Formalization of the Gateaux derivative of functional and application in the principle of virtual work

Zhang Jingzhi\textsuperscript{1,2}, Li Ximeng\textsuperscript{1,2}, Wang Guohui\textsuperscript{1}, Guan Yong\textsuperscript{1}

64 Xisanhuan North Road, Haidian District, Beijing, China

\textsuperscript{1} Beijing Advanced Innovation Center for Imaging Technology, Capital Normal University, Beijing, China

\textsuperscript{2} School of Mathematical Science, Capital Normal University, Beijing, China

Email: ghwang@cnu.edu.cn

Abstract. Analytical mechanics provides the central guidelines for the design of engineering machinery in use today. One of the main pillars for analytical mechanics is the principle of virtual work. In the establishment of this principle, the Gateaux derivative plays an indispensable role. In this paper, we formalize the Gateaux derivative in the interactive theorem prover HOL Light. On this basis, we formally verify the principle of virtual work. This effort paves way for the computerized formalization of analytical mechanics. Thus, it will ultimately contribute to the verified design of engineering machinery, which comes with correctness guarantees beyond what is enabled by the currently adopted validation techniques.

1. Introduction

Safety and reliability are the two main aspects with respect to which guarantees need to be delivered in the design and construction of systems, e.g., vehicles, robots, aeronautical equipment, medical devices, etc [1].

Traditionally, the safety and reliability of these systems are validated either manually on paper, or via computer simulation. The former approach enables the coverage of all the possible situations for the functioning of the machine – by means of mathematical derivation and proof. However, it may be laborious and suffer from human errors. The latter approach, on the other hand, enables a high level of automation, while oftentimes suffering from incomplete coverage of runtime conditions, and from errors introduced by computing with floating-point numbers.

Recent years there have been an increasing adoption of formal verification for safety and reliability in the industry. In a formal verification, mathematical derivation and proof can be performed in a logical language, and under the scrutinization of a computer program (called an interactive theorem prover, or theorem prover in short). This obviates human errors or numerical errors in the validation, while enabling the full coverage of runtime conditions.

For the formal verification of a system in a theorem prover, the formalization of the underlying theories governing the functioning of the system is a prerequisite. That is, these theories have to be formulated and proven inside the prover. Analytical mechanics [2,3] is a piece of theory that underlies the functioning of a great many control systems. It is a reformulation of Newtonian mechanics from the viewpoint of energy. Currently, its formalization is missing from most of the theorem provers in existence. As a result, no formal verification of dynamical control systems can be performed in these provers.
The formalization of mathematical theories in a theorem prover often requires extensive efforts. In this paper, we present our first results toward a full formalization of analytical mechanics. This includes a formalization of the Gateaux derivative of functionals (Section 2), and a verification of the principle of virtual work (Section 3) that is conducted using this formalization. The verification of the principle of virtual work not only illustrates the usefulness of the formalization of the Gateaux derivative [4, 5], but also provides an essential building block for an ultimate formalization of analytical mechanics, and, hence, for the formal verification of dynamical systems. Our work is performed in the theorem prover HOL Light. Hence, the formalization and verification are performed in the formal language of Higher Order Logic.

The rest structure of this paper is as follows: in Section 2, we formally defined the Gateaux derivative of functional and formally proved the Gateaux derivative of integral type functional. Then, as an application of formalization of the Gateaux derivative of functional, we formally verified the principle of virtual work in Section 3. Section 4 and 5 are the related work and conclusion of this paper.

2. Formalization of the Gateaux derivative of functionals

In this section, we introduce the Gateaux derivative and present its formalization. To facilitate the understanding of the concepts we formalize, we give the mathematical expression of these concepts before their formal counterpart.

The Gateaux derivative is a general form of directional derivatives in that the change of the function value can be considered along an arbitrary direction. The Gateaux derivative of functionals lifts this concept to functionals (i.e., mappings from functions to real numbers). Intuitively, it is an indicator of how fast the value of a functional changes along a specific direction.

Mathematically, the Gateaux derivation of the functional \( J(y) \), \( \delta J[y] \), has the following expression

\[
\delta J[y] = \lim_{\varepsilon \to 0} \frac{J[y + \varepsilon h] - J[y]}{\varepsilon}
\] (1)

Here, \( h \) is a function that represents the direction along which the change of the functional \( J(y) \) is considered. This definition can be formalized in HOL Light as follows.

**Definition 1: The Gateaux derivative of functionals (as a predicate)**

let has_gateaux_derivative = new_definition

```
`\( J \) has_gateaux_derivative` \( (s, y) \) \( <= \)

(`!h. continuously_differentiable_on 1 h s ==>

(\( t. \) inv(drop t) \% (\( J (y + vfcmul (drop t) h) - J (y) \)) \(-->\) J' h) (at (vec 0)))`;;
```

In the above, the symbols “!” , “<=”, “==>” correspond to the logical connectives for universal quantification, equivalence, and implication, respectively, for all \( f \), “x. f x” represents the function \( f(x) \), “continuously_differentiable_on 1 h s” means function \( h \) is continuously differentiable on the set \( s \), “-->” corresponds to the “lim” in Eq. (1), “inv” gives the inverse of a real number, “"%"” means the scalar multiplication between a real number and a vector, “vfcmul” means scalar multiplication between a real number and a vector valued function, “drop” transforms a vector of type “\( R^1 \)” into a real number, and “vec 0” represents the zero vector.

Specially, if the functional \( J(y) \) can be expressed as an integral (i.e., it is an integral-type functional),

\[
J[y] = \int_{a}^{b} f(y(x))dx
\] (2)

then, its Gateaux derivative is shown to have the following form.
\[ \delta J[y] = \int_a^b \frac{\partial f}{\partial y} \delta y \, dx \quad (3) \]

This result is formalized and proven in the following theorem.

**Theorem 1:** The Gateaux derivative of integral-type functionals

\[ \forall f \in C[a,b] \ y_0 \in [a,b] \ s \in [a,b] \ s_0. \]

\[ \sim \text{(content(interval[a,b]) = &0)} \land \]

\[ y_0 \in s \ \text{INTER} \ \text{mspace(fspace(interval[a,b]))} \land \]

\[ \{ u \mid ?y. y \in \text{mspace(fspace(interval[a,b]))} \}
\]

\[ \land u \in \text{IMAGE} y (\text{interval}[a,b]) = s \land \]

\[ (\forall u. u \in s \implies (f \text{ has \_ derivative } f^* u) \ (\text{at } u \text{ within } s)) \land \]

\[ (\forall u. u \in s \land j \in \text{dimindex}(N)) \implies \]

\[ (f' u \ (\text{basis } j)) \text{ has \_ derivative } f^* u \ (\text{at } u \text{ within } s)) \]

\[ \implies (\text{flinear} \ (h, \text{integral} \ (\text{interval}[a,b])) \ (x. f'(y_0 x) (h x))) \]

\[ (\text{interval}[a,b]) ) \land \]

\[ (\forall h. h \in \text{mspace(fspace(interval[a,b]))}) \implies \]

\[ (\forall t. \text{inv}(\text{drop } t) \ %
\]

\[ (\text{integral} \ (\text{interval}[a,b]) \ (f \circ (y_0 + \text{vcmul} (\text{drop } t) h)) -
\]

\[ (\text{integral} \ (\text{interval}[a,b]) \ (f \circ y_0)) \implies 
\]

\[ (\text{integral} \ (\text{interval}[a,b]) \ (x. f' (y_0 x) (h x))) 
\]

\[ (\text{at } (\text{vec } 0) \text{ within } \{ t \mid y_0 + \text{vcmul} (\text{drop } t) h \text{ IN } s_0}) \}
\]

Here, “?” , “IN”, “INTER”, and “o” correspond to the mathematical symbols for existential quantification, set membership, set intersection, and functional composition, respectively, “content” gives the volume of a set, “mspace(fspace(interval[a,b]))” means the continuous function space \( C[a, b] \), “IMAGE y (interval[a,b])” means the image set of function \( y \) on the closed interval \([a, b] \), “f' u h” is the derived function of \( f \), “f' u (basis j)” means \( \frac{\partial f}{\partial u_j} \), “flinear” asserts that its argument is a linear functional.

### 3. Application: the principle of virtual work

We apply our formalization of the Gateaux derivative of functionals to formally verify the principle of virtual work. Firstly, we give the formal definition of mechanical work. Secondly, we give the formal definition of virtual work. Finally, we formally verify the principle of virtual work.

The mechanical work \( W \) is the work done by force \( F \) along path \( r \). It has the following mathematical expression.

\[ W = \int_{r(a)}^{r(b)} F \cdot dr = \int_a^b F \cdot \frac{dr}{dt} dt = \int_a^b F \cdot \dot{r} dt \quad (4) \]

This definition of mechanical work can be formalized as follows.

**Definition 2:** Mechanical work

let mechanical_work = new_definition

\[ \forall a \in [a,b] \ f = \]

\[ (\forall r. \text{integral} (\text{interval}[a,b]) (\forall t. \text{lift}(f \ t \ \text{dot} (\text{higher\_vector\_derivative} \ 1 \ r \ (\text{interval}[a,b]) \ t))) )\]

Here, “lift” means the transformation from a real number to a vector with type \( R^3 \), “dot” means the inner product of two vectors, and “higher\_vector\_derivative 1 \ r \ (\text{interval}[a,b]) \ r’” means the derived function of \( r \).
The virtual work of force $F$ along the virtual displacement $h$ is the Gateaux derivative of the mechanical work, and it has the following form

$$\partial W = \lim_{\varepsilon \to 0} \frac{\int_a^b F \cdot d(r + \varepsilon h) - \int_a^b F \cdot dr}{\varepsilon}$$

The formal definition of virtual work is as follows:

**Definition 3: The virtual work of the mechanical work**

let virtual_work = new_definition
`virtual_work [t0,t1] f = gateaux_derivative (mechanical_work [t0,t1] f) (interval[t0,t1])`;;

Here, “gateaux_derivative” has the following formal description.

**Definition 4: The Gateaux derivative of Functionals**

let gateaux_derivative = new_definition
`gateaux_derivative J s y = @J'. (J has_gateaux_derivative J') (s, y)`;;

Here, the expression of the form “X = @J’. P J’”, where P is a predicate, states that X equals the very J’ such that (P J’) holds.

It can be shown that virtual work, as given in (5) (and formally in Definition 3), has the following simpler expression.

$$\partial W = \int_a^b (F \cdot \dot{h}) dt$$

In the derivation of the expression above, the following theorem plays a central role. This theorem can be proven using Definition 2 and Theorem 1.

**Theorem 2: The Gateaux Derivative of Mechanical Work**

`!a b f r0. drop a < drop b /
  f continuous_on interval[a,b] /
  continuously_differentiable_on 1 r0 (interval[a,b])
  ==> (mechanical_work [a,b] f has_gateaux_derivative
       mechanical_work [a,b] f) (interval[a,b], r0)`

In this theorem statement, “f continuous_on interval[a,b]” means function f is continuous in the closed interval $[a,b]$. We are in a position to introduce and prove the principle of virtual work. The principle of virtual work asserts that the virtual work done by the resultant force for a mechanical system with static equilibrium state equals to zero.

$$\partial W = \int_a^b (F \cdot \dot{h}) dt = 0 \iff F = \vec{0}$$

This principle is formally verified in Theorem 3.

**Theorem 3: The principle of virtual work**

`!a b f r0. drop a < drop b /
  f continuous_on interval[a,b] /
  continuously_differentiable_on 1 r0 (interval[a,b])
  ==> (((!h. continuously_differentiable_on 1 h (interval[a,b])
         ==> virtual_work [a,b] f r0 h = vec 0) <=>
         (!t. t IN interval[a,b] ==> f t = vec 0))`
The proof of this theorem is mainly based on a lemma that asserts that if a function $f$ is continuous in closed interval $[a,b]$, for any $h$, it holds that $h(a) = h(b) = h'(a) = h'(b) = 0$, and

$$\int_{a}^{b} f \cdot h dt = 0 \quad (7)$$

then $f' \equiv 0$ is satisfied. The formalization of this lemma has the following form.

**Lemma 1: one lemma of functional**

```
f:real^1->real^N a b.
 ~(content(interval[a,b]) = &0) /
 f continuous_on interval[a,b] /
 (!h. higher_vector_differentiable_on 1 h (interval[a,b]) /
  (higher_vector_derivative 1 h (interval[a,b])) continuous_on interval [a,b] /
  h a = vec 0 /
  higher_vector_derivative 1 h (interval[a,b]) a = vec 0 /
  higher_vector_derivative 1 h (interval[a,b]) b = vec 0 /
 => integral (interval[a,b]) (\x. lift (f x dot h x)) = vec 0)
 => (!x. x IN interval[a,b] => f x = vec 0)```

4. Related work

Existing work on the formalization of the dynamics of control systems is rare [6,7,8]. Hasan and Ahmad [6] formalizes the steady state errors of feedback control systems. Binyameen et al [7] provides the formal kinematic analysis of a two-link planar manipulator. Oberkampf and Trucano [8] discuss the estimating errors and uncertainties in computational fluid dynamics. But the Formalization of dynamical part mainly formalize the equations of motion and verify the solution of the equations, as the lack of library of analytical mechanics.

In general, there is a great amount of work on the formalization of mathematical theories that lay the foundation for the verification of systems. Examples include the formalizations of real and complex analysis [9,10], metric [11,12], topology, etc.

5. Conclusion

The formalization of analytical mechanics plays a crucial role in the formal verification of the safety and reliability of control systems. A full formalization of this subject requires an exceedingly high amount of efforts to be completed. In this paper, we present our initial steps towards this final goal. More concretely, our main contribution has three essential ingredients: the formalization of the Gateaux derivative of functionals, the formalization of mechanical work and virtual work, and the formal verification of the principle of virtual work. The formalization and verification are performed in over 1000 lines of codes in HOL Light. The other main constituent parts of a formalization of analytical mechanics that we plan to complete in future work include Lagrange’s equations and Hamilton Canonical Equation.

References

[1] Dhillon, B., Fashandi, A.: Safety and reliability assessment techniques in robotics. Robotica 15(15), 701–708 (2000).
[2] ALouis, H., Janet, F., Robinett, R.: Analytical mechanics. American Journal of Physics 68(68), 390–393 (1998).
[3] Herbert, G., Charles, P., John, S., Stephen, A.: Classical mechanics, 3rd ed. American Journal of Physics 70(7), 782–783 (2002).
[4] Botelho, F.: Basic Concepts on the Calculus of Variations. Springer International Publishing (2014).
[5] Gelfand, I.M., Fomin, S.V.: Calculus of Variations (translated by R. A. Silverman). Prentice-
Osman Hasan, Muhammad Ahmad: Formal analysis of steady state errors in feedback control systems using hol-light. In: Design, Automation & Test in Europe Conference & Exhibition (2013).

Binyameen, F., Osman, H., Sohail, I.: Formal kinematic analysis of the two-link planar manipulator. In: International Conference on Formal Engineering Methods (2013).

Oberkampf, W., Trucano, T.: Verification and validation in computational fluid dynamics. Advances in Mechanics 38(3), 209–272 (2007).

Boldo, S., Lelay, C., Melquiond, G.: Formalization of real analysis: A survey of proof assistants and libraries. Mathematical Structures in Computer Science 26(7), 1196–1233 (2016).

John, H.: The hol light theory of euclidean space. Journal of Automated Reasoning 50(2), 173–190 (2013).

Marco, M.: A formalization of metric spaces in hol light. Journal of Automated Reasoning 60(12), 1–18 (2017).

J Zhang, G Wang, Zh Shi. Etc.: Formalization of functional variation in HOL Light. Journal of Logic and Algebraic Methods in Programming.