{\texttt{Cx 2} * \texttt{Cx a}}\ )\end{aligned}$$

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 4 formally verifies that the cubic polynomial has three roots.

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

Theorem 5: *Cubic Stability*

$$\begin{aligned}&\vdash \forall\ \texttt{a b1 c1 d1 r x}\ .\\ &\quad \texttt{A1: a} \neq \texttt{0} \wedge \texttt{A2: Cx b} = \texttt{Cx b1} + \texttt{Cx a} * \texttt{Cx r} \wedge\\ &\quad \texttt{A3: Cx c} = \texttt{Cx c1} + \texttt{Cx b1} * \texttt{Cx r} \wedge \texttt{A4: Cx d} = \texttt{Cx c1} * \texttt{Cx r}\\ &\quad \texttt{A4: 0} < \texttt{r} \vee\\ &\qquad (\ (\ \texttt{0} < \tfrac{\texttt{b1}}{\texttt{a}} \wedge (\ \texttt{b1 pow 2 - 4} * \texttt{a} * \texttt{c1} < \texttt{0} \vee\\ &\qquad\qquad\qquad \texttt{b1 pow 2 - 4} * \texttt{a} * \texttt{c1} = \texttt{0}\ )\ ) \vee\\ &\qquad (\ \texttt{0} < \texttt{b1 pow 2 - 4} * \texttt{a} * \texttt{c1} \wedge\\ &\qquad\qquad (\ \texttt{a} < \texttt{0} \wedge (\ \texttt{b1} \sqrt{\texttt{b1 pow 2} - \texttt{4} * \texttt{a} * \texttt{c1}} \vee\\ &\qquad\qquad\qquad \sqrt{\texttt{b1 pow 2} - \texttt{4} * \texttt{a} * \texttt{c1}} < \texttt{- b1}\ ) \vee\\ &\qquad\qquad (\ \texttt{0} < \texttt{a} \wedge (\ \sqrt{\texttt{b1 pow 2} - \texttt{4} * \texttt{a} * \texttt{c1}} < \texttt{b1} \vee\\ &\qquad\qquad\qquad \texttt{- b} < \sqrt{\texttt{b1 pow 2} - \texttt{4} * \texttt{a} * \texttt{c1}}\ )\ )\ )\\ &\quad \Rightarrow \texttt{stable}\ (\lambda \texttt{x}.\ \texttt{Cx a} * \texttt{x pow 3} + \texttt{Cx b} * \texttt{xpow 2} + \texttt{Cx c} * \texttt{x} + \texttt{Cx d})\end{aligned}$$

Theorem 5 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.

4.3 Quartic Polynomial

In this section, we provide formally verified results for the roots, of a quartic polynomial, and their stability, using Definition 1 and Lemmas 1-6. 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 6: *Quartic Factors*

```
⊢ ∀ a1 b1 c1 a2 b2 c2 x .
    A1: Cx a = Cx a1 * Cx a2 ∧
    A2: Cx b = Cx a1 * Cx b2 + Cx a2 * Cx b1 ∧
    A3: Cx c = Cx a1 * Cx c2 + Cx b1 * Cx b2 + Cx a2 * Cx c1 ∧
    A4: Cx d = Cx b1 * Cx c2 + Cx b2 * Cx c1 ∧
    A5: Cx e = Cx c1 * Cx c2
    ⇒ (Cx a * x pow 4 + Cx b * x pow 3 + Cx c * x pow 2 + Cx d * x
       + Cx e = Cx 0) =
       ( (Cx a1 * x pow 2 + Cx b1 * x + Cx c1) *
         (Cx a2 * x pow 2 + Cx b2 * x + Cx c2) )
```

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 6 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 Definition 1, Lemmas 1-6 and Theorem 6 in HOL-Light as:

Theorem 7: *Quartic Roots*

```
⊢ ∀ a1 b1 c1 a2 b2 c2 x .
    A1: a ≠ 0 ∧ A2: Cx a = Cx a1 * Cx a2 ∧
    A3: Cx b = Cx a1 * Cx b2 + Cx a2 * Cx b1 ∧
    A4: Cx c = Cx a1 * Cx c2 + Cx b1 * Cx b2 + Cx a2 * Cx c1 ∧
    A5: Cx d = Cx b1 * Cx c2 + Cx b2 * Cx c1 ∧
    A6: Cx e = Cx c1 * Cx c2
    ⇒ (Cx a * x pow 4 + Cx b * x pow 3 + Cx c * x pow 2 + Cx d * x
       + Cx e = Cx 0) =
       ( x = (- Cx b1 + √(Cx b1 pow 2 - Cx 4 * Cx a1 * Cx c1)) / (Cx 2 * Cx a1) ∨
         x = (- Cx b1 - √(Cx b1 pow 2 - Cx 4 * Cx a1 * Cx c1)) / (Cx 2 * Cx a1) ∨
         x = (- Cx b2 + √(Cx b2 pow 2 - Cx 4 * Cx a2 * Cx c2)) / (Cx 2 * Cx a2) ∨
         x = (- Cx b2 - √(Cx b2 pow 2 - Cx 4 * Cx a2 * Cx c2)) / (Cx 2 * Cx a2) )
```

In the above theorem, Assumption **A1** ensures that the leading coefficient of the the polynomial is not zero and thus confirming that the given polynomial is quartic. Assumptions **A2**-**A6** provide the factor decomposition of the given quartic polynomial. Based on these assumptions, Theorem 7 formally verifies that the quartic polynomial has four roots.

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

Theorem 8: *Quartic Stability*

$$
\begin{aligned}
\vdash\ & \forall\ \mathtt{a1\ b1\ c1\ a2\ b2\ c2\ x}\ .\\
& \mathtt{A1:\ a} \neq \mathtt{0} \wedge \mathtt{A2:\ Cx\,a} = \mathtt{Cx\,a1} * \mathtt{Cx\,a2} \wedge\\
& \mathtt{A3:\ Cx\,b} = \mathtt{Cx\,a1} * \mathtt{Cx\,b2} + \mathtt{Cx\,a2} * \mathtt{Cx\,b1} \wedge\\
& \mathtt{A4:\ Cx\,c} = \mathtt{Cx\,a1} * \mathtt{Cx\,c2} + \mathtt{Cx\,b1} * \mathtt{Cx\,b2} + \mathtt{Cx\,a2} * \mathtt{Cx\,c1} \wedge\\
& \mathtt{A5:\ Cx\,d} = \mathtt{Cx\,b1} * \mathtt{Cx\,c2} + \mathtt{Cx\,b2} * \mathtt{Cx\,c1} \wedge\\
& \mathtt{A6:\ Cx\,e} = \mathtt{Cx\,c1} * \mathtt{Cx\,c2} \wedge\\
& \mathtt{A7:}\ (\ \mathtt{0} < \tfrac{\mathtt{b1}}{\mathtt{a1}} \wedge (\ \mathtt{b1\,pow\,2} - \mathtt{4} * \mathtt{a1} * \mathtt{c1} < \mathtt{0} \vee\\
& \qquad\qquad \mathtt{b1\,pow\,2} - \mathtt{4} * \mathtt{a1} * \mathtt{c1} = \mathtt{0}\ )\ ) \vee\\
& \quad (\ \mathtt{b1\,pow\,2} - \mathtt{4} * \mathtt{a1} * \mathtt{c1} < \mathtt{0} \wedge\\
& \qquad (\ \mathtt{a1} < \mathtt{0} \wedge (\ \mathtt{b1} < \sqrt{\mathtt{b1\,pow\,2} - \mathtt{4} * \mathtt{a1} * \mathtt{c1}} \vee\\
& \qquad\qquad \sqrt{\mathtt{b1\,pow\,2} - \mathtt{4} * \mathtt{a1} * \mathtt{c1}} < -\,\mathtt{b1}\ ) \vee\\
& \qquad (\ \mathtt{0} < \mathtt{a1} \wedge (\ \sqrt{\mathtt{b1\,pow\,2} - \mathtt{4} * \mathtt{a1} * \mathtt{c1}} < \mathtt{b1} \vee\\
& \qquad\qquad -\,\mathtt{b1} < \sqrt{\mathtt{b1\,pow\,2} - \mathtt{4} * \mathtt{a1} * \mathtt{c1}}\ )\ )\ \vee\\
& \quad (\ \mathtt{0} < \tfrac{\mathtt{b2}}{\mathtt{a2}} \wedge (\ \mathtt{0} < \mathtt{b2\,pow\,2} - \mathtt{4} * \mathtt{a2} * \mathtt{c2} \vee\\
& \qquad\qquad \mathtt{b2\,pow\,2} - \mathtt{4} * \mathtt{a2} * \mathtt{c2} = \mathtt{0}\ )\ ) \vee\\
& \quad (\ \mathtt{b2\,pow\,2} - \mathtt{4} * \mathtt{a2} * \mathtt{c2} < \mathtt{0} \wedge\\
& \qquad (\ \mathtt{a2} < \mathtt{0} \wedge (\ \mathtt{b2} < \sqrt{\mathtt{b2\,pow\,2} - \mathtt{4} * \mathtt{a2} * \mathtt{c2}} \vee\\
& \qquad\qquad \sqrt{\mathtt{b2\,pow\,2} - \mathtt{4} * \mathtt{a2} * \mathtt{c2}} < -\,\mathtt{b1}\ ) \vee\\
& \qquad (\ \mathtt{0} < \mathtt{a2} \wedge (\ \sqrt{\mathtt{b2\,pow\,2} - \mathtt{4} * \mathtt{a2} * \mathtt{c2}} < \mathtt{b2} \vee\\
& \qquad\qquad -\,\mathtt{b2} < \sqrt{\mathtt{b2\,pow\,2} - \mathtt{4} * \mathtt{a2} * \mathtt{c2}}\ )\ )\\
& \Rightarrow \mathtt{stable}\ (\lambda\,\mathtt{x}.\ (\mathtt{Cx\,a} * \mathtt{x\,pow\,4} + \mathtt{Cx\,b} * \mathtt{x\,pow\,3} + \mathtt{Cx\,c} * \mathtt{x\,pow\,2}\\
& \qquad + \mathtt{Cx\,d} * \mathtt{x} + \mathtt{Cx\,e})
\end{aligned}
$$

Theorem 8 provides an exhaustive set of conditions for the stability of the quartic polynomial using the HOL-light theorem prover.

Theorem proving is a highly expressive and sound formal method technique and therefore resulted in an exhaustive set of assumptions for the formal verification of poles of the system and their stability, which is not possible using conventional analysis techniques. Moreover, these assumptions reveal the relationship among the coefficients of polynomials, representing system parameters, which provide useful insights from the perspective of a control system design. The formalization is generic, i.e., all the involved variables are universally quantified, and thus the verified theorems can be specialized to conduct the stability analysis of a control system in an almost automatic manner. The corresponding proof script, which is available for download at [1], has 5000 lines of HOL-Light code and required about 380 man hours of development time.

5 Application: Power Converter Controllers used 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 [14]. There has been an enormous increase in the usage of smart grid technology over the world in the last decade or so [6]. Thus, an insecure and unreliable smart grid can even lead to disastrous consequences [3].

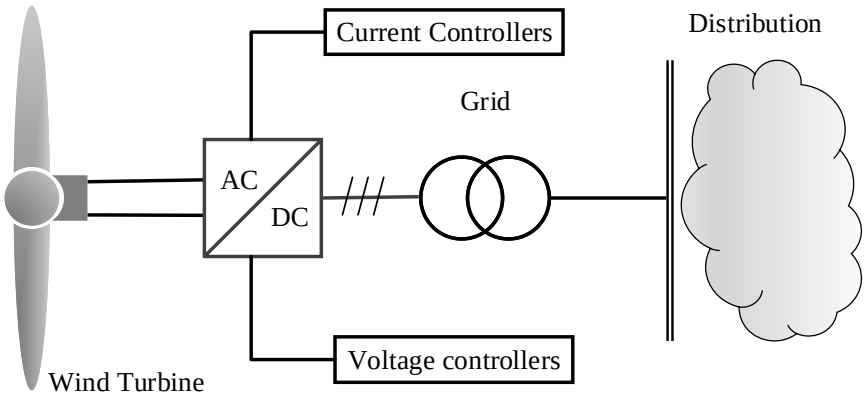

Fig. 3. Efficient energy harvesting using Power converter controllers in smart grids

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 [27]. 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 Fig. 2.

In this paper, we formally verify the stability of an H^∞ current, H^∞ voltage and H^∞ repetitive current controllers designed for the power converters to enhance the efficiency of smart grids [27]. H^∞ [23] and repetitive control [11] 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^∞ current controller is given [27] as:

$$[TF]_i = \frac{1.7998 * 10^9(s + 300)}{s^2 + 4.33403 * 10^8 s + 1.10517 * 10^{12}} \tag{3}$$

The characteristic equation of above transfer function is of second order therefore we utilize Theorem 2 to formally verify the stability in higher-order logic as:

Theorem 9: H^∞ *Current Controller*

$\vdash \forall$ `a b c s .`

`stable (λx. Cx 1 * s pow 2 + Cx 4.3340 * 10^8 * x + Cx 1.10517 * 10^12)`

The transfer function of an H^∞ voltage controller is given [27] as:

$$[TF]_v = \frac{748.649(s^2 + 6954s + 3.026 * 10^8)}{s^3 + 10519s^2 + 3.246 * 10^8 s + 7.7596 * 10^7} \tag{4}$$

The characteristic equation of this transfer function is of third order therefore we utilize Theorem 5 to formally verify the stability in higher-order logic as:

Theorem 10: H^∞ *Voltage Controller*

$$\vdash \forall\ \texttt{a b1 c1 d1 r s}\ .$$
$$\texttt{A1: a} = 1 \wedge \texttt{A2: b1} = 79669 \wedge \texttt{A3: c1} = 3.043 * 10^8 \wedge \texttt{A4: r} = 2550$$
$$\Rightarrow \texttt{stable}\ (\lambda\, \texttt{x.}\ \texttt{Cx}\, 1 * \texttt{s pow}\ 3 + \texttt{Cx}\, 10519 * \texttt{s pow}\ 2 + \texttt{Cx}\, 3.246 * 10^8 * \texttt{s} + \texttt{Cx}\, 7.7596 * 10^7)$$

The transfer function of an H^∞ repetitive current controller is given [27] as:

$$[TF]_{vr} = \frac{8.63 * 10^8 (s + 10^4)(s + 1000)(s + 80)}{s^4 + 1.55 * 10^8 s^3 + 1.83 * 10^{13} s^2 + 1.43 * 10^{17} s + 1.08 * 10^{19}} \tag{5}$$

The characteristic equation of above transfer function is of fourth order therefore we utilize Theorem 8 to formally verify the overall stability in higher-order logic as:

Theorem 11: H^∞ *Repetitive Current Controller*

$$\vdash \forall\ \texttt{a1 b1 c1 a2 b2 c2 s}\ .$$
$$\texttt{A1: a1} = 1 \wedge \texttt{A2: b1} = 1.557 * 10^7 \wedge \texttt{A3: c1} = 1.70538 * 10^3 \wedge$$
$$\texttt{A4: a2} = 1 \wedge \texttt{A5: b2} = 8.403 * 10^3 \wedge \texttt{A6: c2} = 6.375 * 10^5$$
$$\Rightarrow \texttt{stable}\ (\lambda\, \texttt{x.}\ \texttt{Cx}\, 1 * \texttt{s pow}\ 4 + \texttt{Cx}\, 1.55 * 10^8 * \texttt{s pow}\ 3 + \texttt{Cx}\, 1.83 * 10^{13} * \texttt{s pow}\ 2 + 1.43 * 10^{17} * \texttt{s} + \texttt{Cx}\, 1.08 * 10^{19})$$

Theorems 9-11 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 9-11 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 Conclusion

This paper presents a formalization for the stability analysis of control systems, which are used in many safety-critical applications. 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. The formalization framework 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 systems' applications. Based on the formalization presented in this paper, we are in the process of conducting the formal stability analysis of many other safety-critical applications of control systems, including smart grids [5], robotics [22] and smart cars [25].

Acknowledgments. This work is supported by ICT Fund UAE, fund number 21N206 at UAE University, Al Ain, United Arab Emirates

References

1. System Analysis & Verification (SAVe) Lab, `http://save.seecs.nust.edu.pk/projects/fsacs/`, [Online; accessed 12-September-2018]
2. Ahmad, M., Hasan, O.: Formal verification of steady-state errors in unity-feedback control systems. In: International Workshop on Formal Methods for Industrial Critical Systems. pp. 1–15. Springer (2014)
3. Amin, S.M., Wollenberg, B.F.: Toward a smart grid: power delivery for the 21st century. IEEE Power and Energy Magazine 3(5), 34–41 (Sept 2005)
4. Dyke, P.P.: An introduction to Laplace transforms and Fourier series. Springer (2014)
5. Ekanayake, J., Jenkins, N.: Comparison of the response of doubly fed and fixed-speed induction generator wind turbines to changes in network frequency. IEEE Transactions on Energy conversion 19(4), 800–802 (2004)
6. Giordano, V., Gangale, F., Fulli, G., Jiménez, M.S., Onyeji, I., Colta, A., Papaioannou, I., Mengolini, A., Alecu, C., Ojala, T., et al.: Smart grid projects in Europe. JRC Ref Rep Sy 8 (2011)
7. Harrison, J.: HOL Light: An overview. In: International Conference on Theorem Proving in Higher Order Logics. vol. 5674, pp. 60–66. Springer, Springer-Verlag (2009)
8. Harrison, J.: Theorem proving with the real numbers. Springer Science & Business Media (2012)
9. Hasan, O., Ahmad, M.: 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. pp. 1423–1426. EDA Consortium (2013)
10. Heck, A., Heck, A.: Introduction to MAPLE, vol. 1993. Springer-Verlag New York (1993)
11. Hornik, T., Zhong, Q.C.: A current-control strategy for voltage-source inverters in microgrids based on H∞ and repetitive control. IEEE Trans. Power Electron 26(3), 943–952 (2011)
12. MathWorks: Control System Toolbox, `https://ch.mathworks.com/products/control.html`, [Online; accessed 12-Sep-2018]
13. MathWorks: Simulink, `https://www.mathworks.com/products/simulink.html`, [Online; accessed 12-Sep-2018]
14. Momoh, J.A.: Smart grid: fundamentals of design and analysis, vol. 63. John Wiley & Sons (2012)
15. Nise, N.S.: Control Systems Engineering. John Wiley & Sons (2007)
16. Rashid, A., Hasan, O.: Formal analysis of linear control systems using theorem proving. In: International Conference on Formal Engineering Methods. pp. 345–361. Springer (2017)

17. Rashid, A., Siddique, U., Hasan, O.: Formal verification of platoon control strategies. In: International Conference on Software Engineering and Formal Methods. pp. 223–238. Springer (2018)
18. Sanwal, M.U., Hasan, O.: 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. LNCS. vol. 9361, pp. 132–146. Springer (2015)
19. Siddique, U., Aravantinos, V., Tahar, S.: Formal stability analysis of optical resonators. In: NASA Formal Methods Symposium. LNCS. vol. 7871, pp. 368–382. Springer, Berlin, Heidelberg (2013)
20. Skogestad, S., Postlethwaite, I.: Multivariable feedback control: analysis and design, vol. 2. Wiley New York (2007)
21. Sourceforge: Maxima, `http://maxima.sourceforge.net/`, [Online; accessed 12-Sep-2018]
22. Spong, M.W., Hutchinson, S., Vidyasagar, M., et al.: Robot modeling and control, vol. 3. Wiley New York (2006)
23. Stoorvogel, A.A.: The H_∞ Control Problem: A State Space Approach. Citeseer (1992)
24. Taqdees, S.H., Hasan, O.: Formalization of Laplace transform using the multivariable calculus theory of HOL-light. In: International Conference on Logic for Programming Artificial Intelligence and Reasoning. pp. 744–758. Springer (2013)
25. Varaiya, P.: Smart cars on smart roads: problems of control. IEEE Transactions on automatic control 38(2), 195–207 (1993)
26. Wellin, P.R., Gaylord, R.J., Kamin, S.N.: An introduction to programming with Mathematica®. Cambridge University Press (2005)
27. Zhong, Q.C., Hornik, T.: Control of power inverters in renewable energy and smart grid integration, vol. 97. John Wiley & Sons (2012)