Using an Interactive Theorem Prover for Formally Analyzing the Dynamics of the Unmanned Aerial Vehicles

Adnan Rashid, Osman Hasan and Sa'ed Abed

Abstract The dynamical analysis of Unmanned Aerial Vehicles (UAVs) is based on accessing their performance, stability, and various other control systems properties and it involves modelling their dynamical behavior that is generally captured by a set of differential equations. The state-of-the-art approaches used to study the dynamics of UAVs are analytical and computer-based testing or simulations. However, the inherent limitations of these methods, i.e., human error proneness, sampling-based analysis, approximations of the mathematical results and the presence of unverified algorithms in the core of the associated tools, make them unsuitable for analyzing the UAVs, which are extensively being advocated to be used in many safety-critical applications. Recently, interactive theorem proving, a formal verification technique, has been utilized for analyzing the dynamics of UAVs to overcome the above-stated limitations of the conventional approaches. This chapter briefly overviews these interactive theorem proving based efforts while highlighting their strengths and weaknesses.

Key words: Formal methods, Unmanned aerial vehicles, Dynamics, Interactive theorem proving

Adnan Rashid
School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan, e-mail: adnan.rashid@seecs.edu.pk

Osman Hasan
School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan, e-mail: osman.hasan@seecs.edu.pk

Sa'ed Abed
Computer Engineering Department, College of Engineering and Petroleum, Kuwait University, Kuwait, e-mail: s.abed@ku.edu.kw

Acronyms

AEoM	Aircraft Equations of Motion
CAA	Civil Aviation Authority
DAIDALUS	Detect and Avoid Alerting Logic for Unmanned Systems
DE	Differential Equation
DEs	Differential Equations
EoM	Equations of Motion
FD	Frequency-domain
GSN	Goal Structuring Notation
HA	Hybrid Automata
HL	HOL Light
HLMC	Hybrid Logic Model Checker
HLTP	HOL Light theorem prover
LDEoM	Lateral-directional Equations of Motion
LEoM	Longitudinal Equations of Motion
LHA	Linear Hybrid Automata
LT	Laplace Transform
MC	Model Checking
MIMO	Multiple-input Multiple-output
Ocaml	Objective CAML
RPAs	Remotely-Piloted Aircrafts
TALS	Tactical Automated Landing System
TF	Transfer Function
TP	Theorem Proving
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
UAVs	Unmanned Aerial Vehicles
UV	Unmanned Vehicle

1 Introduction

Unmanned Aerial Vehicles (UAVs) [17] are the aircrafts that are operated, either; (i) by a human operator on ground that are also known as Remotely-Piloted Aircrafts (RPAs) or; (ii) using a built-in computer system, such as autopilot assistance, providing a certain degree of autonomy or; (iii) as a fully autonomous aircraft without any involvement of the human intervention. In all these scenarios, UAVs do not require any pilot aboard. Moreover, they are frequently utilized for completing various tasks, like navigation, guidance and the flight control operations in many domains, ranging from civilian [5] to military [27] applications, such as transportation [5], remote sensing [15], surveillance [37] and rescue missions [6] etc. Moreover, due to their extensive utility in the above-stated civilian and military applications, UAVs

are making a remarkable addition to the economic development and safety enhancement.

Notations

x_n	x-axis of the navigation coordinate frame
y_n	y-axis of the navigation coordinate frame
z_n	z-axis of the navigation coordinate frame
x_b	x-axis of the body coordinate frame
y_b	y-axis of the body coordinate frame
z_b	z-axis of the body coordinate frame
O_b	Center of mass of the aircraft
ψ	Yaw angle
ϕ	Roll angle
θ	Pitch angle
U_e	Axial Velocity
V_e	Lateral Velocity
W_e	Normal Velocity
I	Moment of inertia
X	Axial force
Z	Normal force
M	Pitching moment
η	Elevator angle
τ	Thurst

The continuous dynamics of an Unmanned Aerial Vehicle (UAV) incorporating the effect of different forces on the attitude and speed of the Unmanned Vehicle (UV) with reference to time are analyzed to study stability, performance and several other control characteristics of the UAV. This analysis is based on capturing the dynamical behavior of a UAV in term of general Aircraft Equations of Motion (AEoM) containing the effect of the navigation, force, moment and kinematics equations [40]. Moreover, these AEoM, represented as a system of Differential Equations (DEs), requires modeling a coordinate system describing the motion (relative position and movement) of the aircraft in various frames, such as navigation and aircraft's body-fixed frames [14]. Next, these aircraft equations are solved using the Laplace Transform (LT) to get the corresponding Transfer Function (TF), providing a Frequency-domain (FD) representation, or their solutions in time-domain. These results can be further utilized for computing various properties, such as stability, sensitivity and control of UAVs.

The conventional approaches used to study the dynamics of these UAVs are the analytical [12] and computer based simulation techniques [36]. However, the former is subject to human error, specifically, of the larger system. Similarly, the later is based on several procedures existing in the core od the tools that are not verified and are utilized for the dynamical analysis. Therefore, the computer-based simulation methods may compromise the accuracy of the analysis. For example, according to the 2004 report by US department of transportation, 25% of the accidents happened to the US army aircraft, *Shadow* 200 *(RQ-7) Unmanned*, due to the failure of the Tactical Automated Landing System (TALS) [39]. Thus, a rigorous analysis of these UAVs is important, considering the safety-critical nature of UAVs, where these conventional techniques should not be completely relied upon as these may lead to disastrous consequences.

Formal methods [24] are computer-based mathematical methods that can provide a rigorous analysis and have been utilized to cater for the limitations of the above-stated conventional techniques to study the dynamical behaviour of UAVs. Model checking (MC) [10] and Theorem Proving (TP) [22] are two major types of formal methods. MC [10] is based on constructing a mathematical model, using a state diagram, of the given system and the formal verification of its desired behaviour characterized by a temporal logic formula. It has been widely utilized (e.g., [25, 19, 20]) for verifying the dynamics of UAVs. However, it includes discretization of the continuous variables in the model involving differentials and integrals. Moreover, it suffers from the state-space explosion problem [4]. Due to these limitations, the accuracy and completeness of the analysis is somewhat compromised. Higher-order-logic TP [22] includes the construction of a mathematical model of the underlying system in higher-order logic and verification of its desired behaviour using mathematical reasoning within the sound core of a theorem prover. The involvement of the expressive higher-order logic in the construction of a formal model and verification of its corresponding properties of interest within the sound core of a theorem prover guarantees the accuracy and completeness of the associated analysis. Recently, Abed et al. used this method to formally study the continuous dynamics, captured using a set of linear DEs, of UAVs as shown in Figure 1. In particular, the authors formalized several coordinate frames, such as navigation and aircraft's body-fixed frames based on the library of the complex-valued matrices available in the HOL Light theorem prover (HLTP). Moreover, they formalized the AEoM capturing the continuous dynamics of UAVs and formally verified the TF and the FD solutions of the Equations of Motion (EoM) of UAVs using HOL Light (HL). This chapter presents an overview of these efforts, which includes

- the formalization of the coordinate systems
- the formalization of the AEoM and verification of their solutions
- the formal verification of the stability of CropCam UAV using HL
- the highlights of the strengths and weaknesses of the TP approach to study the continuous dynamics of UAVs

The rest of the chapter is organized as follows: The related work on the formal analysis of UAVs is captured in Section 2. Section 3 provides a brief overview of TP,

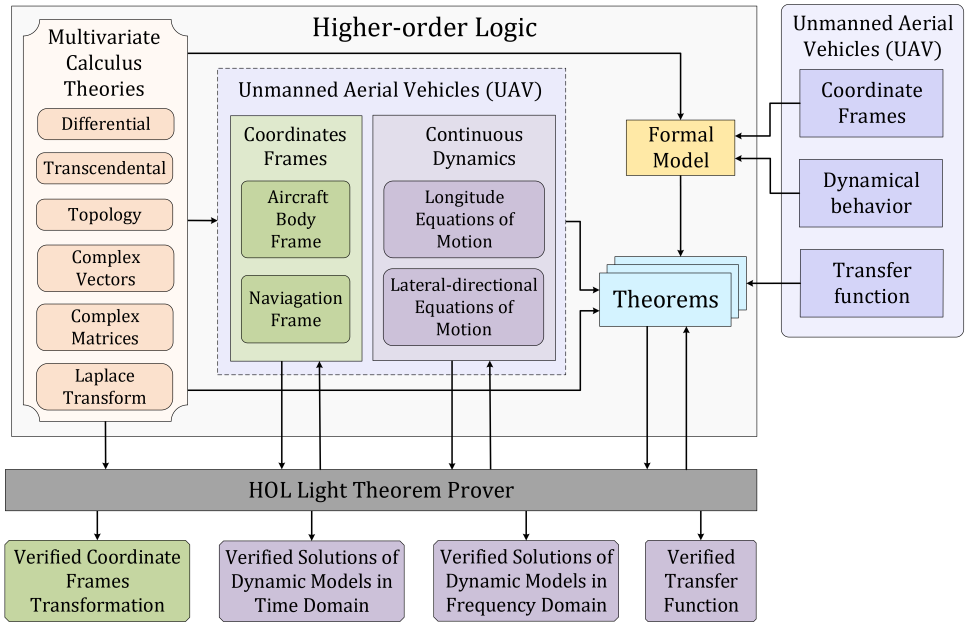

Fig. 1: Proposed Framework

the HLTP, multivariate calculus and the LT theories of HL. The formal verification of various coordinate frames and their transformation, capturing the relative movement and position, of UAVs is presented in Section 4. Section 5 provides the formalization of the AEoM, such as the longitudinal and the Lateral-directional Equations of Motion (LDEoM), captured as a set of linear DEs and the formal verification of their frequency and the time-domain solutions using HL. Section 6 presents the formal stability analysis of CropCam UAV using HL. Some discussion about the higher-order-logic TP based analysis, while highlighting their strengths and weaknesses, is provided in Section 7. Finally, Section 8 concludes the chapter by highlighting some future directions.

2 Related Work

Formal methods, such as MC and higher-order-logic TP have been used for the formal analysis of UAVs. Guzey [20] used Hybrid Automaton (HA) to model the consensus-based formation control of a team of the fixed-wing UAVs flying at a fixed altitude that assists in maintaining their predefined formation and keep them

on track to their destination. Similarly, Seibel et al. [35] proposed a Linear Hybrid Automata (LHA) based framework for flight and mission planning of the rotary-wing UAVs, which incorporates the flight plan of the aircraft, the region of the flight and the meteorological conditions of the flight. Moreover, the authors formally verified the safety and timeliness properties of the LHA based model that helps in increasing the safe flight operation by avoiding any undesired behaviour. Groza et al. [19] formally analyzed UAVs using Hybrid Logic Model Checker (HLMC). The authors constructed a formal Goal Structuring Notation (GSN) model of the aircraft and utilized the description logic for identification of the assurance deficits in the model. Finally, the identified flaws are verified as properties specification in HLMC. Similarly, Karimoddini et al. [25] provided a hybrid approach for modeling and control design of an unmanned helicopter. The authors designed the control structure using multiple layers, namely, motion planning, supervision and the regulation layers, placed in hierarchical form with each layer using a HA. Finally, these layers are synchronized using a compositional operator that is developed as part of the proposed framework.

AJPF, SPIN and PRISM model checkers have also been used for formally analyzing UAVs. Dennis et al. [13] used the autonomous agent language, Gwendolen, for developing a formal model of the Unmanned Aircraft System (UAS) control system and formally verified the model using the agent model checker AJPF. Similarly, Webster et al. [38] used the SPIN model checker for the formal verification of an autonomous UAS. The authors constructed a fundamental control model of the UAS in PROMELA and used the SPIN model checker to formally verify this model against a few subset of rules defined by Civil Aviation Authority (CAA). The authors also captured the probabilistic aspects of UAS by developing a probabilistic model and verified the same set of rules using PRISM. All the MC based analyses, presented above, consider the discrete time models of the aircraft in the form of automata and are unable to capture their continuous dynamics in true form. Moreover, MC suffers from its inherent state-space explosion problem and thus is not well suited for analyzing systems exhibiting the continuous dynamics, which generally leads to large models.

Higher-order-logic theorem provers, such as PVS and Coq theorem provers have been used for formally verifying UAVs. Munoz et al. [31] proposed a Detect and Avoid Alerting Logic for Unmanned Systems (DAIDALUS) and used it for developing the self-separation and alerting algorithms that provide an awareness to UAS remote pilots about any situations. Moreover, the authors formally analyzed these algorithms using PVS. Similarly, Munoz et al. [30] used PVS for formally verifying the extended well-clear boundaries of a UAV that describe the ability of an aircraft to keep itself away from the other aircraft in the airborne traffic to avoid collisions. Similarly, Ghorbal et al. [18] proposed a hybrid TP approach for formally verifying the property of separation between two or more aircraft in the aerospace systems. Narkawicz et al. [32] formally verified a conflict detection algorithms for aircraft flying on arbitrary nonlinear trajectories using PVS. Similarly, Munoz et al. [7] formally verified the correctness of an alerting algorithm for aircraft using the PVS theorem prover. Chen et al. [9] formally verified a control algorithm for automatic

landing of a Helicopter using Coq. Similarly, Ma et al. [28] formally verified the coordinate transformation matrices of the aircraft control system using Coq. Malecha el al. [29] proposed a library, VeriDrone, to formally verify various aspects of CPS. VeriDrone is developed in Coq comprising of theories ranging from floating point numbers to DEs. Similarly, Chan et al. [8] used VeriDrone for formally verifying the stability properties, i.e., Lyapunov and exponential stability, of CPSs.

KeYmaera theorem prover and its various variants have also been used for formally analyzing UAVs. For example, Loos et al. [26] used KeYmaeraD for formally analyzing the control policies for planar aircraft avoidance maneuvers by constructing a formal proof of their safety properties. Arechiga et al. [3] formally verified the closed-loop properties of the control system using KeYmaera. The authors also formally verified the safety of a cooperative intersection collision avoidance system and an intelligent cruise controller. Recently, Abed et al. proposed a higher-order-logic TP based approach for formally analyzing the continuous dynamical behaviour of UAVs. The authors formalized various coordinate frames that captures the relative position and motion of the aircraft, and formally verified their interrelationship using the HLTP. Moreover, they formalized the aircraft's EoM capturing the dynamical behaviour of UAVs and formally verified the TF, and the FD solutions of the EoM of UAVs. The main focus of this chapter is to present the efforts that have been done in this TP based dynamical analysis of UAVs.

3 Higher-order-logic TP and HL

This section includes a brief introduction to the higher-order-logic TP and the HLTP.

3.1 Higher-order-logic TP

Higher-order-logic TP [22] is based on developing a mathematical model of the given system and expressing its desired properties using higher-order logic as shown in Figure 2. In the next step, the relationship between the higher-order logic model and its desired properties is verified as theorems in a theorem prover, which is computer program using deductive reasoning to develop formal proofs using a small set of well-known axioms, inference rules, hypothesis and the already verified theorems. Due to the highly expressiveness of higher-order logic, it enables formal modeling and verification of the continuous dynamics of a system using a higher-order-logic theorem prover. Also, the higher-order logic is undecidable and thus verification of sentences expressed in this logic needs explicit guidance from its user in an interactive manner. Moreover, the involvement of the deductive reasoning in the proof of formal proof development ensure soundness, i.e., every sentence proved in the TP system is actually true.

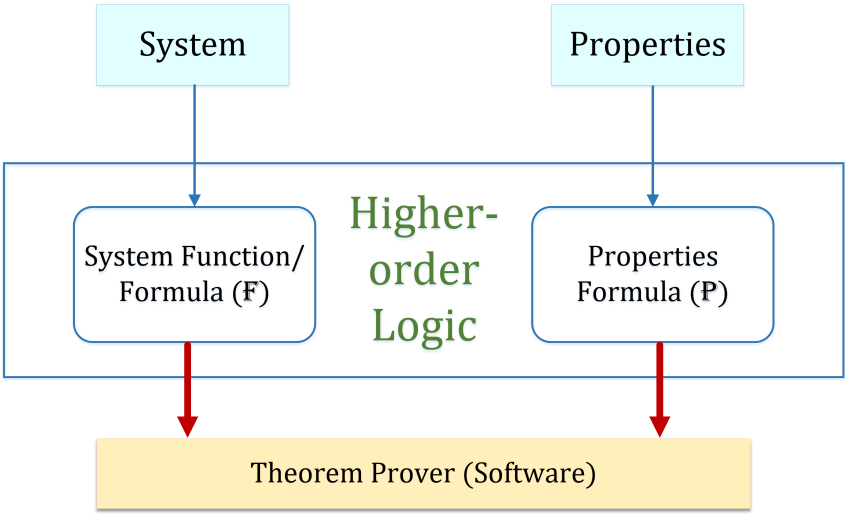

Fig. 2: Higher-order-logic TP

3.2 HLTP

HL [21] is a higher-order-logic TP tool that guarantees secure TP using a strongly-typed functional programming language Objective CAML (OCaml) [33]. HL users can develop higher-order-logic based model of a system and they can interactively verify theorems, capturing the desired properties, by applying the available proof tactics and procedures. A theory in HL comprises of types, constants, definitions and theorems. HL contains a rich set of formalized libraries, such as real arithmetic, multivariate calculus and the LT, which are extensively used in our formalization. Indeed, one of the main motivations for selecting the HLTP for the proposed framework is the availability of the multivariable calculus and the LT theories in HL. There are many automatic proof procedures [23] available in HL, which assist the user in conducting a proof more efficiently.

Table 1 provides some symbols, i.e., their HL and standard representations, and their meanings, which are commonly used in presenting the formal analysis of the dynamical behavior of UAVs in this chapter.

4 Formal Modeling of the Coordinate Systems

Coordinate systems are useful for modeling the position and orientation UAVs at any time instant. The navigation and the aircraft's body-fixed frames are the two commonly used coordinate frames for capturing the dynamics of the aircraft. The

Table 1: HOL Light Symbols

HOL Light Symbols	Standard Symbols	Meanings
/\	and	Logical *and*
\/	or	Logical *or*
~	not	Logical *negation*
==>	$\longrightarrow$	Implication
<=>	$=$	Equality in Boolean domain
!x.t	$\forall x.t$	For all $x : t$
?x.t	$\exists x.t$	There exists $x : t$
λx.t	$\lambda x.t$	Function that maps x to $t(x)$
num	$\{0,1,2,\ldots\}$	Natural numbers data type
real	All Real numbers	Real data type
SUC n	$(n+1)$	Successor of natural number
&a	$\mathbb{N} \rightarrow \mathbb{R}$	Typecasting from natural to real numbers
abs x	$\lvert x \rvert$	Absolute function
EL n l	*element*	n^{th} element of list l

motion of a UAV is generally represented with respect to the navigation coordinate frame (x_n, y_n, z_n), which is oriented as North, East, Down and is attached to earth's local tangent plane as depicted in Figure 3. Moreover, a right-handed orthogonal body coordinate frame (x_b, y_b z_b) is also attached to the aircraft as depicted in Figure 3 and a transformation between these navigation and the aircraft's body-fixed frame is required to efficiently capture the relative motion and the position of the aircraft. The center of mass of the aircraft is located at O_b of the aircraft body-fixed frame. The positive x-axis of the frame is directed forward along the longitudinal axis of the aircraft. Similarly, the positive y-axis is oriented along the right wing of UAV. The positive z-axis is perpendicular to the x and y axes and is pointing downwards from the aircraft as shown in Figure 3.

A point capturing the position and orientation of a UAV in a coordinate system needs to be formalized in order to model the navigation and the aircraft's body-fixed frames. In this regard, the available types, such as Real ($\mathbb{R}$), Complex ($\mathbb{C}$), One-dimensional real-valued vector ($\mathbb{R}^1$)) can be utilized to abbreviate new types. Therefore, the new types for various points are defined using the feature of type abbreviation in HL as follows:

Definition 1. *Points of a Coordinate System*

```
nw_typ_abrv ("1d_pnt",":(ℝ^1 → ℂ)")
nw_typ_abrv ("tmd_1d_pnt",":(1d_pnt × ℝ^1)")
nw_typ_abrv ("2d_pnt",":(1d_pnt × 1d_pnt)")
nw_typ_abrv ("tmd_2d_pnt",":(2d_pnt × ℝ^1)")
nw_typ_abrv ("3d_pnt",":(1d_pnt × 2d_pnt)")
nw_typ_abrv ("tmd_3d_pnt",":(3d_pnt × ℝ^1)")
```

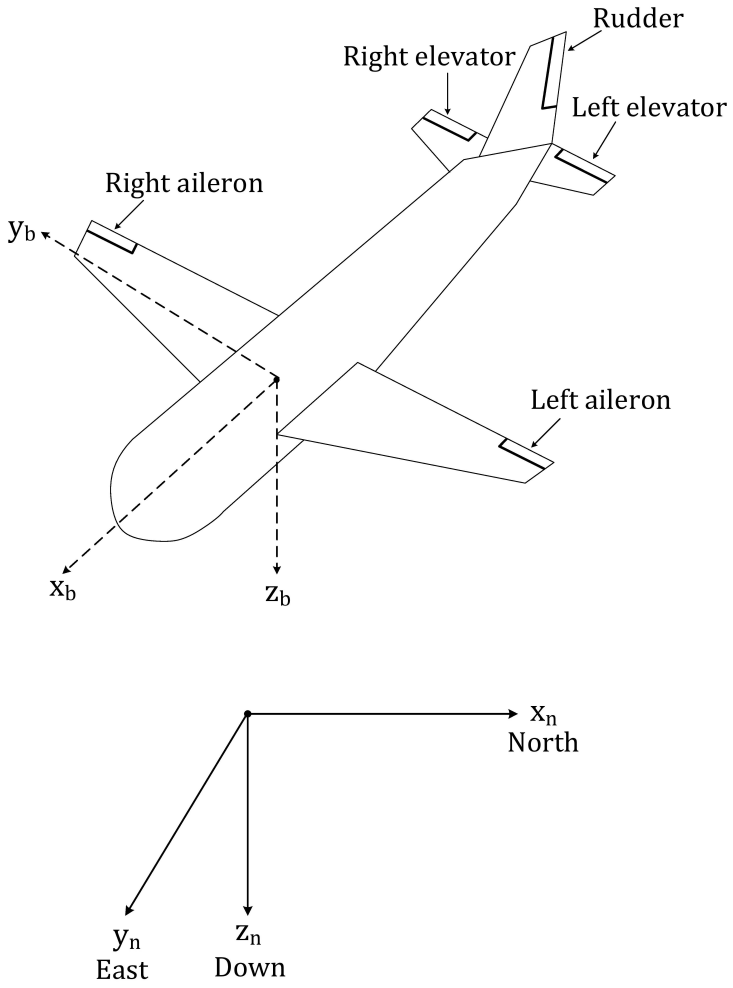

Fig. 3: Aircraft Configuration

The type tmd_1d_pnt is a pair, modeling the orientation and position of a UAV in one-dimensional coordinate system that changes with time, where its second element captures the time. Moreover, the notion of the complex-valued matrices and their various classical properties for the formalization of the coordinate frames are required, which are also formalized as a part of our proposed approach. Some of the verified properties of the complex-valued matrices are given in Table 2. Here, the HL operator %%% models the multiplication of a complex-valued vector with a complex-valued matrix and vice versa. Similarly, cmat 0 captures the complex-valued zero matrix (a matrix having all its entries as zero) of order $M \times N$. The

function cmat 1 represents complex-valued matrix having all its entries as one. Interested users can find more details about the formalization of the complex-valued matrices and formal proofs of their classical properties at [1].

Table 2: Classical Properties of the Complex-valued Matrices

Name	Properties
Commutativity of matrix addition	∀M N. M + N = N + M
Associativity of matrix scalar multiplication	∀m n M. m %%% (n %%% M) = (m ∗ n) %%% M
Right matrix scalar multiplication	∀m M N. M ∗∗ (m %%% N) = m %%% (M ∗∗ N)
Left matrix scalar multiplication	∀m M N. (m %%% M) ∗∗ N = m %%% (M ∗∗ N)
Associativity of matrix addition	∀L M N. L + (M + N) = (L + M) + N
Right Additive identity	∀M. M + cmat 0 = M
Left Additive identity	∀M. cmat 0 + M = M
Right Multiplicative identity	∀M. M ∗ cmat 1 = M
Left Multiplicative identity	∀M. cmat 1 ∗ M = M
Right Multiplicative of zero	∀M. M ∗ cmat 0 = cmat 0
Left Multiplicative of zero	∀M. cmat 0 ∗ M = cmat 0
Right Distributivity of matrix scalar multiplication with respect to addition	∀M N a. a %%% (M + N) = a %%% M + c %%% N
Right Distributivity of matrix scalar multiplication with respect to subtraction	∀M N a. a %%% (M - N) = a %%% M - c %%% N
Left Distributivity of matrix scalar multiplication with respect to addition	∀M m n. (m + n) %%% M = m %%% M + n %%% M
Left Distributivity of matrix scalar multiplication with respect to subtraction	∀M m n. (m - n) %%% M = m %%% M - n %%% M
Associativity of matrix vector multiplication	∀M N y. M ∗∗ N ∗∗ y = (M ∗∗ N) ∗∗ y

The navigation and the aircraft's body-fixed coordinate frames are three-dimensional coordinates and are formally defined in HL as follows:

Definition 2. *Three-dimensional Coordinates*

$\vdash_{def}$ ∀x y z t. **3d_cord_systm** (((x,y,z),t):tmd_3d_pnt) = $\begin{bmatrix} x(t) \\ y(t) \\ z(t) \end{bmatrix}$

The function 3d_cord_systm accepts a variable of data-type *tmd_3d_pnt* and returns a three-dimensional vector capturing the corresponding coordinate frame.

Next, to transform an orientation of the navigation frame to the aircraft's body-fixed frame, a continuous rotation of the navigation frame is done by the Euler angles, which are defined by performing a rotation about the axes of three-dimensional right-handed coordinate system as shown in Figure 4. These Euler angles are formalized using the type abbreviation feature in HL, which are further used for verification of the transformation of the navigation frame to aircraft's body-fixed frame.

Definition 3. *Euler Angles*

nw_typ_abrv ("θ", ':$\mathbb{C}$')
nw_typ_abrv ("ϕ", ':$\mathbb{C}$')
nw_typ_abrv ("ψ", ':$\mathbb{C}$')
nw_typ_abrv ("eulr_angls", ':($\theta \times \phi \times \psi$)')

The complex data-type ($\mathbb{C}$) in HL is selected to formally define the Euler angles, as this choice enables us to formally verify the stability of UAV, which is based on the placement of the poles in the complex plane, as will be described in Section 6 of the chapter. Figure 4 provides the Euler angles and the corresponding frame transformations. A rotation of yaw angle (ψ) about the z_n axes converts the navigation frame to *Intrmdt Frame* 1 defining the aircraft's heading. Next, we rotate the *Intrmdt Frame* 1 by pitch angle (θ) about the new y_1 axis to *Intrmdt Frame* 2. Finally, *Intrmdt Frame* 2 is transformed to the aircraft's body-fixed frame by a rotation of roll angle (ϕ) about the new x_2 axis.

Next, the notion of the rotation matrices for rolling, pitching and yawing is formalized. These matrices provide the orientations of the aircraft with respect to various coordinate frames and are used in the verification of the corresponding transformations from navigation to *Intrmdt Frame* 1, *Intrmdt Frame* 1 to *Intrmdt Frame* 2 and *Intrmdt Frame* 2 to the aircraft's body-fixed frame.

Definition 4. *Rotation Matrices*

$\vdash_{def} \forall \theta\ \psi\ \phi.$ **rotat_matrx_rolng** $(\theta,\psi,\phi) =$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\ \phi & \text{csin}\ \phi \\ 0 & -\sin\ \phi & \cos\ \phi \end{bmatrix}$$

$\vdash_{def} \forall \phi\ \psi\ \theta.$ **rotat_matrx_ptchng** $(\theta,\psi,\phi) =$

$$\begin{bmatrix} \cos\ \theta & 0 & -\sin\ \theta \\ 0 & 1 & 0 \\ \sin\ \theta & 0 & \cos\ \theta \end{bmatrix}$$

$\vdash_{def} \forall \theta\ \phi\ \psi.$ **rotat_matrx_yawng** $(\theta,\psi,\phi) =$

$$\begin{bmatrix} \cos\ \psi & \sin\ \psi & 0 \\ -\sin\ \psi & \cos\ \psi & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Now, the transformation from the navigation frame to *Intrmdt Frame* 1 is verified in HL as follows:

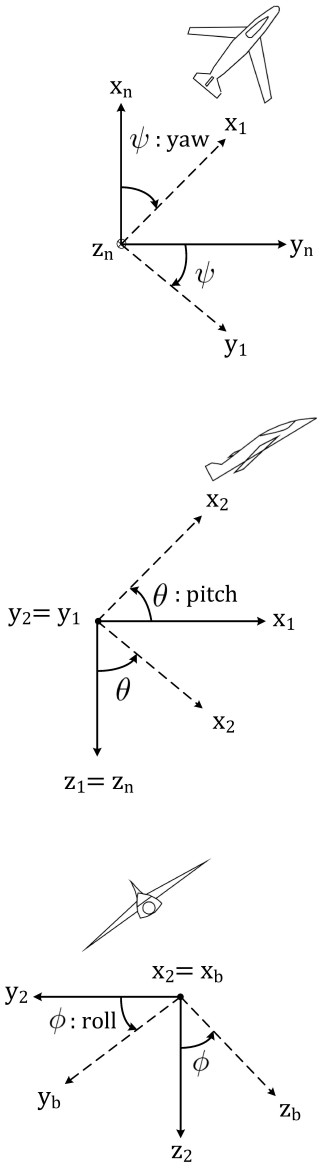

Fig. 4: Euler Angles and Frame Transformation

Theorem 1. Navigation Frame to *Intrmdt Frame* 1

$\vdash_{thm} \forall x_n\ y_n\ z_n\ x_1\ y_1\ z_1\ \theta\ \phi\ \psi$ t. trnsfrm_nvgat_frame_to_intrmd_frame1 (x_1,y_1,z_1)

$$(x_n,y_n,z_n)\ (\theta,\phi,\psi)\ \mathsf{t} \Leftrightarrow \left(\begin{bmatrix} x_1(t) \\ y_1(t) \\ z_1(t) \end{bmatrix} = \begin{bmatrix} x_n(t)\ *\ \cos\ \psi\ +\ y_n(t)\ *\ \sin\ \psi \\ -\ x_n(t)\ *\ \sin\ \psi\ +\ y_n(t)\ *\ \cos\ \psi \\ z_n(t) \end{bmatrix}\right)$$

The function trnsfrm_nvgat_frame_to_intrmd_frame1 captures the corresponding transformation. The proof process of Theorem 1 is mainly based on the properties of complex vectors and matrices, and transcendental functions along with some arithmetic reasoning. In a similar manner, the transformations from *Intrmdt Frame* 1 to aircraft's body-fixed frame are verified in HL as given in Table 3.

Table 3: Verification of Transformation Matrices

Names of Theorems and their Formalized Form
Intermediate Frame 1 *to Intermediate Frame* 2
$\vdash_{thm} \forall x_2\ y_2\ z_2\ x_1\ y_1\ z_1\ \theta\ \phi\ \psi$ t. trnsfrm_intrmd_frame1_intrmd_frame2 (x_2,y_2,z_2) $(x_1,y_1,z_1)\ (\theta,\phi,\psi)\ \mathsf{t} \Leftrightarrow \left(\begin{bmatrix} x_2(t) \\ y_2(t) \\ z_2(t) \end{bmatrix} = \begin{bmatrix} x_1(t)\ *\ \cos\ \theta\ -\ z_1(t)\ *\ \sin\ \theta \\ y_1(t) \\ x_1(t)\ *\ \sin\ \theta\ +\ z_1(t)\ *\ \cos\ \theta \end{bmatrix}\right)$
Intermediate Frame 2 *to Aircraft's Body-fixed Frame*
$\vdash_{thm} \forall x_b\ y_b\ z_b\ x_2\ y_2\ z_2\ \theta\ \phi\ \psi$ t. trnsfrm_intrmd_frame2_aircrft_fxd (x_b,y_b,z_b) $(x_2,y_2,z_2)\ (\theta,\phi,\psi)\ \mathsf{t} \Leftrightarrow \left(\begin{bmatrix} x_b(t) \\ y_b(t) \\ z_b(t) \end{bmatrix} = \begin{bmatrix} x_2(t) \\ y_2(t)\ *\ \cos\ \phi\ +\ z_2(t)\ *\ \sin\ \phi \\ -\ y_2(t)\ *\ \sin\ \phi\ +\ z_2(t)\ *\ \cos\ \phi \end{bmatrix}\right)$

Next, the direction cosine matrix is formalized, which is necessary for the verification of the transformation of the navigation to aircraft's body-fixed frame.

Definition 5. *Direction Cosine Matrix*

$$\vdash_{def} \forall \psi\ \phi\ \theta.\ \textbf{dirctn\_cosne\_mtrx}\ (\theta,\phi,\psi) = \begin{bmatrix} \mathsf{R} & \mathsf{S} & \mathsf{T} \\ \mathsf{U} & \mathsf{V} & \mathsf{W} \\ \mathsf{X} & \mathsf{Y} & \mathsf{Z} \end{bmatrix}$$

where,

R = cos θ $*$ cos ψ
S = cos θ $*$ cos ψ
T = - sin θ
U = sin ϕ $*$ sin θ $*$ cos ψ - cos ϕ $*$ sin ψ
V = sin ϕ $*$ sin θ $*$ sin ψ + cos ϕ $*$ cos ψ
W = sin ϕ $*$ cos θ
X = cos ϕ $*$ sin θ $*$ cos ψ + sin ϕ $*$ sin ψ
Y = cos ϕ $*$ sin θ $*$ sin ψ - sin ϕ $*$ cos ψ
Z = cos ϕ $*$ cos θ

Now, the direction cosine matrix, formalized as Definition 5), is utilized to formally model the transformation from the navigation frame to aircraft's body-fixed frame in HL as:

Definition 6. *Navigation Frame to Aircraft's Body-fixed Frame*

$\vdash \forall x_b\ y_b\ z_b\ x_n\ y_n\ z_n\ \theta\ \phi\ \psi$ t.
trnsfrm_aircrft_fxd_nvgat_frame (x_b,y_b,z_b) (x_n,y_n,z_n) (θ,ϕ,ψ) t $\Leftrightarrow$
(3d_cord_systm $((x_b,y_b,z_b)$, t) =
dirctn_cosne_mtrx (θ,ϕ,ψ) $**$ 3d_cord_systm $((x_n,y_n,z_n)$, t))

Next, the transformation from the navigation to aircraft's body-fixed frame (Definition 6) is formally verified in HL as follows:

Theorem 2. Navigation Frame to Aircraft's Body-fixed Frame

$\vdash \forall x_b\ y_b\ z_b\ x_2\ y_2\ z_2\ x_1\ y_1\ z_1\ x_n\ y_n\ z_n\ \theta\ \phi\ \psi$ t.
[C_1] trnsfrm_nvgat_frame_to_intrmd_frame1 (x_1,y_1,z_1) (x_n,y_n,z_n) (θ,ϕ,ψ) t $\wedge$
[C_2] trnsfrm_intrmd_frame1_intrmd_frame2 (x_2,y_2,z_2) (x_1,y_1,z_1) (θ,ϕ,ψ) t $\wedge$
[C_3] trnsfrm_intrmd_frame2_aircrft_fxd (x_b,y_b,z_b) (x_2,y_2,z_2) (θ,ϕ,ψ) t
$\Rightarrow$ trnsfrm_aircrft_fxd_nvgat_frame (x_b,y_b,z_b) (x_n,y_n,z_n) (θ,ϕ,ψ) t

Conditions C_1, C_2 and C_3 provide the transformations from the navigation frame to *Intrmdt Frame* 1, *Intrmdt Frame* 1 to *Intrmdt Frame* 2 and *Intrmdt Frame* 2 to aircraft's body-fixed frame, respectively. The conclusion captures the transformation of the navigation frame to aircraft's body-fixed frame. The verification of Theorem 2 is mainly based on Theorem 1, theorems given in Table 3 and the properties of complex matrices and vectors alongside some arithmetic reasoning. This concludes the formalization of the coordinate frames and verification of their transformation. Further details about the formalization can be found at [1].

5 Formal Verification of the Dynamics of UAVs

This section provides the formal verification of the continuous dynamical behaviour of UAVs, which includes the formalization of the longitudinal and LDEoM (set of

the DEs) capturing the dynamics of the aircraft, and the verification of their FD solutions. These equations are developed by the application of the physical and mathematical laws regarding force and inertia, providing a relationship between the input and output variables of the aircraft as depicted in Figure 5. Since multiple input and output variables are involved for capturing the dynamics of the underlying system, therefore, it is declared as a MIMO system. To formally verify these equations in the HLTP, first, various parameters involved in the development of these equations, such as velocities, force and the moment of inertia etc needs to be incorporated.

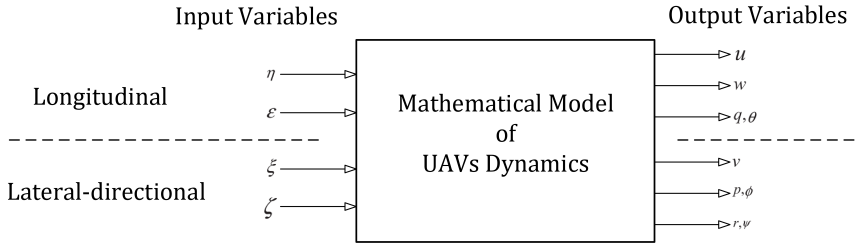

Fig. 5: UAV Input-output Relationship

First, the linear and angular disturbance velocities are modelled using the feature of type abbreviation in HL as follows:

Definition 7. *Linear Disturbance Velocities*

nw_typ_abrv ("u", ':$\mathbb{R}^1 \to \mathbb{C}$')
nw_typ_abrv ("v", ':$\mathbb{R}^1 \to \mathbb{C}$')
nw_typ_abrv ("w", ':$\mathbb{R}^1 \to \mathbb{C}$')
nw_typ_abrv ("linr_dstrbnc_veloc", ':$(\theta \times \phi \times \psi)$')

Definition 8. *Angular Disturbance Velocities*

nw_typ_abrv ("p", ':$\mathbb{R}^1 \to \mathbb{C}$')
nw_typ_abrv ("q", ':$\mathbb{R}^1 \to \mathbb{C}$')
nw_typ_abrv ("r", ':$\mathbb{R}^1 \to \mathbb{C}$')
nw_typ_abrv ("anglr_dstrbnc_veloc", ':$(\theta \times \phi \times \psi)$')

where each component of the linear and angular disturbance velocities is a function of type $\mathbb{R}^1 \to \mathbb{C}$. Similarly, the aerodynamics stability derivatives represent constant values of type $\mathbb{C}$ for the linear LEOM of UAVs, as presented in Table 4. These derivatives for the axial force, normal force and the pitching moment are modeled using type abbreviations in HL as follows:

Definition 9. *Aerodynamics Stability Derivatives*

nw_typ_abrv ("arodyn_stbl_dervt_axl_frce", ':
$(X_u \times X_v \times X_w \times X_{wd} \times X_q \times X_\eta \times X_\tau)$')
nw_typ_abrv ("arodyn_stbl_dervt_nrml_frce", ':

Table 4: Aerodynamics Stability Derivatives and their Data-types

Symbol	Type	Symbol	Type	Symbol	Type
X_u	$\mathbb{C}$	Z_w	$\mathbb{C}$	M_u	$\mathbb{C}$
X_w	$\mathbb{C}$	Z_{wd}	$\mathbb{C}$	M_w	$\mathbb{C}$
X_{wd}	$\mathbb{C}$	Z_q	$\mathbb{C}$	M_{wd}	$\mathbb{C}$
X_q	$\mathbb{C}$	Z_u	$\mathbb{C}$	M_q	$\mathbb{C}$
X_v	$\mathbb{C}$	Z_τ	$\mathbb{C}$	M_η	$\mathbb{C}$
X_τ	$\mathbb{C}$	Z_η	$\mathbb{C}$	M_τ	$\mathbb{C}$
X_η	$\mathbb{C}$				

$(Z_u \times Z_w \times Z_{wd} \times Z_q \times Z_\eta \times Z_\tau)$‘)

nw_typ_abrv (”arodyn_stbl_dervt_pitchng_momnt”, ‘:
$(M_u \times M_w \times M_{wd} \times M_q \times M_\eta \times M_\tau)$‘)

Similarly, the linear velocity and moment of inertia of UAVs are modelled using the type abbreviation feature of HL as follows:

Definition 10. *Linear Velocity*

nw_typ_abrv (”U_e”, ‘:$\mathbb{C}$‘)
nw_typ_abrv (”V_e”, ‘:$\mathbb{C}$‘)
nw_typ_abrv (”W_e”, ‘:$\mathbb{C}$‘)
nw_typ_abrv (”lnr_vlcty”, ‘:$(U_e \times V_e \times W_e)$‘)

Definition 11. *Moment of Inertia*

nw_typ_abrv (”I_x”, ‘:$\mathbb{C}$‘)
nw_typ_abrv (”I_y”, ‘:$\mathbb{C}$‘)
nw_typ_abrv (”I_z”, ‘:$\mathbb{C}$‘)
nw_typ_abrv (”momnt_of_inrtia”, ‘:$(I_x \times I_y \times I_z)$‘)

where U_e, V_e and W_e capture the axial, lateral and normal velocities, respectively. Similarly, I_x, I_y and I_z model the x, y and z components of the moment of inertia, respectively.

The motion of a UAV is generally described by decoupled equations of motion [11], such as longitudinal and LDEoM. The LEoM for the aircraft are described by the axial force (X), the normal force (Z) and the pitching moment (M) and are mathematical described as [11, 40]:

$$\begin{aligned} m\dot{u} - X_u u - X_{\dot{w}}\dot{w} - X_w w - (X_q - mW_e)q + mg\theta cos\theta_e = X_\eta \eta + X_\tau \tau \\ -Z_u u + (m - Z_{\dot{w}})\dot{w} - Z_w w - (Z_q + mU_e)q + mg\theta sin\theta_e = Z_\eta \eta + Z_\tau \tau \\ M_u u - M_{\dot{w}}\dot{w} - M_w w + I_y\dot{q} - M_q q = M_\eta \eta + M_\tau \tau \end{aligned} \quad (1)$$

where $\dot{u}$, $\dot{w}$ and $\dot{q}$ represent the first order-derivatives of the linear and angular disturbance velocities, respectively. Similarly, m, θ_e and g are the total mass of the UAV,

the steady pitch attitude of the UAV and the acceleration due to gravity, respectively. The variables η and τ model the elevator angle and thrust, respectively. Under the conditions $q(t) = \dot{\theta}(t)$ and $\tau(t) = 0$, the above LEoM of the UAV become [11]:

$$\begin{aligned} m\dot{u} - X_u u - X_{\dot{w}}\dot{w} - X_w w - (X_q - mW_e)\dot{\theta} + mg\theta cos\theta_e = X_\eta \eta \\ -Z_u u + (m - Z_{\dot{w}})\dot{w} - Z_w w - (Z_q + mU_e)\dot{\theta} + mg\theta sin\theta_e = Z_\eta \eta \\ M_u u - M_{\dot{w}}\dot{w} - M_w w + I_y\ddot{\theta} - M_q\dot{\theta} = M_\eta \eta \end{aligned} \tag{2}$$

In order to model the above set of linear DEs, first, a linear Differential Equation (DE) of order n is formalized as follows:

Definition 12. *DE of Order n*

$\vdash_{def}$ $\forall$n lst f t. **n_ord_diffren_equat** n L f t = $\sum_0^n$ (λk. EL k L $*$ $\frac{d^k f(t)}{dt}$)

The function n_ord_diffren_equat accepts the order of the DE n, a list of constant coefficients L, a differentiable function f and the differentiation variable t and return a DE of order n. It uses the function EL k L, which returns the k^{th} element of a list L, to generate the DE corresponding to the given parameters.

The first DE of the LEoM (Equation (2)) is formalized in HL as follows:

Definition 13. *LEoM* 1

$\vdash_{def}$ $\forall X_v\ X_w\ X_{wd}\ X_q\ X_\eta\ X_\tau\ X_u$ m.
list_u_longtnl_eqtn_motn_fst m (X_u,X_v, X_w, X_{wd}, X_q, X_η, X_τ) = [-X_u; m]

$\vdash_{def}$ $\forall X_u\ X_v\ X_q\ X_\eta\ X_\tau\ X_w\ X_{wd}$.
list_w_longtnl_eqtn_motn_fst (X_u,X_v, X_w, X_{wd}, X_q, X_η, X_τ) = [X_w; X_{wd}]

$\vdash_{def}$ $\forall X_u\ X_v\ X_w\ X_{wd}\ X_\eta\ X_\tau\ U_e\ V_e$ g $\theta_e\ X_q$ m W_e.
list_thta_longtnl_eqtn_motn_fst m g θ_e
(X_u,X_v, X_w, X_{wd}, X_q, X_η, X_τ) (U_e,V_e,W_e) = [-(m $*$ g $*$ cos θ_e); X_q - m $*$ W_e]

$\vdash_{def}$ $\forall X_u\ X_v\ X_w\ X_{wd}\ X_q\ X_\tau\ X_\eta$.
list_eta_longtnl_eqtn_motn_fst (X_u,X_v, X_w, X_{wd}, X_q, X_η, X_τ) = [X_η]

$\vdash_{def}$ $\forall$p q r v u w m g $\theta_e\ U_e\ V_e\ W_e\ \theta\ X_u\ X_v\ X_w\ X_{wd}\ X_q\ X_\eta\ X_\tau\ \eta$ t.
longtnl_eqtn_motn_fst (X_u,X_v, X_w, X_{wd}, X_q, X_η, X_τ)
(U_e,V_e,W_e) m g θ_e (p,q,r) (u,v,w) θ η t $\Leftrightarrow$
n_ord_diffren_equat 1
(list_u_longtnl_eqtn_motn_fst m (X_u,X_v, X_w, X_{wd}, X_q, X_η, X_τ)) u t -
n_ord_diffren_equat 1
(list_w_longtnl_eqtn_motn_fst (X_u,X_v, X_w, X_{wd}, X_q, X_η, X_τ)) w t -
n_ord_diffren_equat 1
(list_thta_longtnl_eqtn_motn_fst m g thetae (X_u,X_v, X_w, X_{wd}, X_q, X_η, X_τ)
(U_e,V_e,W_e)) θ t =
n_ord_diffren_equat 0
(list_eta_longtnl_eqtn_motn_fst (X_u,X_v, X_w, X_{wd}, X_q, X_η, X_τ)) η t

where the function longtnl_eqtn_motn_fst accepts the function variables u, w, θ and η and the lists of coefficients list_u_longtnl_eqtn_motn_fst, list_w_longtnl_eqtn_motn_fst,

list_thta_longtnl_eqtn_motn_fst and list_eta_longtnl_eqtn_motn_fst and returns the corresponding DE. Similarly, the other two DEs of the LEoM (Equation (2)) are modelled as follows:

Definition 14. *LEoM* 2

$\vdash_{def}$ $\forall Z_w\ Z_{wd}\ Z_q\ Z_\eta\ Z_\tau\ Z_u$.
list_u_longtnl_eqtn_motn_snd $(Z_u,Z_w,Z_{wd},Z_q,Z_\eta,Z_\tau)$ = [-Z_u]

$\vdash_{def}$ $\forall Z_u\ Z_q\ Z_\eta\ Z_\tau\ Z_w$ m Z_{wd}.
list_w_longtnl_eqtn_motn_snd m $(Z_u,Z_w,Z_{wd},Z_q,Z_\eta,Z_\tau)$ = [Z_w; -(m - Z_{wd})]

$\vdash_{def}$ $\forall Z_u\ Z_w\ Z_{wd}\ Z_\eta\ Z_\tau\ U_e\ W_e$ g $\theta_e\ Z_q$ m V_e.
list_thta_longtnl_eqtn_motn_snd m g θ_e $(Z_u,Z_w,Z_{wd},Z_q,Z_\eta,Z_\tau)$
(U_e,V_e,W_e) = [-(m $*$ g $*$ sin θ_e); Z_q + m $*$ V_e]

$\vdash_{def}$ $\forall Z_u\ Z_w\ Z_{wd}\ Z_q\ Z_\eta\ Z_\tau$.
list_eta_longtnl_eqtn_motn_snd $(Z_u,Z_w,Z_{wd},Z_q,Z_\eta,Z_\tau)$ = [Z_η]

$\vdash_{def}$ $\forall$p q r v u w m g $\theta_e\ U_e\ V_e\ W_e\ \theta\ Z_u\ Z_w\ Z_{wd}\ Z_q\ Z_\eta\ Z_\tau\ \eta$ t.
longtnl_eqtn_motn_snd
$(Z_u,Z_w,Z_{wd},Z_q,Z_\eta,Z_\tau)$ (U_e,V_e,W_e) m g θ_e (p,q,r) (u,v,w) $\theta\ \eta$ t $\Leftrightarrow$
n_ord_diffren_equat 0
(list_u_longtnl_eqtn_motn_snd $(Z_u,Z_w,Z_{wd},Z_q,Z_\eta,Z_\tau)$) u t -
n_ord_diffren_equat 1
(list_w_longtnl_eqtn_motn_snd $(Z_u,Z_w,Z_{wd},Z_q,Z_\eta,Z_\tau)$) w t -
n_ord_diffren_equat 1
(list_thta_longtnl_eqtn_motn_snd m g thetae $(Z_u,Z_w,Z_{wd},Z_q,Z_\eta,Z_\tau)$
(U_e,V_e,W_e)) θ t =
n_ord_diffren_equat 0
(list_eta_longtnl_eqtn_motn_snd $(Z_u,Z_w,Z_{wd},Z_q,Z_\eta,Z_\tau)$) η t

Definition 15. *LEoM* 3

$\vdash_{def}$ $\forall M_w\ M_{wd}\ M_q\ M_\eta\ M_\tau\ M_u$.
list_u_longtnl_eqtn_motn_trd $(M_u,M_w,M_{wd},M_q,M_\eta,M_\tau)$ = [-M_u]

$\vdash_{def}$ $\forall M_w\ M_{wd}\ M_q\ M_\eta\ M_\tau\ M_u$.
list_w_longtnl_eqtn_motn_trd $(M_u,M_w,M_{wd},M_q,M_\eta,M_\tau)$ = [M_w; M_{wd}]

$\vdash_{def}$ $\forall M_w\ M_{wd}\ M_q\ M_\eta\ M_\tau\ M_u\ I_x\ I_z\ I_y$.
list_thta_longtnl_eqtn_motn_trd $(M_u,M_w,M_{wd},M_q,M_\eta,M_\tau)$
(I_x,I_y,I_z) = [0; -M_q; I_y]

$\vdash_{def}$ $\forall M_w\ M_{wd}\ M_q\ M_\eta\ M_\tau\ M_u$.
list_eta_longtnl_eqtn_motn_trd $(M_u,M_w,M_{wd},M_q,M_\eta,M_\tau)$ = [M_η]

$\vdash_{def}$ $\forall$Ue Ve We v u w Ix Iy Iz theta $M_w\ M_{wd}\ M_q\ M_\eta\ M_\tau\ M_u\ \eta$ t.
longtnl_eqtn_motn_trd
$(M_u,M_w,M_{wd},M_q,M_\eta,M_\tau)$ (U_e,V_e,W_e) (u,v,w) (I_x,I_y,I_z) $\theta\ \eta$ t $\Leftrightarrow$
n_ord_diffren_equat 0
(list_u_longtnl_eqtn_motn_trd $(M_u,M_w,M_{wd},M_q,M_\eta,M_\tau)$) u t -
n_ord_diffren_equat 1
(list_w_longtnl_eqtn_motn_trd $(M_u,M_w,M_{wd},M_q,M_\eta,M_\tau)$) w t +
n_ord_diffren_equat 2
(list_thta_longtnl_eqtn_motn_trd $(M_u,M_w,M_{wd},M_q,M_\eta,M_\tau)$ (I_x,I_y,I_z)) θ t =

n_ord_diffren_equat 0
(list_eta_longtnl_eqtn_motn_trd (M_u,M_w,M_{wd},M_q,M_η,M_τ)) η t

Next, the LT of the LEoM, described by Equation (2), is taken to compute the TF of the UV corresponding to its various inputs and outputs.

$$\begin{aligned}(ms-X_u)u(s)-(X_{\dot{w}}ws+X_w)w(s)-((X_q-mW_e)s-mgcos\theta_e)\theta(s)&=X_\eta\,\eta(s)\\ -Z_u u(s)-((Z_{\dot{w}}-m)s+Z_w)w(s)-((Z_q+mU_e)s+mgsin\theta_e)\theta(s)&=Z_\eta\,\eta(s)\\ M_u u(s)-(M_{\dot{w}}s+M_w)w(s)+(I_y s^2-M_q s)\theta(s)&=M_\eta\,\eta(s)\end{aligned} \quad (3)$$

The LT of the LEoM of the aircraft (Equation 3) is verified as follows:

Theorem 3. LT of the LEoM

$\vdash_{thm}$ ∀s u v w θ η U_e V_e W_e Z_q Z_τ Z_u Z_w Z_{wd} Z_η g m p q r θ_e.
[C_1] (∀t. $\frac{du}{dt}$ diff_at t) ∧
[C_2] (∀t. $\frac{dw}{dt}$ diff_at t) ∧
[C_3] (∀t. $\frac{d^2\theta}{dt^2}$ diff_at t) ∧
[C_4] (∀t. η diff_at t) ∧
[C_5] zero_intl_cndtns 0 u ∧
[C_6] zero_intl_cndtns 0 w ∧
[C_7] zero_intl_cndtns 1 θ ∧
[C_8] &0 < m ∧
[C_9] &0 < g ∧
[C_{10}] laplc_exst $\frac{du}{dt}$ s ∧
[C_{11}] laplc_exst $\frac{dw}{dt}$ s ∧
[C_{12}] laplc_exst $\frac{d^2\theta}{dt^2}$ s ∧
[C_{13}] laplc_exst η s ∧
[C_{14}] (∀t. longtnl_eqtn_motn_fst (X_u,X_v, X_w, X_{wd}, X_q, X_η, X_τ) (U_e,V_e,W_e)
m g θ_e (p,q,r) (u,v,w) θ η t) ∧
[C_{15}] (∀t. longtnl_eqtn_motn_snd (Z_u,Z_w,Z_{wd},Z_q,Z_η,Z_τ) (U_e,V_e,W_e)
m g θ_e (p,q,r) (u,v,w) θ η t) ∧
[C_{16}] (∀t. longtnl_eqtn_motn_trd (M_u,M_w,M_{wd},M_q,M_η,M_τ) (U_e,V_e,W_e)
(u,v,w) (I_x,I_y,I_z) θ η t)
⇒ laplc_trnsfm_longtnl_eqtn_motn_fst (X_u,X_v, X_w, X_{wd}, X_q, X_η, X_τ) (U_e,V_e,W_e)
m g θ_e (u,v,w) θ η s ∧
laplc_trnsfm_longtnl_eqtn_motn_snd (Z_u,Z_w,Z_{wd},Z_q,Z_η,Z_τ) (U_e,V_e,W_e)
m g θ_e (u,v,w) θ η s ∧
laplc_trnsfm_longtnl_eqtn_motn_trd (M_u,M_w,M_{wd},M_q,M_η,M_τ) (U_e,V_e,W_e)
(I_x,I_y,I_z) θ η s

Conditions C_1-C_4 capture the differentiability of the higher-order derivatives of the input and outputs u, w, θ and η up to the order 1, 1, 2 and 0, respectively. Similarly,

Conditions C_5-C_7 provide the *zero initial conditions* for the functions u, w and θ, respectively. Conditions C_8-C_9 present the positivity of the mass of the aircraft m and acceleration due to gravity g. Conditions C_{10}- C_{13} assert that the LT of the functions u, w, θ and η exist up to the order 1, 1, 2 and 0, respectively. The last three conditions C_{14}- C_{16} describe the LEoM of the UAV. The verification of the above theorem is mainly based on the following Lemma along with some arithmetic reasoning.

Lemma 1. LT of the Generalized Equation of Motion of Aircraft

$\vdash_{thm}$ ∀z y x w m n p q fslst snlst trlst ftlst s.
[C_1] (∀t. $\frac{d^m w}{dt^m}$ diff_at t) ∧
[C_2] (∀t. $\frac{d^n x}{dt^n}$ diff_at t) ∧
[C_3] (∀t. $\frac{d^p y}{dt^p}$ diff_at t) ∧
[C_4] (∀t. $\frac{d^q z}{dt^q}$ diff_at t) ∧
[C_5] (0 < m ⇒ zero_intl_cndtns (m - 1) w) ∧
[C_6] (0 < n ⇒ zero_intl_cndtns (n - 1) w) ∧
[C_7] (0 < p ⇒ zero_intl_cndtns (p - 1) w) ∧
[C_8] (0 < q ⇒ zero_intl_cndtns (q - 1) w) ∧
[C_9] laplc_exst $\frac{d^m w}{dt^m}$ s ∧
[C_{10}] laplc_exst $\frac{d^n x}{dt^n}$ s ∧
[C_{11}] laplc_exst $\frac{d^p y}{dt^p}$ s ∧
[C_{12}] laplc_exst $\frac{d^q z}{dt^q}$ s ∧
[C_{13}] (∀t. diffren_equat_uav_gnrlzd m n p q fslst snlst trlst ftlst w x y z
⇒ laplc_trnsfrm w s ∗ $\sum_0^m$ (λk. EL k fslst ∗ s^k) +
laplc_trnsfrm x s ∗ $\sum_0^n$ (λk. EL k snlst ∗ s^k) +
laplc_trnsfrm y s ∗ $\sum_0^p$ (λk. EL k trlst ∗ s^k) =
laplc_trnsfrm z s ∗ $\sum_0^q$ (λk. EL k ftlst ∗ s^k)

Conditions C_1-C_4, C_5-C_8 and C_9-C_{12} are similar to Conditions C_1-C_4, C_5-C_7 and C_{10}-C_{13} of Theorem 3. For example, C_9-C_{12} of Lemma 1 provide the Laplace existence condition for the functions w, x, y and z exist up to the order m, n, p and q, respectively. Assumption C_{13} captures the DE modeling a generic equation of motion of UAV acting as a MIMO system and is formalized in HL as Definition 16. The formal proof of the above lemma is mainly based on the classical properties of the LT along with some complex arithmetic reasoning.

Definition 16. *Generic DE of Aircraft (MIMO System)*

$\vdash_{def}$ ∀m fslst w n snlst x p trlst y q ftlst z.
diffren_equat_uav_genrc m n p q fslst snlst trlst ftlst w x y z ⇔
(n_ord_diffren_equat m fslst w t + n_ord_diffren_equat n snlst x t +
n_ord_diffren_equat p trlst y t = n_ord_diffren_equat q ftlst z t)

Next, the LT of the LEoM (Equation (3)) is written in matrix form as:

$$\begin{bmatrix} (ms-X_u) & -(X_{\dot{w}}ws+X_w) & -((X_q-mW_e)s-mgcos\theta_e) \\ -Z_u & -((Z_{\dot{w}}-m)s+Z_w) & -((Z_q+mU_e)s+mgsin\theta_e) \\ M_u & -(M_{\dot{w}}s+M_w) & (I_ys^2-M_qs) \end{bmatrix} \begin{bmatrix} u(s) \\ w(s) \\ \theta(s) \end{bmatrix} = \begin{bmatrix} X_\eta\,\eta(s) \\ Z_\eta\,\eta(s) \\ M_\eta\,\eta(s) \end{bmatrix} \tag{4}$$

By applying the Crammer's rule, the TF of the UV for various inputs and outputs corresponding to the LEoM can be mathematically described as:

$$\frac{u(s)}{\eta(s)} \equiv \frac{N^u_\eta(s)}{\Delta_{lon}(s)}\ \frac{w(s)}{\eta(s)} \equiv \frac{N^w_\eta(s)}{\Delta_{lon}(s)}\ \frac{\theta(s)}{\eta(s)} \equiv \frac{N^\theta_\eta(s)}{\Delta_{lon}(s)} \tag{5}$$

where

$$N^u_\eta(s) = \begin{vmatrix} X_\eta & -(X_{\dot{w}}ws+X_w) & -((X_q-mW_e)s-mgcos\theta_e) \\ Z_\eta & -((Z_{\dot{w}}-m)s+Z_w) & -((Z_q+mU_e)s+mgsin\theta_e) \\ M_\eta & -(M_{\dot{w}}s+M_w) & (I_ys^2-M_qs) \end{vmatrix}$$

$$N^w_\eta(s) = \begin{vmatrix} (ms-X_u) & X_\eta & -((X_q-mW_e)s-mgcos\theta_e) \\ -Z_u & Z_\eta & -((Z_q+mU_e)s+mgsin\theta_e) \\ M_u & M_\eta & (I_ys^2-M_qs) \end{vmatrix}$$

$$N^\theta_\eta(s) = \begin{vmatrix} (ms-X_u) & -(X_{\dot{w}}ws+X_w) & X_\eta \\ -Z_u & -((Z_{\dot{w}}-m)s+Z_w) & Z_\eta \\ M_u & -(M_{\dot{w}}s+M_w) & M_\eta \end{vmatrix}$$

$$\Delta_{lon}(s) = \begin{vmatrix} (ms-X_u) & -(X_{\dot{w}}ws+X_w) & -((X_q-mW_e)s-mgcos\theta_e) \\ -Z_u & -((Z_{\dot{w}}-m)s+Z_w) & -((Z_q+mU_e)s+mgsin\theta_e) \\ M_u & -(M_{\dot{w}}s+M_w) & (I_ys^2-M_qs) \end{vmatrix}$$

The TF $\eta(s)/u(s)$ for the input $\eta(t)$ and output $u(t)$ is verified in HL as the following theorem:

Theorem 4. TF $\eta(s)/u(s)$ for the Input $\eta(t)$ and Output $u(t)$

$\vdash_{thm} \forall I_x\ I_y\ I_z\ M_\eta\ M_q\ M_\tau\ M_u\ M_w\ M_{wd}\ U_e\ V_e\ W_e\ X_\eta\ X_q\ X_\tau\ X_u\ X_v\ X_w\ X_{wd}\ Z_\eta\ Z_q\ Z_\tau\ Z_u\ Z_w\ Z_{wd}\ \eta$ g m s θ θ_e u v w.

$[C_1]$ ($\forall$t. $\frac{du}{dt}$ diff_at t) $\wedge$
$[C_2]$ ($\forall$t. $\frac{dw}{dt}$ diff_at t) $\wedge$
$[C_3]$ ($\forall$t. $\frac{d^2\theta}{dt^2}$ diff_at t) $\wedge$
$[C_4]$ ($\forall$t. η diff_at t) $\wedge$
$[C_5]$ zero_intl_cndtns 0 u $\wedge$
$[C_6]$ zero_intl_cndtns 0 w $\wedge$
$[C_7]$ zero_intl_cndtns 1 θ $\wedge$
$[C_8]$ &0 $<$ m $\wedge$
$[C_9]$ &0 $<$ g $\wedge$
$[C_{10}]$ laplc_exst $\frac{du}{dt}$ s $\wedge$
$[C_{11}]$ laplc_exst $\frac{dw}{dt}$ s $\wedge$
$[C_{12}]$ laplc_exst $\frac{d^2\theta}{dt^2}$ s $\wedge$
$[C_{13}]$ laplc_exst η s $\wedge$
$[C_{14}]$ nz_dnmntr_cndtn (X_u,X_v,X_w,X_{wd},X_q, X_η, X_τ) (Z_u,Z_w,Z_{wd},Z_q,Z_η,Z_τ)
(M_u,M_w,M_{wd},M_q,M_η,M_τ) (U_e,V_e,W_e) m g θ_e (u,v,w) (I_x,I_y,I_z) θ η s $\wedge$
$[C_{15}]$ ($\forall$t. longtnl_eqtn_motn_fst (X_u,X_v, X_w, X_{wd}, X_q, X_η, X_τ) (U_e,V_e,W_e)
m g θ_e (p,q,r) (u,v,w) θ η t) $\wedge$
$[C_{16}]$ ($\forall$t. ($\forall$t. longtnl_eqtn_motn_snd (Z_u,Z_w,Z_{wd},Z_q,Z_η,Z_τ) (U_e,V_e,W_e)
m g θ_e (p,q,r) (u,v,w) θ η t) $\wedge$
$[C_{17}]$ ($\forall$t. longtnl_eqtn_motn_trd (M_u,M_w,M_{wd},M_q,M_η,M_τ) (U_e,V_e,W_e)
(u,v,w) (I_x,I_y,I_z) θ η t)
$\Rightarrow$ laplc_trnsfm u s / laplc_trnsfm η s =
cdet (lngtd_nmrtr_polyn_mtrx_uη (X_u,X_v, X_w, X_{wd}, X_q, X_η, X_τ)
(Z_u,Z_w,Z_{wd},Z_q,Z_η,Z_τ) (M_u,M_w,M_{wd},M_q,M_η,M_τ) (U_e,V_e,W_e)
m g θ_e (u,v,w) (I_x,I_y,I_z) θ η s) /
cdet (lt_lngtd_eqtn_mtrx (X_u,X_v, X_w, X_{wd}, X_q, X_η, X_τ) (Z_u,Z_w,Z_{wd},Z_q,Z_η,Z_τ)
(M_u,M_w,M_{wd},M_q,M_η,M_τ) (U_e,V_e,W_e) m g θ_e (u,v,w) (I_x,I_y,I_z) θ η s)

where cdet models the determinant of a complex valued square matrix. Conditions C_1-C_{13} are same as that of Theorem 3. Condition C14 ensures that the denominators of the TF expression are non-zero. Conditions C_{15}-C_{17} present the LEoM of the aircraft. The verification of Theorem 4 is mainly based on Theorem 3, properties of complex matrices and vectors along with the following lemma regarding application of the Crammer's rule.

Lemma 2. Application of Crammer's Rule on a Matrix Representation
$\vdash_{thm}$ $\forall$a b c d e f g h i u w z n p q r.

$$[C_1] \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} ** \begin{bmatrix} \frac{u}{n} \\ \frac{w}{n} \\ \frac{z}{n} \end{bmatrix} = \begin{bmatrix} p \\ q \\ r \end{bmatrix} \wedge$$

$[C_2]$ n $\neq$ 0 $\wedge$

$$[C_3]\ a * d \neq 0 \wedge$$
$$[C_4]\ a * g \neq 0 \wedge$$
$$[C_5]\ d * g \neq 0 \wedge$$
$$[C_6]\ b * d * g - a * d * h \neq 0 \wedge$$
$$[C_7]\ b * d * g - a * e * g \neq 0 \wedge$$
$$[C_8]\ a * e * i - a * f * h - b * d * i + b * f * g + c * d * h - c * e * g = 0$$
$$[C_9]\ (b * d * g - a * d * h) * (c * d * g - a * f * g) - (b * d * g - a * e * g) * (c * d * g - a * d * i) \neq 0 \wedge$$
$$\Rightarrow \frac{u}{n} = \frac{\mathrm{cdet}\begin{bmatrix} p & b & c \\ q & e & f \\ r & h & i \end{bmatrix}}{\mathrm{cdet}\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}}$$

Condition C_1 captures the matrix representation of the DEs modeling the continuous dynamical behavior of a system. Conditions C_2-C_9 assert the non-zero conditions for the corresponding denominators the complex arithmetic manipulation of the matrix representation of the underlying system. Finally, the conclusion provides the TF $u(s)/n(s)$ by Crammer's rule. The construction of the formal proof of Lemma 2 mainly requires the properties of the complex-valued matrices and vectors along with some arithmetic reasoning. We also formally verified the Transfer Functions (TFs) corresponding to output functions, $w(t)$ and $\theta(t)$, i.e., $w(s)/\eta(s)$ and $\theta(s)/eta(s)$ and the details about their verification can be found at [1]. This concludes our formalization of the LEoM of UAVs, their FD solutions and the associated TFs.

The lateral-directional motion of UAVs is described by the side force (Y), rolling moment (L) and Yawing moment (N). To formalize the LDEoM, we first formalize the aerodynamics stability derivatives corresponding to lateral-directional motion, given in Table 5, using the type abbreviation feature of HL.

Table 5: Aerodynamics Stability Derivatives and their Data-types

Symbol	Type	Symbol	Type	Symbol	Type
Y_v	$\mathbb{C}$	L_v	$\mathbb{C}$	N_v	$\mathbb{C}$
Y_p	$\mathbb{C}$	L_r	$\mathbb{C}$	N_r	$\mathbb{C}$
Y_r	$\mathbb{C}$	L_p	$\mathbb{C}$	N_p	$\mathbb{C}$
Y_ξ	$\mathbb{C}$	L_ξ	$\mathbb{C}$	N_ξ	$\mathbb{C}$

Definition 17. *Aerodynamics Stability Derivatives*

nw_typ_abrv ("arodyn_stbl_dervt_ltrl_frce", ':($Y_v \times Y_p \times Y_r \times Y_\xi$)')
nw_typ_abrv ("arodyn_stbl_dervt_rll_mmnt", ':($L_v \times L_p \times L_r \times L_\xi$)')
nw_typ_abrv ("arodyn_stbl_dervt_yw_mmnt", ':($N_v \times N_p \times N_r \times N_\xi$)')

The LDEoM of UAVs can be mathematically expressed as the following set of DEs [11, 40].

$$\begin{aligned} m\dot{v} - Y_v v - (Y_p + mW_e)p - (Y_r - mU_e)r - mg\phi cos\theta_e - mg\psi sin\theta_e = Y_\xi \xi + Y_\zeta \zeta \\ -L_v v + I_x \dot{p} - L_p p - I_{xz}\dot{r} - L_r r = L_\xi \xi + L_\zeta \zeta \\ -N_v v - I_{xz}\dot{p} - N_p p + I_z \dot{r} - N_r r = N_\xi \xi + N_\zeta \zeta \end{aligned} \tag{6}$$

where $\dot{v}$, $\dot{p}$ and $\dot{r}$ presents the first order-derivatives of the linear and angular disturbance velocities, respectively. Similarly, the variables ξ and ζ model the aileron and rudder angles, respectively. Under the conditions $p(t) = \dot{\phi}(t)$, $r(t) = \dot{\psi}(t)$ and $\zeta(t) = 0$, the above LDEoM become [11]:

$$\begin{aligned} m\dot{v} - Y_v v - (Y_p + mW_e)\dot{\phi} - (Y_r - mU_e)\dot{\psi} - mg\phi cos\theta_e - mg\psi sin\theta_e = Y_\xi \xi \\ -L_v v + I_x \ddot{\phi} - L_p \dot{\phi} - I_{xz}\ddot{\psi} - L_r \dot{\psi} = L_\xi \xi \\ -N_v v - I_{xz}\ddot{\phi} - N_p \dot{\phi} + I_z \ddot{\psi} - N_r \dot{\psi} = N_\xi \xi \end{aligned} \tag{7}$$

The first DE of the LDEoM of the UAV (Equation (7)) is formalized as:

Definition 18. *LDEoM* 1

$\vdash_{def}$ $\forall Y_p\ Y_r\ Y_\xi\ Y_v$ m. **list_v_latrl_eqtn_motn_fst** m (Y_v,Y_p,Y_r,Y_ξ) = [-Y_v; m]

$\vdash_{def}$ $\forall U_e\ V_e\ Y_v\ Y_r\ Y_\xi$ g $\theta_e\ Y_p$ m W_e.
list_phi_latrl_eqtn_motn_fst m g θ_e (U_e,V_e,W_e) (Y_v,Y_p,Y_r,Y_ξ) =
[m ∗ g ∗ cos θ_e; Y_p + m ∗ W_e]

$\vdash_{def}$ $\forall Y_v\ Y_p\ Y_r\ Y_\xi\ V_e\ W_e$ g $\theta_e\ Y_r$ m U_e.
list_psi_latrl_eqtn_motn_fst m g $theta_e$ (Y_v,Y_p,Y_r,Y_ξ) (U_e,V_e,W_e) =
[m ∗ g ∗ sin θ_e; Y_r - m ∗ U_e]

$\vdash_{def}$ $\forall Y_v\ Y_p\ Y_r\ Y_\xi$. **list_xi_latrl_eqtn_motn_fst** (Y_v,Y_p,Y_r,Y_ξ) = [Y_ξ]

$\vdash_{def}$ $\forall$u w v ϕ m g $\theta_e\ U_e\ V_e\ W_e\ \psi\ Y_v\ Y_p\ Y_r\ Y_\xi\ \xi$ t.
latrl_eqtn_motn_fst (Y_v,Y_p,Y_r,Y_ξ) (U_e,V_e,W_e) m g θ_e (u,v,w) $\phi\ \psi\ \xi$ t ⇔
n_ord_diffren_equat 1 (list_v_latrl_eqtn_motn_fst m (Y_v,Y_p,Y_r,Y_ξ)) v t -
n_ord_diffren_equat 1 (list_phi_latrl_eqtn_motn_fst m g θ_e (U_e,V_e,W_e) (Y_v,Y_p,Y_r,Y_ξ)) ϕ t -
n_ord_diffren_equat 1 (list_psi_latrl_eqtn_motn_fst m g θ_e (Y_v,Y_p,Y_r,Y_ξ) (U_e,V_e,W_e)) ψ t =
n_ord_diffren_equat 0 (list_xi_latrl_eqtn_motn_fst (Y_v,Y_p,Y_r,Y_ξ)) ξ t

where the function latrl_eqtn_motn_fst accepts the function variables v, ϕ, ψ and ξ and the lists of coefficients list_v_latrl_eqtn_motn_fst, list_phi_latrl_eqtn_motn_fst, list_psi_latrl_eqtn_motn_fst and list_xi_latrl_eqtn_motn_fst and returns the corresponding DE modeling the dynamical behavior of the UAVs. Similarly, the other two DEs of the LDEoM of the UAV (Equation (7)) are modelled as:

Definition 19. *LDEoM* 2

$\vdash_{def}$ $\forall L_p\ L_r\ L_\xi\ L_v$. **list_v_latrl_eqtn_motn_snd** (L_v,L_p,L_r,L_ξ) = [-L_v]

$\vdash_{def}$ $\forall I_y\ I_z\ L_v\ L_r\ L_\xi\ L_p\ I_x$. **list_phi_latrl_eqtn_motn_snd** (I_x,I_y,I_z) (L_v,L_p,L_r,L_ξ) = [0; L_p; -I_x]

$\vdash_{def}$ $\forall L_p\ L_r\ L_\xi\ L_v\ I_{xz}$. **list_psi_latrl_eqtn_motn_snd** I_{xz} (L_v,L_p,L_r,L_ξ) = [0; L_r; I_{xz}]
$\vdash_{def}$ $\forall L_p\ L_r\ L_\xi\ L_v$. **list_xi_latrl_eqtn_motn_snd** (L_v,L_p,L_r,L_ξ) = [L_ξ]
$\vdash_{def}$ $\forall$u w v $I_x\ I_y\ I_z\ \phi\ I_{xz}\ \psi\ L_v\ L_p\ L_r\ L_\xi\ \xi$ t.
latrl_eqtn_motn_snd (L_v,L_p,L_r,L_ξ) I_{xz} (I_x,I_y,I_z) (u,v,w) $\phi\ \psi\ \xi$ t $\Leftrightarrow$
n_ord_diffren_equat 0 (list_v_latrl_eqtn_motn_snd (L_v,L_p,L_r,L_ξ)) v t -
n_ord_diffren_equat 2 (list_phi_latrl_eqtn_motn_snd (I_x,I_y,I_z) (L_v,L_p,L_r,L_ξ)) ϕ t -
n_ord_diffren_equat 2 (list_psi_latrl_eqtn_motn_snd I_{xz} (L_v,L_p,L_r,L_ξ)) ψ t =
n_ord_diffren_equat 0 (list_xi_latrl_eqtn_motn_snd (L_v,L_p,L_r,L_ξ)) ξ t

Definition 20. *LDEoM* 3
$\vdash_{def}$ $\forall N_p\ N_r\ N_\xi\ N_v$. **list_v_latrl_eqtn_motn_trd** (N_v,N_p,N_r,N_ξ) = [-N_v]
$\vdash_{def}$ $\forall N_p\ N_r\ N_\xi\ N_v\ I_{xz}$. **list_phi_latrl_eqtn_motn_trd** I_{xz} (N_v,N_p,N_r,N_ξ) = [0; N_p; I_{xz}]
$\vdash_{def}$ $\forall N_p\ N_r\ N_\xi\ N_v\ I_x\ I_y\ I_z$. **list_psi_latrl_eqtn_motn_trd** (N_v,N_p,N_r,N_ξ) (I_x,I_y,I_z) = [0; N_r; -I_z]
$\vdash_{def}$ $\forall N_p\ N_r\ N_\xi\ N_v$. **list_xi_latrl_eqtn_motn_trd** (N_v,N_p,N_r,N_ξ) = [N_ξ]
$\vdash_{def}$ $\forall$u w v $I_{xz}\ \phi\ I_x\ I_y\ I_z\ \psi\ N_v\ N_p\ N_r\ N_\xi\ \xi$ t. **latrl_eqtn_motn_trd**
(N_v,N_p,N_r,N_ξ) (I_x,I_y,I_z) I_{xz} (u,v,w) $\phi\ \psi\ \xi$ t $\Leftrightarrow$
n_ord_diffren_equat 0 (list_v_latrl_eqtn_motn_trd (N_v,N_p,N_r,N_ξ)) v t -
n_ord_diffren_equat 2 (list_phi_latrl_eqtn_motn_trd I_{xz} (N_v,N_p,N_r,N_ξ)) ϕ t -
n_ord_diffren_equat 2 (list_psi_latrl_eqtn_motn_trd (N_v,N_p,N_r,N_ξ) (I_x,I_y,I_z)) ψ t =
n_ord_diffren_equat 0 (list_xi_latrl_eqtn_motn_trd (N_v,N_p,N_r,N_ξ)) ξ t

Next, in order to find out the TFs of the UV corresponding to its various inputs and outputs, the LT of the LDEoM is taken as follows:

$$\begin{aligned}(ms-Y_v)v(s)-((Y_p+mW_e)s+mgcos\theta_e)\phi(s)-((Y_r-mV_e)s+mgsin\theta_e)\psi(s)=\\ Y_\xi\xi(s)\\ -L_v v(s)+(I_x s^2-L_p s)\phi(s)-(I_{xz}+L_r s)\psi(s)=\\ L_\xi\xi(s)\\ -N_v v(s)-(I_{xz}s^2+N_p s)\phi(s)-(I_z-N_r s)\psi(s)=\\ L_\xi\xi(s)\end{aligned} \tag{8}$$

The LT of the LDEoM, i.e, Equation 8 and various TFs, such as $v(s)/\xi(s)$, $\Delta(s)/\xi(s)$ and $\theta(s)/\xi(s)$ are also formally verified. The details about their verification can be found at [1].

6 Formal Stability Analysis of CropCam UAV

CropCam UAV [34, 2] is an autopilot aircraft that captures the GPS based digital images by flying at low-altitude. It provides the high resolutions images that are somewhat impossible to take using the conventional ways, such as satellite. It is widely utilized for remote sensing in various applications, such as large scale topographic

mapping, agriculture and georeferencing etc. Stability is an important control characteristic of UAVs that smoothes the motion of the aircraft by dampening out any oscillation caused by various disturbances and thus ensures the equilibrium flight conditions [16]. It is based on the TFs of the UAV that are obtained by analyzing the dynamical behavior of the aircraft captures as the aircraft's equations of motion.

The TF of a system is mathematically expressed as follows:

$$\frac{Y(s)}{X(s)} = \frac{Numer(s)}{Denomer(s)} = \frac{b_m s^m + b_{m-1} s^{m-1} + ... + b_0}{a_n s^n + a_{n-1} s^{n-1} + ... + a_0} \tag{9}$$

where $X(s)$ and $Y(s)$ present the LT of the input function $x(t)$ and output function $y(t)$, respectively. Similarly, $Numer(s)$ and $Denomer(s)$ are complex-valued polynomials. The mathematical equation $Denomer(s) = 0$ is known as the characteristic equation and its roots are called the poles of the system. The locations of these poles in the complex plane presents important information about the stability of the corresponding system. A system is said to be stable if all the poles are located on the left half of the complex plane [16].

The notion of the stability of a UAV is formalized in HL as :

Definition 21. *Stability of a UAV*
$\vdash_{def}$ ∀Y. uav_stble Y = {s | Y s = 0 ∧ Re s < 0} ≠ { }

where uav_stble accepts the denominator Y: $\mathbb{C} \to \mathbb{C}$ of the TF corresponding to the aircraft's equations of motion of a UAV and returns a stable UAV. Similarly, s: $\mathbb{C}$ provides the root of the characteristic equation. The conjunct Y s = 0 provides the characteristic equation. Similarly, Re s < 0 ensures the location of the poles in the left half complex plane.

The LEoM for the CropCam UAV are mathematically modelled as below:

$$\begin{bmatrix} \dot{u} \\ \dot{w} \\ \dot{\theta} \end{bmatrix} = \begin{bmatrix} z_u & z_w & 0 \\ m_u & m_w & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} u \\ w \\ \theta \end{bmatrix} = \begin{bmatrix} z_\eta \\ m_\eta \\ 0 \end{bmatrix} \eta \tag{10}$$

Alternatively, Equation (10) can be written as follows:

$$\begin{bmatrix} \dot{u} \\ \dot{w} \end{bmatrix} = \begin{bmatrix} z_u & z_w \\ m_u & m_w \end{bmatrix} \begin{bmatrix} u \\ w \end{bmatrix} = \begin{bmatrix} z_\eta \\ m_\eta \end{bmatrix} \eta \tag{11}$$

Next, the LT of above equation is taken for extracting the TFs of the CropCam UAV corresponding to its various inputs and outputs.

$$\begin{bmatrix} s - z_u & -z_w \\ s - m_u & -m_w \end{bmatrix} \begin{bmatrix} u(s) \\ w(s) \end{bmatrix} = \begin{bmatrix} z_\eta \eta(s) \\ m_\eta \eta(s) \end{bmatrix} \tag{12}$$

The TF $u(s)/\eta(s)$ corresponding to the LEoM for the CropCam UAV is given as follows [40]:

$$\frac{u(s)}{\eta(s)} = \frac{X_\eta \left(s + Z_w + X_w \frac{Z_\eta}{X_\eta}\right)}{s^2 - (Z_w + X_u)s + (Z_w X_u - Z_u X_w)} \tag{13}$$

Next, the stability of the CropCam UAV is formally verified by utilizing the denominator of the TF ($u(s)/\eta(s)$) as follows:

Theorem 5. Stability of CropCam UAV

$\vdash_{thm} \forall \alpha\ \mathtt{Z_w}\ \mathtt{Z_u}\ \mathtt{X_w}\ \mathtt{X_u}.$

$[C_1]$ $((\mathsf{Re}\ \mathtt{Z_w} + \mathsf{Re}\ \mathtt{X_u} < 0 \wedge$

$((\mathsf{Re}\ \mathtt{Z_w} + \mathsf{Re}\ \mathtt{X_u})^2 - 4 * (\mathsf{Re}\ \mathtt{Z_w} * \mathsf{Re}\ \mathtt{X_u} - \mathsf{Re}\ \mathtt{Z_u} * \mathsf{Re}\ \mathtt{X_w}) < 0 \vee$

$(\mathsf{Re}\ \mathtt{Z_w} + \mathsf{Re}\ \mathtt{X_u})^2 - 4 * (\mathsf{Re}\ \mathtt{Z_w} * \mathsf{Re}\ \mathtt{X_u} - \mathsf{Re}\ \mathtt{Z_u} * \mathsf{Re}\ \mathtt{X_w}) = 0)) \vee$

$(0 < (\mathsf{Re}\ \mathtt{Z_w} + \mathsf{Re}\ \mathtt{X_u})^2 - 4 * (\mathsf{Re}\ \mathtt{Z_w} * \mathsf{Re}\ \mathtt{X_u} - \mathsf{Re}\ \mathtt{Z_u} * \mathsf{Re}\ \mathtt{X_w}) \wedge$

$(\sqrt{(\mathsf{Re}\ \mathtt{Z_w} + \mathsf{Re}\ \mathtt{X_u})^2 - 4 * (\mathsf{Re}\ \mathtt{Z_w} * \mathsf{Re}\ \mathtt{X_u} - \mathsf{Re}\ \mathtt{Z_u} * \mathsf{Re}\ \mathtt{X_w})} < -(\mathsf{Re}\ \mathtt{Z_w} + \mathsf{Re}\ \mathtt{X_u}) \vee$

$(\mathsf{Re}\ \mathtt{Z_w} + \mathsf{Re}\ \mathtt{X_u}) < \sqrt{(\mathsf{Re}\ \mathtt{Z_w} + \mathsf{Re}\ \mathtt{X_u})^2 - 4 * (\mathsf{Re}\ \mathtt{Z_w} * \mathsf{Re}\ \mathtt{X_u} - \mathsf{Re}\ \mathtt{Z_u} * \mathsf{Re}\ \mathtt{X_w})}))) \wedge$

$[C_2]$ $\mathsf{Im}\ \mathtt{Z_w} = 0 \wedge$

$[C_3]$ $\mathsf{Im}\ \mathtt{Z_u} = 0 \wedge$

$[C_4]$ $\mathsf{Im}\ \mathtt{X_w} = 0 \wedge$

$[C_5]$ $\mathsf{Im}\ \mathtt{X_u} = 0 \wedge$

$\Rightarrow \mathsf{uav\_stble}\ (\lambda \mathtt{s}.\ \mathtt{s}^2\ -\ \mathtt{s}\ *\ (\mathtt{Z_w} + \mathtt{X_u}) + \mathtt{Z_w} * \mathtt{X_u} - \mathtt{Z_u} * \mathtt{X_w})$

Conditions C_1-C_5 assert constraints for the stability of the CropCam UAV. The proof process of the above theorem is mainly based on Definition 21 along with some arithmetic reasoning. Similarly, the stability of the CropCam UAV based on its TF $w(s)/\eta(s)$ corresponding to its LEoM is formally verified. More details about the analysis can be found in the corresponding HL proof script at [1].

7 Discussions

The higher-order-logic TP based approach for analyzing the continuous dynamical behaviour of UAVs provided in this chapter allow us to clearly define all of the parameters along with their types that contribute to the dynamics of the aircraft. On the other hand, in the conventional approaches, like paper-and-pencil-proof and computer based techniques, there is always a chance of misinterpreting any of these parameters in analyzing the dynamics of UAVs. Moreover, all of the verified theorems and lemmas are of generic nature, i.e., they are verified for the universally quantified functions and variables and thus can be specialized for a particular scenario. Whereas, in computer based simulations, each of the cases are modelled individually. Moreover, the inherent soundness of our proposed approach ensures that all the required assumptions are explicitly mentioned along with the theorem and are incorporated in the corresponding proof. Table 6 provides a comparison of various methods used for analyzing the continuous dynamical behavior of UAVs and

summarizes their strength and weaknesses. This comparison is performed based on various parameters, such as accuracy, expressiveness, accuracy and automation. For example, in higher-order-logic TP, we can truly model the continuous dynamics of UAVs, such as the DEs based aircraft's equations of motion and the corresponding TF in their true continuous form, whereas, in the MC based analysis, they are mostly discretized, which may compromise the accuracy of the analysis.

Table 6: Comparison of Techniques for Analyzing Continuous Dynamics of UAVs

	Paper-and-Pencil Proof	Computer-based Simulations	Model Checking	Theorem Proving
Expressiveness	✓	✓		✓
Accuracy	✓(?)		✓	✓
Automation		✓	✓	

8 Conclusions

This chapter proposes a higher-order-logic TP based framework for formally analyzing the continuous dynamical behaviour of UAVs. Various coordinate frames, such as navigation and aircraft's body-fixed frames are formalized and their their associated transformations are also verified. This ensure the correctness of the relative movement and position of the aircraft. The longitudinal and LDEoM for UAVs are formalized their various properties, such as TF and stability, and solutions in FD are also formally verified. Finally, the stability analysis of the CropCam UAV is performed. In future, the formalization of the coordinate frames can be extended by incorporating other coordinates systems, such as quaternion. Another future direction is to formally verify some other interesting control system properties of UAVs, such as sensitivity.

References

1. (2022) Formal Analysis of Unmanned Aerial Vehicles using Higher-order-logic Theorem Proving: Project Webpage. `http://save.seecs.nust.edu.pk/fauav/`
2. Ahmad A, Samad AM (2010) Aerial Mapping using High Resolution Digital Camera and Unmanned Aerial Vehicle for Geographical Information System. In: International Colloquium on Signal Processing & its Applications, IEEE, pp 1–6
3. Aréchiga N, Loos SM, Platzer A, Krogh BH (2012) Using Theorem Provers to Guarantee Closed-loop System Properties. In: American Control Conference, IEEE, pp 3573–3580

4. Baier C, Katoen JP (2008) Principles of Model Checking. MIT Press
5. Barmpounakis EN, Vlahogianni EI, Golias JC (2016) Unmanned Aerial Aircraft Systems for Transportation Engineering: Current Practice and Future Challenges. International Journal of Transportation Science and Technology 5(3):111–122
6. Birk A, Wiggerich B, Bülow H, Pfingsthorn M, Schwertfeger S (2011) Safety, Security, and Rescue Missions with an Unmanned Aerial Vehicle (UAV). Journal of Intelligent & Robotic Systems 64(1):57–76
7. Carreno V, Muñoz C (2000) Aircraft Trajectory Modeling and Alerting Algorithm Verification. In: Theorem Proving in Higher Order Logics, Springer, LNCS, vol 1869, pp 90–105
8. Chan M, Ricketts D, Lerner S, Malecha G (2016) Formal Verification of Stability Properties of Cyber-physical Systems. In: Coq for Programming Languages
9. Chen X, Chen G (2018) Formal Verification of Helicopter Automatic Landing Control Algorithm in Theorem Prover Coq. International Journal of Performability Engineering 14(9)
10. Clarke EM, Zuliani P (2011) Statistical Model Checking for Cyber-Physical Systems. In: Automated Technology for Verification and Analysis, Springer, LNCS, vol 6996, pp 1–12
11. Cook MV (2012) Flight Dynamics Principles: A Linear Systems Approach to Aircraft Stability and Control. Butterworth-Heinemann
12. Cooper J, Goodrich MA (2008) Towards Combining UAV and Sensor Operator Roles in UAV-enabled Visual Search. In: Human Robot Interaction, ACM, pp 351–358
13. Dennis LA, Fisher M, Webster MP, Bordini RH (2012) Model Checking Agent Programming Languages. Automated Software Engineering 19(1):5–63
14. Ducard GJ (2009) Fault-tolerant Flight Control and Guidance Systems: Practical Methods for Small Unmanned Aerial Vehicles. Springer Science & Business Media
15. Everaerts J, et al (2008) The Use of Unmanned Aerial Vehicles (UAVs) for Remote Sensing and Mapping. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences 37(2008):1187–1192
16. Foster T, Bowman J (2005) Dynamic Stability and Handling Qualities of Small Unmanned-Aerial Vehicles. In: AIAA Aerospace Sciences Meeting and Exhibit, p 1023
17. Gallington RW, Berman H, Entzminger J, Francis MS, Palmore P, Stratakes J (1997) Unmanned Aerial Vehicles. Future Aeronautical and Space Systems, AIAA, Progress in Astronautics and Aeronautics 172:251–295
18. Ghorbal K, Jeannin JB, Zawadzki E, Platzer A, Gordon GJ, Capell P (2014) Hybrid Theorem Proving of Aerospace Systems: Applications and Challenges. Journal of Aerospace Information Systems 11(10):702–713
19. Groza A, Letia IA, Goron A, Zaporojan S (2015) A Formal Approach for Identifying Assurance Deficits in Unmanned Aerial Vehicle Software. In: Progress in Systems Engineering, vol 366, Springer, pp 233–239

20. Guzey HM (2017) Hybrid Consensus-Based Formation Control of Fixed-Wing MUAVs. Cybernetics and Systems 48(2):71–83
21. Harrison J (1996) HOL Light: A Tutorial Introduction. In: Formal Methods in Computer-Aided Design, Springer, LNCS, vol 1166, pp 265–269
22. Harrison J (2009) Handbook of Practical Logic and Automated Reasoning. Cambridge University Press
23. Harrison J, et al (1996) Formalized Mathematics. Tech. Rep. 36, Turku Centre for Computer Science, Finland
24. Hasan O, Tahar S (2015) Formal Verification Methods. Encyclopedia of Information Science and Technology, IGI Global Publication pp 7162–7170
25. Karimoddini A, Lin H, Chen BM, Lee TH (2014) Hierarchical Hybrid Modelling and Control of an Unmanned Helicopter. International Journal of Control 87(9):1779–1793
26. Loos SM, Renshaw D, Platzer A (2013) Formal Verification of Distributed Aircraft Controllers. In: International Conference on Hybrid Systems: Computation and Control, ACM, pp 125–130
27. Lyon DH (2004) A Military Perspective on Small Unmanned Aerial Vehicles. Instrumentation & Measurement Magazine 7(3):27–31
28. Ma Z, Chen G (2017) Formal Derivation and Verification of Coordinate Transformations in Theorem Prover Coq. In: International Conference on Dependable Systems and Their Applications, pp 127–136
29. Malecha G, Ricketts D, Alvarez MM, Lerner S (2016) Towards Foundational Verification of Cyber-physical Systems. In: Science of Security for Cyber-Physical Systems, IEEE, pp 1–5
30. Munoz C, Narkawicz A (2016) Formal Analysis of Extended Well-Clear Boundaries for Unmanned Aircraft. In: NASA Formal Methods Symposium, Springer, LNCS, vol 9690, pp 221–226
31. Munoz C, Narkawicz A, Hagen G, Upchurch J, Dutle A, Consiglio M, Chamberlain J (2015) DAIDALUS: Detect and Avoid Alerting Logic for Unmanned Systems. In: Digital Avionics Systems Conference, IEEE, pp 5A1–1–5A1–12
32. Narkawicz A, Munoz C (2012) Formal Verification of Conflict Detection Algorithms for Arbitrary Trajectories. Reliable Computing 17(2):209–237
33. Paulson LC (1996) ML for the Working Programmer. Cambridge University Press
34. Ping JTK, Ling AE, Quan TJ, Dat CY (2012) Generic Unmanned Aerial Vehicle (UAV) for Civilian Application-A Feasibility Assessment and Market Survey on Civilian Application for Aerial Imaging. In: Sustainable Utilization and Development in Engineering and Technology, IEEE, pp 289–294
35. Seibel CW, Farines JM, Cury JE (1997) Towards using Hybrid Automata for the Mission Planning of Unmanned Aerial Vehicles. In: International Hybrid Systems Workshop, Springer, LNCS, vol 1567, pp 324–340
36. Shim D, Kim H, Sastry S (2000) Hierarchical Control System Synthesis for Rotorcraft-based Unmanned Aerial Vehicles. In: AIAA Guidance, Navigation, and Control Conference and Exhibit, pp 1–9

37. Valavanis KP (2008) Advances in Unmanned Aerial Vehicles: State of the Art and the Road to Autonomy. Springer Science & Business Media
38. Webster M, Fisher M, Cameron N, Jump M (2011) Formal Methods for the Certification of Autonomous Unmanned Aircraft Systems. In: Computer Safety, Reliability, and Security, Springer, LNPSE, vol 6894, pp 228–242
39. Williams KW (2004) A Summary of Unmanned Aircraft Accident/Incident Data: Human Factors Implications. Tech. rep., Federal Aviation Adminstration
40. Xu Jr K (2014) Frequency Domain System Identification of Fixed-wing Unmanned Aerial Vehicles