


# A Formalization of the General Theory of Quaternions

Thaynara Arielly de Lima ✉ 

Universidade Federal de Goiás, Goiânia, Brazil

André Luiz Galdino ✉ 

Universidade Federal de Catalão, Catalão, Brazil

Bruno Berto de Oliveira Ribeiro

Universidade de Brasília, Brasília D.F., Brazil

Mauricio Ayala-Rincón ✉ 

Universidade de Brasília, Brasília D.F., Brazil

---

## Abstract

This paper discusses the formalization of the theory of quaternions in the Prototype Verification System (PVS). The general approach in this mechanization relies on specifying quaternion structures using any arbitrary field as a parameter. The approach allows the inheritance of formalized properties on quaternions when the parameters of the general theory are instantiated with specific fields such as reals or rationals. The theory includes characterizing algebraic properties that lead to constructing quaternions as division rings. In particular, we illustrate how the general theory is applied to formalize Hamilton's quaternions using the field of reals as a parameter, for which we also mechanized theorems that show the completeness of three-dimensional rotations, proving that Hamilton's quaternions mimic any 3D rotation.

**2012 ACM Subject Classification** Computing methodologies → Symbolic and algebraic manipulation; Theory of computation → Automated reasoning; Theory of computation → Logic and verification

**Keywords and phrases** Theory of quaternions, Hamilton's quaternions, Algebraic formalizations, PVS

**Digital Object Identifier** 10.4230/LIPIcs.ITP.2024.11

**Funding** *Thaynara Arielly de Lima*: Project supported by FAPEG 202310267000223.

*Mauricio Ayala-Rincón*: Project supported by FAPDF DE 00193.00001175/21-11 and CNPq Universal 409003/21-2 grants. The author was partially funded by the CNPq grant 313290/21-0.

## 1 Introduction

Quaternions can be identified with the general theory of algebraic structures consisting of quadruples built over a field,  $\langle \mathbb{F}, +_{\mathbb{F}}, *_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{one}_{\mathbb{F}} \rangle$  and two selected elements of the field  $a, b \in \mathbb{F}$ , where the quaternion addition is built from the field addition component to component, and the product quaternion is a distributive product, that satisfies a series of axioms, including

$$(\text{zero}_{\mathbb{F}}, \text{one}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}})^2 = (a, \text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}})$$

$$(\text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{one}_{\mathbb{F}}, \text{zero}_{\mathbb{F}})^2 = (b, \text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}})$$

$$(\text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{one}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}) * (\text{zero}_{\mathbb{F}}, \text{one}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}) = (\text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{one}_{\mathbb{F}})$$

among others, from which all properties of addition and multiplication of quaternions are inferred. In general, given a field  $\mathbb{F}$ , and elements  $a, b \in \mathbb{F}$ , the quaternion algebra is



© Thaynara Arielly de Lima, André Luiz Galdino, Bruno Berto de Oliveira Ribeiro, and Mauricio Ayala-Rincón;

licensed under Creative Commons License CC-BY 4.0

15th International Conference on Interactive Theorem Proving (ITP 2024).

Editors: Yves Bertot, Temur Kutsia, and Michael Norrish; Article No. 11; pp. 11:1–11:18



Leibniz International Proceedings in Informatics

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

## 11:2 A Formalization of the General Theory of Quaternions

represented as  $\left(\frac{a, b}{\mathbb{F}}\right)$ . It is a vector space in  $\mathbb{F}$ , with the basis

$$\begin{aligned} 1 &= (\text{one}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}) & i &= (\text{zero}_{\mathbb{F}}, \text{one}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}) \\ j &= (\text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{one}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}) & k &= (\text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{one}_{\mathbb{F}}) \end{aligned}$$

and a distributive product, such that :  $i^2 = a, j^2 = b, ij = k$  (cf. axioms above), and  $ij = -ji$ , for  $a = (a, \text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}})$ ,  $b = (b, \text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{zero}_{\mathbb{F}})$ .


Hamilton's quaternions are the first introduced structure of quaternions [11]. After its discovery, the research for structures similar to the original quaternions started, leading to a more generic and algebraic definition than the classic approach of Hamilton. Our specification in PVS uses such a generic definition.

Using the notation above, Hamilton's quaternions is the algebra  $\mathbb{H} = \left(\frac{-1, -1}{\mathbb{R}}\right)$ .

The structure of Hamilton's quaternions is the most popular because of its well-known efficient applicability in manipulating three-dimensional (3D) objects. Despite this fact, the interest in quaternions is not limited to Hamilton's ones but also to other structures of quaternions that are of great interest (e.g., [22]).

### 1.1 Main results


This paper describes the formalization of the general theory of the structures of quaternions in the interactive proof assistant PVS. It provides a characterization of quaternions as division rings based on algebraic properties of fields. The characterization is crucial to building multiplicative inverses for non-zero quaternion elements, an essential element in structures such as Hamilton's quaternions. In addition, the formalization shows how to build the structure of Hamilton's quaternions with adequate theory parameters. Finally, we formalize a completeness theorem of Hamilton's quaternions to rotate any 3D vector.

The quaternions theory is developed over the PVS nasalib theory [algebra](#) . Recent developments on this theory are reported in [4]. The theory includes complete proofs of the three isomorphism theorems for rings, characterizations of principal, prime, and maximal ideals, and an abstract algebraic-theoretical version of the Chinese Remainder Theorem for arbitrary rings [7]. Also, it includes a division algorithm for Euclidean rings and Unique Factorization Domains [6].

As far as we know, there are three solid formalizations restricted to the structure of Hamilton's quaternions, one of them in HOL Light [9], another in Coq [2], and the third one in Isabelle/HOL [18]. The HOL Light formalization applies to verify basic parts of theories related to slicing regular functions and Pythagorean-Hodograph curves; the second one in Coq has been applied to formalize 3D robot manipulators; and the one in Isabelle/HOL inspired Koutsoukou-Argraki's formalization of octonions [13]. In contrast, some elements of the general theory of quaternions built over any abstract field, as in our case, were only developed as part of the Lean mathlib library [16].

### 1.2 Organization

Section 2 is divided into subsections discussing the basic elements used in the specification and axiomatization of the general theory of quaternions (2.1), discussing how the algebraic properties of such structures are inferred from the axiomatization (2.2), and how quaternions are characterized as division rings (2.3). Section 3 is divided into two subsections presenting the theory parameters used to obtain Hamilton's quaternions (3.1), and the formalization


■ **Specification 1** Quaternion addition and scalar multiplication [quaternion\\_def](#) 

```

+(u,v): quat = ( u'x + v'x, u'y + v'y, u'z + v'z, u't + v't ) ;
*(c,v): quat = ( c * v'x, c * v'y, c * v'z, c * v't ) ;
                                                    %scalar multiplication
* :[quat,quat -> quat] ;
                                                    %quaternion multiplication

```

of the completeness of this structure to deal with 3D vector rotations (3.2). Finally, before concluding and discussing future lines of research in Section 5, Section 4 briefly discusses how other structures of quaternions can be specified.


The paper includes links to the specific points of the specification. The formalization is part of the PVS nasalib theory [algebra](#) . Formalizations in PVS are given in two files with extensions *.pvs* and *.prf*. The former contains the specifications, whereas the latter contains the proofs. The system itself, as well as relevant documentation about it, can be found in [1]. Also, an extension for PVS is available for VSCode [15].

## 2 Mechanization of the theory of quaternions

This section presents the formalization of the theory of quaternions using as a parameter an algebraic field and two constants:  $\langle \mathbb{F}, +_{\mathbb{F}}, *_{\mathbb{F}}, \text{zero}_{\mathbb{F}}, \text{one}_{\mathbb{F}}, a, b \rangle$ .

### 2.1 Specification of Basic Notions

The general theory of quaternions is built from any abstract type  $T$ , with binary operators for addition and multiplication  $+, * : [T, T] \rightarrow T$ , with constants  $\text{zero}, \text{one}, a, b : T$ .

Initially, in the theory defining the structure and type `quat`, [quaternion\\_def](#) , it is only assumed that  $[T, +, \text{zero}]$  is a group: `group?(fullset[T])`. An element  $q$  of type `quat` is a quadruple of elements of type  $T$ , represented as  $q = (x, y, z, t)$ , and through the use of a macro, components of  $q$  can be accessed, for instance  $q.y = y$ . Quadruples for the quaternion basis  $1, i, j, k$ , and for quaternions  $a$  and  $b$  are defined; distinguishing them with names `one_q, i, j, k, a_q, b_q`. The substring `_q` refers to quaternions. Thus, field elements with the suffix `_q` refer to the associated quaternions; for instance, `a_q` refers to the quaternion  $(a, \text{zero}, \text{zero}, \text{zero})$ , and `zero_q` specifies the zero quaternion. The conjugate and the additive inverse of a quaternion are specified in the usual manner: they are well-defined since  $[T, +, \text{zero}]$  is a group, and each element of the quadruple has an additive inverse. Tuple addition and scalar multiplication are defined in Specification 1. Finally, note that quaternion multiplication is defined as a binary operator over quaternions.

The required axioms of the theory of quaternions are given in Specification 2, where variable types are  $u, v : \text{quat}$ , and  $c, d : T$ . Notice that the axioms include associativity and (right and left) distributivity of the quaternion multiplication over the addition (`q_assoc, q_distr` and `q_distr1`), and associativity and commutativity regarding scalar multiplication over quaternion multiplication (`sc_quat_assoc, sc_comm` and `sc_assoc`). Also, it is required that `one_q` be the identity for quaternion multiplication: the axioms `one_q_times` and `times_one_q` are essential to prove the characterization of the quaternion multiplication provided in the Subsection 2.2.

■ **Specification 2** [Axioms for the Theory of Quaternion](#) [↗](#)

```
sqr_i      :AXIOM i * i = a_q
sqr_j      :AXIOM j * j = b_q
ij_is_k    :AXIOM i * j = k
ji_prod    :AXIOM j * i = inv(k)
sc_quat_assoc :AXIOM c*(u*v) = (c*u)*v
sc_comm    :AXIOM (c*u)*v = u*(c*v)
sc_assoc   :AXIOM c*(d*u) = (c*d)*u
q_distr    :AXIOM distributive?[quat](*, +)
q_distr1   :AXIOM (u + v) * w = u * w + v * w
q_assoc    :AXIOM associative?[quat](*)
one_q_times :AXIOM one_q * u = u
times_one_q :AXIOM u * one_q = u
```

■ **Specification 3** [Quaternion Basis](#) [↗](#)

```
basis_quat: LEMMA
  FORALL (q: quat): q = q'x * one_q + q'y * i + q'z * j + q't * k
```

## 2.2 Inference of Algebraic Properties of Quaternions

The PVS theory [quaternions](#) [↗](#) completes the basic structure of quaternions, refining the parameters in such a manner that  $a$  and  $b$  are different from zero, and  $[T, +, *, \text{zero}, \text{one}]$  is a field (specified in theory [field\\_def](#) [↗](#)). So, the type  $T$  with addition and  $\text{zero}$ , as well as  $T - \{\text{zero}\}$  with multiplication and  $\text{one}$  are Abelian groups.

From this basis, it is now possible to infer a series of lemmas about quaternions, such as  $j*i = -(i*j)$ ,  $k*k = -a_q * b_q$ ,  $k * i = -a_q * j$ ,  $k * j = b_q * i$ ,  $i * k = a_q * j$ , and  $j * k = -b_q * i$  (see [basic lemmas](#) [↗](#)).

Such lemmas allow us to infer that quaternions  $\text{one}_q$ ,  $i$ ,  $j$ , and  $k$  act as a basis as given in Specification 3, and the characterization of quaternion multiplication as given in Specification 4. The proof of this characterization uses the decomposition according to the lemma [basis\\_quaternion](#) and requires exhaustive algebraic manipulation using quaternion axioms, a series of auxiliary lemmas, including the previous ones mentioned, and others about the algebra of quaternions, such as lemmas for the scalar product. The advantage of such formulation is that the characterization of quaternion multiplication, usually presented as a definition, is obtained from a minimal axiomatization.

Further results include the formalization of the fact that any quaternion abstract structure,  $\text{quat}[T, +, *, \text{zero}, \text{one}, a, b]$ , is a ring with identity as given in the Specification 5. A ring is not necessarily commutative regarding multiplication. The proof requires expanding the field definition for  $[T, +, *, \text{zero}, \text{one}]$ , then using that it is a commutative division ring, a commutative group with identity. From this, and the

■ **Specification 4** [Quaternion Multiplication Characterization](#) [↗](#)

```
q_prod_charac: LEMMA FORALL (u,v:quat):
  u * v = (u'x * v'x + u'y * v'y * a + u'z * v'z * b + u't * v't * inv(a)*b,
          u'x * v'y + u'y * v'x + (inv(b)) * u'z * v't + b * u't * v'z,
          u'x * v'z + u'z * v'x + a * u'y * v't + inv(a) * u't * v'y,
          u'x * v't + u'y * v'z + inv(u'z * v'y) + u't * v'x );
```


■ **Specification 5** [Quaternions are Rings with identity](#) 


```
quat_is_ring_w_one: LEMMA
  ring_with_one?[quat,+,*,zero_q,one_q](fullset[quat])
```

■ **Specification 6** [Conjugate of Multiplication of Quaternions](#) 

```
conj_product_quat : LEMMA FORALL(q, u : quat) :
  conjugate(q * u) = conjugate(u) * conjugate(q)
```



algebraic properties inferred until this point, it is possible to prove that the structure of quaternions given as  $[\text{quat}[T,+,*,\text{zero},\text{one},a,b], +, *, \text{zero}_q, \text{one}_q]$  is indeed a ring with identity. The last is done expanding the notion of ring-with-identity and proving first that  $[\text{quat}[T,+,*,\text{zero},\text{one},a,b], +, *, \text{zero}_q]$  is a ring, and then that  $[\text{quat}[T,+,*,\text{zero},\text{one},a,b], *, \text{one}_q]$  is a monoid.

Some of the formalizations benefit from PVS strategies to automatize manipulation of the algebra of quaternions. For instance, the lemma in Specification 6 states that for quaternions  $q, u$ ,  $\text{conjugate}(q * u) = \text{conjugate}(u) * \text{conjugate}(q)$ , where [conjugate\(u\)](#)  is given by the quaternion  $(u'x, -u'y, -u'z, -u't)$ . The proof of this lemma is done by applying the theorem of characterization of quaternion multiplication [q\\_prod\\_charac](#), showing that each pair of corresponding components of the resulting quadruples are equal. Quaternions' operations are defined from addition and multiplication over arbitrary fields. PVS allows the manipulation of numerical algebraic structures, such as the field of reals. Indeed, Manip is a package of PVS tactics that simplify numerical manipulation [8]. However, it does not support algebraic manipulations over arbitrary fields.

Simple strategies were developed to handle quaternions' operations [PVS strategies](#) . Roughly, a strategy in PVS is a proof script that can be applied as a PVS proof command to improve automation. For instance, at some point in the proof, one must show that the quadruples' first components coincide with the corresponding equation presented below. However, proving this equality is not straightforward, requiring exhaustive applications of quaternions' addition and multiplication properties, which justified the development of such strategies.

$$\begin{aligned} &-(q'x * u't + q'y * u'z + -(q'z * u'y) + q't * u'x) = \\ &-(u'x * q't) + u'y * q'z + -(u'z * q'y) + -(u't * q'x) \end{aligned}$$

Some additional lemmas and definitions are formalized to characterize quaternions as division rings.

Two important predicates and subtypes of `quat` are defined, the type of pure quaternions, [pure\\_quat](#) , and the type of scalar quaternions, [scalar\\_F](#) , which consists of quaternions with null scalar component and with null components  $i, j, k$ , respectively. Also, we specify the *reduced norm* of a quaternion  $q$  as  $\text{red\_norm}(q) = q * \text{conjugate}(q)$ . The lemmas obtained for such definitions cover the properties in the Specification 7, among others.

The lemma [center\\_quat\\_is\\_sc\\_F](#) expresses the fact that if the characteristic of the ring  $[T, +, *, \text{zero}]$  is different from two, i.e., there exists an element  $x \in T$  such that  $x + x \neq \text{zero}$ , the center of the structure built with the quaternions and its multiplication is exactly the subtype of all the scalar quaternions.

■ **Specification 7** Pure and Scalar Quaternions Conjugate and Norm Properties [↗](#)

```

red_norm_charac: LEMMA FORALL (q: quat):
  red_norm(q) = (q'x * q'x +
                inv(a) * (q'y * q'y) +
                inv(b) * (q'z * q'z) +
                (a * b) * (q't * q't),
                zero, zero, zero)

conj_product_quat_scalar : LEMMA FORALL(s : T, q : quat) :
  conjugate(s * q) = s * conjugate(q)

red_norm_conj: LEMMA FORALL(q:quat):
  red_norm(conjugate(q)) = red_norm(q)

center_quat_is_sc_F: LEMMA charac(fullset[T]) /= 2 IMPLIES
  center[(quat),*](fullset[quat]) = scalar_F

q_x_v_cq : LEMMA FORALL (q:quat, v:(pure_quat)) :
  pure_quat(q * v * conjugate(q))

```

■ **Specification 8**  $T_q(q)(v)$  Operator [↗](#)

```

T_q(q: quat)(v:(pure_quat)): (pure_quat) = q * v * conjugate(q)

T_q_is_linear: LEMMA FORALL (c,d: T, q: quat, v,w: (pure_quat)):
  T_q(q)(c * v + d * w) = c * T_q(q)(v) + d * T_q(q)(w)

T_q_red_norm_invariant: LEMMA FORALL (q: quat, v:(pure_quat)):
  red_norm(q) = one_q IMPLIES red_norm(T_q(q)(v)) = red_norm(v)

T_q_invariant_red_norm: LEMMA FORALL (c: T, q: quat):
  red_norm(q) = one_q IMPLIES T_q(q)(c * pure_part(q)) = c * pure_part(q)

```

The center of such structure is given by the quaternions that multiplicatively commute with all other quaternions:  $\{ q \mid \forall u : q * u = u * q \}$ . This theorem is obtained, proving that for any quaternion  $q$  in the center, commutativity with the basis quaternions  $i$ ,  $j$ ,  $k$  implies the pure components of  $x$  should be zero.

Finally, from the last lemma in Specification 7,  $q\_x\_v\_cq$ , the transformation given as the curried operator  $T_q(q:quat)(v:(pure\_quat))$  is specified, and crucial properties about it are proved, as presented in Specification 8. Such properties express the linearity of the operator,  $T\_q\_is\_linear$ ; the fact that if the  $red\_norm$  of  $q$  is one, the resulting transformation of the pure quaternion  $v$ ,  $T\_q(q)(v)$ , has the same norm as  $v$ ; and, that the transformation over the pure quaternion  $pure\_part(q)$ , obtained from  $q$ , does not affect any multiple of it. In fact, the last lemma could be obtained by proving that  $T\_q(q)(pure\_part(q))=pure\_part(q)$  and by the fact that  $T\_q(q)$  is linear.

Quaternions of characteristic two require specialized definitions but are not the subject of this paper (e.g., Chapter six of [22]).

## 2.3 Characterization of Quaternions as Division Rings

The characterization of quaternions as division rings is given by a series of six lemmas presented in Specification 9.

The first lemma, `nz_red_norm_if_inv_exist`, is proved constructively. Assuming  $\text{red\_norm}(q) \neq \text{zero\_q}$ , using the characterization of `red_norm` in Specification 7, one has that the scalar component of  $\text{red\_norm}(q) = q'x * q'x + -(a) * (q'y * q'y) + -(b) * (q'z * q'z) + (a * b) * (q't * q't)$  is not null and consequently has a multiplicative inverse in the field, say  $y$ . From this, one builds the desired quaternion multiplicative inverse of  $q$  as the quaternion  $\text{conjugate}(q) * (y * \text{one\_q})$ . We have to consider the quaternion  $y * \text{one\_q}$  in the previous multiplication since  $y$  is a scalar. The exhaustive job is once again related to the algebraic manipulation to prove that  $q * (\text{conjugate}(q) * (y * \text{one\_q})) = \text{one\_q}$  and vice-versa. This involves repeated applications of the characterization of quaternion multiplication, the definition and characterization of `red_norm`, and several algebraic properties of quaternions.

The second lemma in Specification 9, `div_ring_iff_nz_rednorm`, established that a quaternion is a division ring exactly when all non-zero quaternions have a reduced norm different from `zero_q`. Necessity is proved by contradiction, assuming the existence of an inverse for  $q$ , say  $y * q = \text{one\_q}$ . Then, by expanding the definition of reduced norm, one obtains  $q * \text{conjugate}(q) = \text{zero\_q}$ . From these equations, by simple algebraic manipulations, one obtains  $y * (q * \text{conjugate}(q)) = \text{one\_q} * \text{conjugate}(q)$ , and finally one obtains  $\text{zero\_q} = \text{conjugate}(q)$ , which contradicts the assumption that  $q \neq \text{zero\_q}$ . The proof of sufficiency is obtained by applying the first lemma.

The third lemma in Specification 9, `inv_q_prod_charac`, characterizes the inverse of a non `zero_q` quaternion  $q$  through the equation  $\text{inv}(q) = \text{conjugate}(q) * \text{inv}(\text{red\_norm}(q))$  whenever the quaternion structure is a division ring. This lemma uses the previous one and exhaustive algebraic manipulation. The key of the proof is to show that  $\text{conjugate}(q) * (\text{red\_norm}(q))^{-1}$  is the inverse of  $q$ . This is proved showing that  $q * (\text{conjugate}(q) * (\text{red\_norm}(q))^{-1}) = \text{one\_q}$  and  $(\text{conjugate}(q) * (\text{red\_norm}(q))^{-1}) * q = \text{one\_q}$ . The former equation requires only associativity and expansion of the definition of `red_norm` to obtain the equation  $(q * \text{conjugate}(q)) * (q * \text{conjugate}(q))^{-1} = \text{one\_q}$ , from which one concludes. The latter equation requires the application of the previous lemma to obtain the multiplicative inverse of `red_norm`, say  $y$ , such that  $\text{red\_norm}(q) * y = \text{one\_q}$ . Expanding the definition of `red_norm`, one obtains the equation  $(q * \text{conjugate}(q)) * y = \text{one\_q}$ . In this manner, one obtains the equation  $q * ((\text{conjugate}(q) * y) * q) = q * \text{one\_q}$ , from which one concludes.

The fourth lemma in Specification 9, `quat_div_ring_aux1`, is a simple auxiliary result from the theory of fields. If  $t = \text{zero}$ , the type of  $a$  implies  $-a \neq \text{zero}$ . For the case in which  $t \neq \text{zero}$ , after Skolemization, one obtains the premise  $t*t = a$ ; also,  $t$  has a multiplicative inverse, say  $y$ . Then, by instantiating the premise with  $y$  and  $\text{zero}$ , one obtains objective equality  $a*(y*y) + b * \text{zero} = \text{one}$ . By replacing  $a$  with  $t*t$ , one obtains  $(t*t)*(y*y) = \text{one}$ . The formalization, as expected, requires simple field algebraic manipulations.

The fifth lemma, `quat_div_ring_aux2`, is another auxiliary result on fields. When  $t = \text{zero}$ , one concludes by the inequation results from the type of  $b$ . Otherwise, let  $y$  and  $y1$  be the multiplicative inverses of  $t$  and  $a + a$ , respectively. Notice that since the characteristic of the field is different from two,  $a + a \neq \text{zero}$ , allowing the use of the latter inverse. The second premise is then instantiated with  $(\text{one} + a) * y1$  and  $(\text{one} - a) * y1 * y$  giving the objective

$$a((\text{one} + a) * y1)^2 + b((\text{one} - a) * y1 * y)^2 = \text{one}$$

Algebraic manipulation transforms the left-hand side of this equation into the term below,

■ **Specification 9** Characterization of Quaternions as Division Rings [↗](#)

```

nz_red_norm_iff_inv_exist: LEMMA
  (FORALL (q:nz_quat):
    red_norm(q) /= zero_q) IFF
    inv_exists?[quat,*,one_q](remove(zero_q, fullset[quat]))

div_ring_iff_nz_rednorm: LEMMA
  division_ring?[quat,+,*,zero_q,one_q](fullset[quat]) IFF
  (FORALL(q: nz_quat): red_norm(q) /= zero_q)

inv_q_prod_charac: LEMMA
  division_ring?[quat,+,*,zero_q,one_q](fullset[quat]) IMPLIES
  (FORALL (q: nz_quat):
    inv[nz_quat,*,one_q](q) = conjugate(q)*inv[nz_quat,*,one_q](red_norm(q)))

quat_div_ring_aux1: LEMMA
  (FORALL (x,y:T): a * (x*x) + b * (y*y) /= one) IMPLIES
  (FORALL (t:T): t*t + inv[T,+,zero](a) /= zero)

quat_div_ring_aux2: LEMMA
  (charac(fullset[T]) /= 2 AND (FORALL (x,y:T): a * (x*x)+b * (y*y) /= one))
  IMPLIES
  (FORALL (t:T): a*(t*t) + b /= zero)

quat_div_ring_char: LEMMA
  charac(fullset[T]) /= 2 IMPLIES
  ((FORALL (x,y:T): a*(x*x) + b*(y*y) /= one) IFF
  division_ring?[quat,+,*,zero_q,one_q](fullset[quat]))

```

where for the integer  $k$ ,  $k$   $t$  abbreviates  $t+t+\dots+t$   $k$  times.

$$a * y1^2 + 2(a^2 * y1^2) + a^3 * y1^2 + b * y1^2 * y^2 + 2(b * (-a) * y1^2 * y^2) + b * (-a)^2 * y1^2 * y^2$$

By multiplying  $a*(t*t) + b = \text{zero}$  by  $y * y$ , one obtains the equation  $a + b (y * y) = \text{zero}$ , which allows the elimination of the first and second component of the above term; indeed

$$a * y1^2 + b * y1^2 * y^2 = (a + b * y^2)y1^2 = \text{zero}$$

The third and last components are also eliminated:

$$a^3 * y1^2 + b * (-a)^2 * y1^2 * y^2 = (a + b * y^2) * a^2 * y1^2 = \text{zero}$$

Finally, the remaining four components are proved equal to **one** using the equation  $-b * (y * y) = a$ :

$$2(a^2 * y1^2) + 2(b * (-a) * y1^2 * y^2) = 4(a^2 * y1^2) = (a + a) * (a + a) * y1^2 = \text{one}$$

The final lemma, `quat_div_ring_char`, states that the structure of quaternions with multiplication is a division ring whenever the characteristic of the ring  $[T, +, *, \text{zero}]$  with field multiplication is different from two and the condition  $\forall x, y \in T : a * x^2 + b * y^2 \neq \text{one}$ , used in previous two lemmas, holds. The proof applies the second lemma in the series of lemmas given in Specification 9, `div_ring_iff_nz_rednorm`, thus, changing the objective to proving that  $\text{red\_norm}(q) \neq \text{zero}_q$ , for any  $q \neq \text{zero}_q$  under these conditions.

On the one side, if there exists  $x, y$  in the field such that  $a * x^2 + b * y^2 = \text{one}$ , one can select the quaternion element  $q = \text{one}_q + x * i + y * j$ . So,  $q \neq \text{zero}_q$ , and its reduced norm,  $1 - a * x^2 - b * y^2$  is different from **zero**. Therefore, the quaternion cannot be a



division ring. On the other side, suppose the quaternion is not a division ring, but the condition  $\forall x, y \in T : a * x^2 + b * y^2 \neq \text{one}$  holds. Then, there exists  $q \neq \text{zero}_q$  such that  $\text{red\_norm}(q) = q'x^2 - a * q'y^2 - b * q'z^2 + a * b * q't^2 = \text{zero}_q$ . For short, let this  $q$  be equal to  $(x, y, z, t)$ .

The first component of the reduced norm gives the field equation:

$$x^2 - a * y^2 - b * z^2 + a * b * t^2 = \text{zero} \quad (1)$$

From the last equation, one has that  $x^2 - a * y^2 = b * (z^2 - a * t^2)$ . From this equation, one obtains  $(x^2 - a * y^2) * (z^2 - a * t^2) = b * (z^2 - a * t^2)^2$ . This equation gives

$$(x^2 * z^2 + a^2 * y^2 * t^2 - a * x^2 * t^2 - a * y^2 * z^2) = b * (z^2 - a * t^2)^2$$

From the last equation, one obtains

$$a * (x * t + y * z)^2 + b * (z^2 - a * t^2)^2 = (x * z + a * y * t)^2 \quad (2)$$

Notice that  $(x * z + a * y * t) = \text{zero}$ ; otherwise, multiplying the equation by the square of the inverse of this term, one contradicts the hypothesis  $\forall x, y \in T : a * x^2 + b * y^2 \neq \text{one}$ . Therefore, equation (2) becomes:

$$a * (x * t + y * z)^2 + b * (z^2 - a * t^2)^2 = \text{zero} \quad (3)$$

Suppose now that  $z^2 - a * t^2 \neq \text{zero}$ . Thus, multiplying the equation by the square of the inverse of this term, one obtains an equation of the form  $a * t'^2 + b = \text{zero}$ , which gives a contradiction by lemma `quat_div_ring_aux2`. Thus,  $z^2 - a * t^2 = \text{zero}$ .

Assume now that  $t \neq \text{zero}$ . Multiplying by the square of the inverse of  $t$ , one obtains an equation of the form  $t'^2 - a = \text{zero}$ , which gives a contradiction by lemma `quat_div_ring_aux1`. Therefore, the fourth component of the quaternion element  $q$  is zero:  $t = \text{zero}$ , which also implies the third component  $z = \text{zero}$ .

Thus the reduced norm of  $q$  is equal to  $x^2 - ay^2$ , and by hypothesis,  $x^2 - ay^2 = \text{zero}$ . Once again, if  $y \neq \text{zero}$ , multiplying the equation by the square of the inverse of  $y$ , one obtains an equation of the form  $t'^2 - a = \text{zero}$ , which gives a contradiction by lemma `quat_div_ring_aux1`. So,  $y = \text{zero}$ , and also  $x = \text{zero}$ .

This completes the proof.

### 3 Parameterization of the Algebra of Hamilton's Quaternions

By providing parameters `quaternions[real,+,*,0,1,-1,-1]` to the theory `quaternions` [↗](#), one obtains Hamilton's quaternions,  $\mathbb{H}$ , mentioned in the introduction. This structure is usually characterized in textbooks by the identities  $i^2 = j^2 = k^2 = ijk = -1$  (e.g., [22]). In this section, we will present the completeness of 3D rotation by using Hamilton's quaternion, as well as the main properties to achieve such results formalized in the PVS theory `quaternions_Hamilton` [↗](#). In this section, "quaternions" reference elements of the structure of Hamilton's quaternions.

#### 3.1 Specification of Basic Properties

The structure given by  $(\mathbb{H}, +_{\mathbb{H}}, \text{zero}_q, *_{\mathbb{R}})$ , where  $*_{\mathbb{R}}$  indicates the scalar product induced by the multiplication over real numbers, is a vector space isomorphic to  $\mathbb{R}^4$  equipped with their standard operations. A pure part of a quaternion can be mimicked by a vector from

## 11:10 A Formalization of the General Theory of Quaternions

### ■ Specification 10 [Connection between quaternions and vectors](#)

```
Real_part(q: quat): real = q.x

Vector_part(q: quat): Vect3 = (q.y, q.z, q.t)

conversion_quot: LEMMA
  FORALL(r: real, nz: nzreal): r/nz = number_fields./(r,nz)

quat_is_Real_p_Vector_part: LEMMA
  FORALL (q: quat):
    q = (Real_part(q), Vector_part(q).x, Vector_part(q).y, Vector_part(q).z)

decompose_eq_Real_Vector_part: LEMMA
  FORALL (q, p : quat):
    Real_part(q) = Real_part(p) AND Vector_part(q) = Vector_part(p) IFF
    q = p

Vector_part_scalar: LEMMA
  FORALL (k:real, q: quat): Vector_part(k*q) = k * Vector_part(q)
```

$\mathbb{R}^3$  and has a fundamental role in the theorems regarding the completeness of 3D rotations. To reuse results about real vectors, formalized in theory [vectors](#) in PVS nasalib, we specified operators that return the real and pure part of a quaternion as a real number and a three-dimensional vector, respectively, and formalized basic properties about them (see Specification 10).

### 3.2 Rotational completeness of Hamilton's Quaternions

Hamilton's quaternions is a suitable structure to perform rotations in  $\mathbb{R}^3$ , and it has some advantages when compared with techniques based on rotating by Euler angles:

- The rotation using quaternions relies on the application of the linear transformation  $T_q(q)(v)$ , defined in Specification 8. This operator is based on the multiplication of three quaternions which, in the light of the lemma [q\\_prod\\_charac](#), is computed using multiplication and sum of real numbers in this context. On the other hand, rotating by Euler angles relies on the multiplication of three matrices of order 3, whose entries contain trigonometric functions, each one of these matrices represents a rotation around the axes  $x, y$ , and  $z$  of a 3D coordinate system (e.g., Chapter 4 in [3], and [19]). Thus, Hamilton's quaternions provide a computational, more efficient manner to perform rotations.
- Rotating by Euler angles can lead to a *gimbal lock*. This well-known phenomenon occurs when two axes align, causing the loss of one degree of freedom and *locking* the system to rotate in a degenerated two-dimensional space [10]. Hamilton's quaternions avoid *gimbal lock*.
- A rotation by Euler angles is based on the composition of rotations around three axes, e.g., yaw, pitch, and roll. In contrast, only the pure part of a quaternion element  $q$  defines the axis of a rotation using Hamilton's quaternions [10]. Therefore, it is easier to visualize the transformation by quaternions.

The landmark results of this section, presented in the Specification 11, are the formalizations of theorems [Quaternions\\_Rotation](#) and [Quaternions\\_Rotation\\_Deform](#). The former states that given two pure quaternions  $a$  and  $b$ , which can be identified as vectors of  $\mathbb{R}^3$  of the same norm, there is a quaternion  $q = \text{rot\_quat}(a, b)$  such that the operator

■ **Specification 11** Completion of rotation using Hamilton's quaternions [↗](#)

```

Quaternions_Rotation: THEOREM
  FORALL (a:(pure_quat), b:(pure_quat) |
    norm(Vector_part(a)) = norm(Vector_part(b)) AND
    linearly_independent?(Vector_part(a), Vector_part(b))):
    LET q = rot_quat(a,b) IN b = T_q(q)(a)

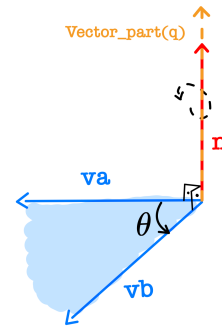
Quaternions_Rotation_Deform: THEOREM
  FORALL (a:(pure_quat), b:(pure_quat) |
    linearly_independent?(Vector_part(a), Vector_part(b))):
    LET q =
      (sqrt(number_fields./(norm(Vector_part(b)),norm(Vector_part(a))))*
        rot_quat(a,
          number_fields./(norm(Vector_part(a)),norm(Vector_part(b)))*b)
    IN b = T_q(q)(a)

```

$T_q(q)$  rotates  $a$  into  $b$ . The latter theorem ensures the existence of a quaternion  $q$  such that the operator  $T_q(q)$  transforms  $a$  into  $b$ , even when they are not, necessarily, of the same length. For the second transformation, it is only needed multiplying  $\text{rot\_quat}\left(a, \frac{|a|}{|b|}b\right)$  by

the scalar  $\sqrt{\frac{|a|}{|b|}}$ , where  $|v|$  denotes the usual norm of  $v$  in  $\mathbb{R}^3$ .

The following will highlight the main steps to formalize those theorems. Initially, consider two pure quaternions  $a$  and  $b$  such that  $va = \text{Vector\_part}(a)$  and  $vb = \text{Vector\_part}(b)$  are linearly independent; i.e., such vectors are nonparallel and non-null. Let  $\theta$  be the smallest angle between  $va$  and  $vb$  and consider  $n = \frac{va \times vb}{|va||vb|}$ , where  $va \times vb$  denotes the usual cross product of vectors in  $\mathbb{R}^3$ . The idea is to consider  $n$  as the rotation axis and built the quaternion  $q$  that leads  $a$  into  $b$  from  $\theta$  and  $n$ , as follows:



$$q = \left( \cos\left(\frac{\theta}{2}\right), n'_x * \sin\left(\frac{\theta}{2}\right), n'_y * \sin\left(\frac{\theta}{2}\right), n'_z * \sin\left(\frac{\theta}{2}\right) \right)$$

The elements  $\theta$ ,  $n$  and  $q$  were specified as  $r\_angle(a,b)$  [↗](#),  $n\_rot\_axis(a,b)$  [↗](#), and  $rot\_quat(a,b)$  [↗](#), respectively (See Specification 12). They use some structures formalized in the theories [vectors](#) [↗](#) and [trig](#) [↗](#) in the PVS nasalib. For example,  $r\_angle(a,b)$  is formalized from the operator  $angle\_between(\text{Vector\_part}(a), \text{Vector\_part}(b))$  [↗](#), which, in turn, is specified by using the `arccosine` function and the usual *inner product* of  $\mathbb{R}^3$ ; whereas,  $n\_rot\_axis(a,b)$  uses the specification of *cross product* defined as the vector  $cross(a,b)$  [↗](#). Notice that  $r\_angle(a,b)$  [↗](#) has type `nnreal_le_pi`, inheriting the adequate type (reals in the interval  $(0, \pi]$ ) in which the function `acos` is specified in the PVS trigonometry library.

Four main lemmas are needed to formalize the Theorem [Quaternions\\_Rotation](#) [↗](#).

The first one consists of a characterization of the operator  $T_q(q)(a)$  specified as the lemma [T\\_q\\_Real\\_charac](#) [↗](#). According to this result, for any quaternion  $q$  and any pure quaternion  $a$ , the following equality holds:

## 11:12 A Formalization of the General Theory of Quaternions

### ■ Specification 12 Basic elements to built a rotation by quaternions [↗](#)

```

r_angle(a,b:(nzpure_quat)): nreal_le_pi =
    angle_between(Vector_part(a),Vector_part(b))

n_rot_axis(a:(pure_quat),b:(pure_quat) |
    linearly_independent?(Vector_part(a), Vector_part(b))): Vect3 =
    normalize(cross(Vector_part(a), Vector_part(b)))

rot_quat(a:(pure_quat),b:(pure_quat) |
    linearly_independent?(Vector_part(a), Vector_part(b))): quat =
    LET rot_angl_halve : nreal_le_pi = number_fields./(r_angle(a,b), 2),
        sin_ha = sin(rot_angl_halve),
        cos_ha = cos(rot_angl_halve),
        n = n_rot_axis(a,b)
    IN (cos_ha, sin_ha * n'x, sin_ha * n'y, sin_ha * n'z)

```

$$\begin{aligned} \text{Vector\_part}(T\_q(q)(a)) &= ((q'x)^2 - |\text{Vector\_part}(q)|^2) * va && + \\ & (2 * (\text{Vector\_part}(q) * va)) * \text{Vector\_part}(q) && + \quad (4) \\ & (2 * q'x) * (\text{Vector\_part}(q) \times va) \end{aligned}$$

In Equation 4, the multiplication  $v * w$  between vectors is interpreted as the dot product.

The vector part of  $T\_q(q)(a)$  expresses all the relevant information of the resulting quaternion: since the type established for  $T\_q(q)(a)$  is `pure_quat`, see Specification 8, the prover automatically generates a *proof obligation*, called in PVS *Type Correctness Condition (TCC)*, to verify that the first component of this quaternion is zero. Also, according to the lemma `T_q_is_linear`, showed in Specification 8,  $T\_q(q)(a)$  is a linear transformation. And since  $|q| = 1$ , it preserves the norm of  $|a|$ , acting as a rotation.

The other three key lemmas consist of established equivalent expressions for each term in the addition appearing in `T_q_Real_charac`, see Equation 4.

The lemma `Quat_Rot_Aux1` [↗](#) ensures that  $\text{Vector\_part}(q) * va = 0$ . Consequently, the equation  $(2 * (\text{Vector\_part}(q) * va)) * \text{Vector\_part}(q) = 0$  also holds.

The formalization of this lemma applies the lemma `orth_cross` [↗](#), of the PVS theory `vectors`, that guarantees that the vectors  $(va \times vb)$  and  $va$  are orthogonal. This is a consequence of the equalities  $\text{Vector\_part}(q) = \sin\left(\frac{\theta}{2}\right) * n = \frac{\sin\left(\frac{\theta}{2}\right)}{|va||vb|} * (va \times vb)$ .

The lemma `Quat_Rot_Aux2` [↗](#) establishes the equality

$$((q'x)^2 - |\text{Vector\_part}(q)|^2) * va = \cos(\theta) * va$$

By definition of  $q$  and since  $|n| = 1$ ,

$$(q'x)^2 - |\text{Vector\_part}(q)|^2 = \cos^2\left(\frac{\theta}{2}\right) - \sin^2\left(\frac{\theta}{2}\right) * |n|^2 = \cos^2\left(\frac{\theta}{2}\right) - \sin^2\left(\frac{\theta}{2}\right)$$

Thus, `Quat_Rot_Aux2` follows as a consequence of the lemma `cos_2a` [↗](#), formalized in the theory `trig@trig_basic`, from which one can infer that  $\cos^2\left(\frac{\theta}{2}\right) - \sin^2\left(\frac{\theta}{2}\right) = \cos(\theta)$ .

Finally, in the lemma `Quat_Rot_Aux3` [↗](#), it is formalized that

$$(2 * q'x) * (\text{Vector\_part}(q) \times va) = vb - \cos(\theta) * va$$

In fact, by definition of  $q$  and  $n$ , and the associative property for scalar elements, one can infer that:

$$(2 * q'x) * (\text{Vector\_part}(q) \times va) = \left( 2 \cos\left(\frac{\theta}{2}\right) \sin\left(\frac{\theta}{2}\right) \frac{1}{|va \times vb|} \right) ((va \times vb) \times va)$$

Applying the lemmas [cross\\_cross](#) and [sin\\_2a](#), specified in theories `vectors@cross_3D` and `trig@trig_basic`, respectively, one obtains the equality

$$\left( 2 \cos\left(\frac{\theta}{2}\right) \sin\left(\frac{\theta}{2}\right) \frac{1}{|va \times vb|} \right) ((va \times vb) \times va) = \frac{\sin(\theta)}{|va \times vb|} ((va * va) * vb - (vb * va) * va)$$

Since,  $(va * va) = |va|^2$  and  $(vb * va) = \cos(\theta)|va||vb|$ , it holds that

$$\frac{\sin(\theta)}{|va \times vb|} ((va * va) * vb - (vb * va) * va) = \frac{\sin(\theta)}{|va \times vb|} (|va|^2 * vb - (\cos(\theta) * |va||vb|) * a)$$

Thus, by using the fact the  $|va| = |vb|$  and applying the identity  $|va \times vb| = |va||vb|\sin(\theta)$ , formalized in the lemma [norm\\_cross\\_charac](#) of the theory `vectors`, one obtains the equality

$$\frac{\sin(\theta)}{|va \times vb|} (|va|^2 * vb - (\cos(\theta) * |va||vb|) * va) = vb - \cos(\theta)va$$

The Theorem [Quaternions\\_Rotation](#) is then obtained as a direct consequence of the lemmas `T_q_Real_charac`, `Quat_Rot_Aux1`, `Quat_Rot_Aux2` and `Quat_Rot_Aux3`.

The formalization of the Theorem [Quaternions\\_Rotation\\_Deform](#) ensures that Hamilton's quaternions are useful to promote not only rotations in  $\mathbb{R}^3$  but also linear scaling since the transformation  $T_q(q)(a)$  maps  $a$  into  $b$  even when they are not of the same length.

For this, we have only to consider  $q = \sqrt{\frac{|b|}{|a|}} * \text{rot\_quat}\left(a, \frac{|a|}{|b|}b\right)$ . In fact, using this  $q$  as argument of the transformation,

$$T_q(q)(a) = \sqrt{\frac{|b|}{|a|}} * \text{rot\_quat}\left(a, \frac{|a|}{|b|}b\right) * a * \text{conjugate}\left(\sqrt{\frac{|b|}{|a|}} * \text{rot\_quat}\left(a, \frac{|a|}{|b|}b\right)\right)$$

Then, applying the lemma [conj\\_product\\_quat\\_scalar](#), behind some algebraic manipulations, it holds that

$$\begin{aligned} T_q(q)(a) &= \sqrt{\frac{|b|}{|a|}} * \sqrt{\frac{|b|}{|a|}} * \text{rot\_quat}\left(a, \frac{|a|}{|b|}b\right) * a * \text{conjugate}\left(\text{rot\_quat}\left(a, \frac{|a|}{|b|}b\right)\right) \\ &= \frac{|b|}{|a|} * T_q\left(\text{rot\_quat}\left(a, \frac{|a|}{|b|}b\right)\right)(a) \end{aligned}$$

Finally, since  $|\text{Vector\_part}(a)| = \left|\text{Vector\_part}\left(\frac{|a|}{|b|}b\right)\right|$ , the proof of the Theorem [Quaternions\\_Rotation\\_Deform](#) is completed instantiating [Quaternions\\_Rotation](#) with the pure quaternions  $a$  and  $\frac{|a|}{|b|}b$ , which guarantees that

$$T_q\left(\text{rot\_quat}\left(a, \frac{|a|}{|b|}b\right)\right)(a) = \frac{|a|}{|b|}b,$$

and, consequently, that  $T_q(q)(a) = b$ .

It is important to note that only the crucial lemmas for formalizing the previous results were highlighted. Although the automation for the simplification of equations over reals is in an advanced stage in PVS, several algebraic manipulations involving associative property for scalars, characterization of the norm of a vector, and properties derived from linear independence, among others, were necessary to conclude the formal proofs.

#### 4 Theory Parameters to Specify other Quaternions

Quaternion theory, as defined in Section 1, can describe many algebraic structures. Depending on the field  $\mathbb{F}$  and  $a, b \in \mathbb{F}^\times$ , the subset of invertible elements of the field, some quaternion algebra can be isomorphic to the matrix ring  $M_2(\mathbb{F})$ . In these cases, we say that the quaternion algebra *splits over*  $\mathbb{F}$ . In fact, it has been proved that a quaternion algebra  $\left(\frac{a, b}{\mathbb{F}}\right)$ , which is not a division ring, is indeed isomorphic to  $M_2(\mathbb{F})$  [5].

An example is given by the quaternion built over the complex field:  $\left(\frac{a, b}{\mathbb{C}}\right) \xrightarrow{\sim} M_2(\mathbb{C})$ , in which not only, it splits for some values  $a, b \in \mathbb{C} \setminus \{0\} = \mathbb{C}^\times$ .

On the other hand, all  $\left(\frac{a, b}{\mathbb{F}}\right)$  that are not isomorphic to  $M_2(\mathbb{F})$  are division rings; an example are Hamilton's quaternions.

Another case of a quaternion that is a division ring is  $\left(\frac{a, p}{\mathbb{Q}}\right)$ , where  $p$  is an odd prime and  $a$  is a quadratic non-residue, or  $\left(\frac{a, p}{\mathbb{Q}_p}\right)$ , where  $\mathbb{Q}_p$  are the  $p$ -adic numbers and  $a, p$  having the same restrictions [22].

The formalization of the general theory of quaternions constitutes a starting point for dealing with other interesting applications of the theory of quaternions. Surveying only a few of the applications covered in Voight's book [22], we can mention the following: applications of quaternion algebras in analytic number theory, geometry (hyperbolic geometry and low-dimensional topology), arithmetic geometry, and supersingular elliptic curves. Also, Lewis surveys relevant applications of quaternion theory in several areas [14].

Many of these application topics use these different types of quaternions or their order. In this case, an order is understood as a subring of the quaternion algebra, which is also a lattice. In Voight's book [22], a more detailed description of interesting orders such as maximal order, Eichler order, and more general orders is given.

The Hurwitz quaternion order is one such maximal order used for proving theorems. This quaternion order is a subring of the quaternions  $\mathbb{H}$  and  $\left(\frac{-1, -1}{\mathbb{Q}}\right)$ , and is given by

$$H = \{\alpha\zeta + \beta i + \gamma j + \delta k \mid \alpha, \beta, \gamma, \delta \in \mathbb{Z}\}, \text{ where } \zeta = \frac{1}{2}(1 + i + j + k).$$

It is used to prove Lagrange's theorem that every positive integer is a sum of four squares. Furthermore, it is possible to prove that, short of commutativity,  $H$  has all the properties of Euclidean rings.

In the aforementioned proof of Lagrange's four-square theorem. Considering  $u, v \in \mathbb{H}$ :

$$u = a_0 + a_1 i + a_2 j + a_3 k, \text{ and } v = b_0 + b_1 i + b_2 j + b_3 k$$

Since  $\text{Red\_norm}(uv) = \text{Red\_norm}(u) * \text{Red\_norm}(v)$  [↗](#), the reduced norm in  $\mathbb{H}$  can be used to prove the Lagrange Identity in  $\mathbb{Z}$ :

$$(a_0^2 + a_1^2 + a_2^2 + a_3^2)(b_0^2 + b_1^2 + b_2^2 + b_3^2) = c_0^2 + c_1^2 + c_2^2 + c_3^2$$

where, by the characterization of quaternion multiplication:

$$\begin{aligned} c_0 &= a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 & c_1 &= a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2 \\ c_2 &= a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1 & c_3 &= a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0 \end{aligned}$$

With this identity and by restricting the domain from  $\mathbb{H}$  to  $H$ , we can change the original problem from finding a solution for all positive integers into finding it for all primes. In this manner, the four integer square problem is expressed using only quaternions, which turns the Number Theory problem into an easier algebraic one. A didactic proof approach appears in Chapter 7 of Herstein's textbook [12]. Among other formalized properties available in the PVS nasalib theory algebra [\[4\]](#), the mechanization of this theorem uses the first isomorphism theorem for rings and results about maximal ideals [7].

Among the interesting applications in physics, it is possible to express gravity as part of a simple quaternion wave equation [21], the four Maxwell equations as a nonhomogeneous quaternion wave equation, as well as the Klein-Gordon equation as a quaternion simple harmonic oscillator [20]. Furthermore, under some restrictions, it is possible to express a quaternion analog to the Schrödinger equation, a well-known differential equation that governs the behavior of wave functions in quantum mechanics. The Schrödinger equation gives the kinetic energy plus the potential. To do this, we first look at the quaternions as the external tensor product of a scalar and an  $\mathbb{R}^3$ -vector, denoted by  $(\mathbf{s}, \tilde{\mathbf{v}})$ , and write the quaternion in its polar form, namely:

$$\mathbf{q} = (\mathbf{s}, \tilde{\mathbf{v}}) = \|\mathbf{q}\| e^{\theta * \mathbf{I}} = \|\mathbf{q}\| (\cos(\theta) + \mathbf{I} * \sin(\theta)),$$

where  $\|\mathbf{q}\| = \sqrt{\mathbf{q} * \text{conjugate}(\mathbf{q})}$ ,  $\theta = \arccos\left(\frac{\mathbf{s}}{\|\mathbf{q}\|}\right)$ , and  $\mathbf{I} = \frac{\tilde{\mathbf{v}}}{\|\tilde{\mathbf{v}}\|}$ . Note that  $\mathbf{I}^2 = -1$ .

Next, it is necessary to determine the quaternion wave function,  $\psi$ . Therefore, consider the quaternion  $(\mathbf{t}, \tilde{\mathbf{R}})$  representing time and space, the quaternion  $(\mathbf{E}, \tilde{\mathbf{P}})$  representing the electric field and momentum, and the quaternion  $\mathbf{V}(0, \mathbf{X})$  representing the potential. Thus, with  $\hbar$  being the reduced Planck constant, we have:

$$\psi \equiv \frac{(\mathbf{t}, \tilde{\mathbf{R}}) * (\mathbf{E}, \tilde{\mathbf{P}})}{\hbar} = \frac{(\mathbf{E}\mathbf{t} - \tilde{\mathbf{R}} * \tilde{\mathbf{P}}, \mathbf{E} * \tilde{\mathbf{R}} + \tilde{\mathbf{P}} * \mathbf{t} + \tilde{\mathbf{R}} \times \tilde{\mathbf{P}})}{\hbar}$$

Passing  $\psi$  to its polar form, and assuming that  $\psi$  is normalized, we have the quaternion wave function:

$$\psi = e^{(\mathbf{E} * \mathbf{t} - \tilde{\mathbf{R}} * \tilde{\mathbf{P}}) * \mathbf{I} / \hbar}, \text{ where } \mathbf{I} = \frac{\mathbf{E} * \tilde{\mathbf{R}} + \tilde{\mathbf{P}} * \mathbf{t} + \tilde{\mathbf{R}} \times \tilde{\mathbf{P}}}{\|\mathbf{E} * \tilde{\mathbf{R}} + \tilde{\mathbf{P}} * \mathbf{t} + \tilde{\mathbf{R}} \times \tilde{\mathbf{P}}\|}$$

Now, the derivatives of  $\psi$  with respect to time and space give, respectively:

$$\frac{\partial \psi}{\partial \mathbf{t}} = \frac{\mathbf{E} * \mathbf{I}}{\hbar} \frac{\psi}{\sqrt{1 + \left(\frac{\mathbf{E} * \mathbf{t} - \tilde{\mathbf{R}} * \tilde{\mathbf{P}}}{\hbar}\right)^2}} \quad \text{and} \quad \nabla \psi = -\frac{\tilde{\mathbf{P}} * \mathbf{I}}{\hbar} \frac{\psi}{\sqrt{1 + \left(\frac{\mathbf{E} * \mathbf{t} - \tilde{\mathbf{R}} * \tilde{\mathbf{P}}}{\hbar}\right)^2}}$$

To achieve the objective, which is to establish an analog to the Schrödinger equation in terms of quaternions, it is necessary to consider some assumptions and verify the behavior of the quaternion wave function  $\psi$ . Among these assumptions are, for example, the conservation of energy and momentum and the assumption that  $\mathbf{E} * \mathbf{t} - \tilde{\mathbf{R}} * \tilde{\mathbf{P}} = 0$ . Therefore,

$$\frac{\partial \psi}{\partial \mathbf{t}} = \frac{\mathbf{E} * \mathbf{I}}{\hbar} \psi \Rightarrow -\mathbf{I} * \hbar \frac{\partial \psi}{\partial \mathbf{t}} = \mathbf{E} \psi \Rightarrow \mathbf{E} = -\mathbf{I} * \hbar \frac{\partial}{\partial \mathbf{t}}$$

## 11:16 A Formalization of the General Theory of Quaternions

$$\nabla\psi = -\frac{\tilde{\mathbf{P}} * \mathbf{I}}{\hbar}\psi \Rightarrow \mathbf{I} * \hbar\nabla\psi = \tilde{\mathbf{P}}\psi \Rightarrow \tilde{\mathbf{P}} = \mathbf{I} * \hbar\nabla$$

It is known that the momentum  $\tilde{\mathbf{P}}$  is the product of the mass,  $m$ , and velocity,  $v$ . Consequently,

$$\tilde{\mathbf{P}}^2 = (mv)^2 = 2m\frac{mv^2}{2} = 2m \text{ KE} = -\hbar^2\nabla^2 \Rightarrow \text{KE} = -\frac{\hbar^2}{2m}\nabla^2$$

Since the Hamiltonian  $\mathbf{H}$  corresponds to the total energy ( $\mathbf{E}$ ), that is, it is equal to the sum of the kinetic energy  $\text{KE}$  and the potential energy  $\mathbf{V}$ , we obtain the following equation, which is similar to the Schrödinger equation:

$$\mathbf{H}\psi = -\frac{\hbar^2}{2m}\nabla^2\psi + \mathbf{V} * \psi.$$

### 5 Conclusions and Future Work

Table 1 presents the number of lines in the proofs of the crucial lemmas and theorems on the characterization of quaternions as division rings and rotational completeness of Hamilton's quaternions formalized in the theories [quaternions](#) and [quaternions\\_Hamilton](#), respectively.

Although the complexity of proving rotational completeness is high, PVS supplies satisfactory algebraic automation of the field of reals  $\mathbb{R}$ , which makes the formalization of rotational completeness much simpler than the formalization of characterization of an arbitrary structure of quaternion as a division ring (observe the number of proof lines). Indeed, algebraic manipulation on standard number types, such as the type `real`, has been studied and implemented during the evolution of PVS, as reported by Muñoz and Mayero in [17] and di Vito in [8], among others. Although some simple strategies were developed in this work to apply automatically commutative and associative properties of the (general) field parameter over which quaternions were defined, the improvement of tactics and the availability of techniques to detect and cancel equal terms over algebraic theories as `field` and `quat` is indispensable. This will surely make it possible to simplify substantially the length of the proofs presented in Table 1 for the case of the theory of quaternions.















Possible future work includes formalizations of applications of quaternions theory in other areas as discussed in Section 4. For instance, a formalization of Lagrange's four-square theorem (in progress) required adequate parameters to the quaternion theory, proving that Hurwitz's substructure is indeed a ring and almost a Euclidean ring, except for commutativity. After such proof, a few more auxiliary arithmetic lemmas, such as Lagrange's Identity, which can turn the problem from finding solutions to all integers into finding for all primes, can be used for proving Lagrange's Theorem using quaternions.

In addition to the availability of the abstract theory of quaternions, other available PVS theories may be useful to formalize the application of quaternions in quantum mechanics discussed in Section 4. For instance, to specify quaternions in their polar form and the quaternion wave function, the core of theorems related to quaternion arithmetic and trigonometric theory should be useful; also, to formalize the Schrödinger equation, it will be extremely relevant to develop theorems or axioms on the differentiation of quaternions, and physics concepts, for example, momentum.

Of course, another urgent line of research is extending PVS tactics, strategies, and, in general, mechanisms of arithmetic manipulation for standard types as `int`, `nat`, and `reals` to abstract algebraic structures as `ring`, `field`, and `quat`.



■ **Table 1** Quantitative information.

Theory/Formula Name	Proof Line Numbers	Number of Proved Formulas
		Lemmas/Theorems
<a href="#">nz_red_norm_iff_inv_exist</a> 	125	1
<a href="#">div_ring_iff_nz_rednorm</a> 	95	1
<a href="#">inv_q_prod_charac</a> 	259	1
<a href="#">quat_div_ring_aux1</a> 	40	1
<a href="#">quat_div_ring_aux2</a> 	388	1
<a href="#">quat_div_ring_char</a> 	487	1
<a href="#">quaternions.pvs</a> 	10981	63
<a href="#">T_q_Real_charac</a> 	190	1
<a href="#">Quat_Rot_Aux1</a> 	10	1
<a href="#">Quat_Rot_Aux2</a> 	116	1
<a href="#">Quat_Rot_Aux3</a> 	106	1
<a href="#">Quaternions_Rotation</a> 	38	1
<a href="#">Quaternions_Rotation_Deform</a> 	94	1
<a href="#">quaternions_Hamilton.pvs</a> 	3662	30

## References

- 1 PVS system. <https://pvs.csl.sri.com/index.html>. Accessed: 2024-05-27.
- 2 Reynald Affeldt and Cyril Cohen. Formal Foundations of 3D Geometry to Model Robot Manipulators. In *Proceedings of the 6th ACM SIGPLAN Conference on Certified Programs and Proofs, CPP 2017, Paris, France, January 16-17, 2017*, pages 30–42. ACM, 2017. doi: 10.1145/3018610.3018629.
- 3 Howard Anton and Chris Rorres. *Elementary Linear Algebra: Applications Version*. John Wiley & Sons. Inc., 10th edition, 2010.
- 4 Mauricio Ayala-Rincón, Thaynara Arielly de Lima, André Luiz Galdino, and Andréia Borges Avelar. Formalization of Algebraic Theorems in PVS (Invited Talk). In *Proc. 24th International Conference on Logic for Programming, Artificial Intelligence and Reasoning LPAR*, volume 94 of *EPiC Series in Computing*, pages 1–10, 2023. doi:10.29007/7jbv.
- 5 Keith Conrad. Quaternion algebras. Accessed in March 13, 2024. URL: <https://kconrad.math.uconn.edu/blurbs/ringtheory/quaternionalg.pdf>.
- 6 Thaynara Arielly de Lima, Andréia Borges Avelar, André Luiz Galdino, and Mauricio Ayala-Rincón. Formalizing factorization on euclidean domains and abstract euclidean algorithms. *CoRR*, abs/2404.14920, 2024. In *Proceedings 18th Logical and Semantic Frameworks with Applications LSFA 2023*. doi:10.48550/arXiv.2404.14920.
- 7 Thaynara Arielly de Lima, André Luiz Galdino, Andréia Borges Avelar, and Mauricio Ayala-Rincón. Formalization of Ring Theory in PVS - Isomorphism Theorems, Principal, Prime and Maximal Ideals, Chinese Remainder Theorem. *J. Autom. Reason.*, 65(8):1231–1263, 2021. doi:10.1007/s10817-021-09593-0.
- 8 Ben L. Di Vito. *Manip User's Guide, Version 1.3*, 2012. URL: <https://pvs.csl.sri.com/doc/manip-guide.pdf>.
- 9 Andrea Gabrielli and Marco Maggesi. Formalizing Basic Quaternionic Analysis. In *Proceedings of the 8th International Conference on Interactive Theorem Proving, ITP*, volume 10499 of *Lecture Notes in Computer Science*, pages 225–240. Springer, 2017. doi: 10.1007/978-3-319-66107-0\_15.
- 10 Gökmen Günaşti. Quaternion algebra, their applications in rotations and beyond quaternions. Technical report, Linnaeus University, Digitala Vetenskapliga Arkivet, 2012.

- 11 William Rowan Hamilton. On quaternions, or on a new system of imaginaries in algebra. *Philosophical Magazine*, 25(3):489–495, 1844. doi:10.1080/14786444408645047.
- 12 Israel (Yitzchak) Nathan Herstein. *Topics in Algebra*. John Wiley and Sons, New York, Chichester, Brisbane, Toronto, Singapore, second edition, 1975.
- 13 Angeliki Koutsoukou-Argyaki. Octonions. *Arch. Formal Proofs*, 2018. URL: <https://www.isa-afp.org/entries/Octonions.html>.
- 14 David W. Lewis. Quaternion Algebras and the Algebraic Legacy of Hamilton’s Quaternions. *Irish Math. Soc. Bulletin*, 57:41–64, 2006. doi:10.33232/bims.0057.41.64.
- 15 Paolo Masci and Aaron Dutle. Proof Mate: An interactive proof helper for PVS (tool paper). In *Proceedings of the 14th International Symposium NASA Formal Methods, NFM 2022*, volume 13260 of *Lecture Notes in Computer Science*, pages 809–815. Springer International Publishing, 2022. doi:10.1007/978-3-031-06773-0\_44.
- 16 The mathlib Community. The Lean Mathematical Library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020*, pages 367–381. ACM, 2020. doi:10.1145/3372885.3373824.
- 17 César Muñoz and Micaela Mayero. Real Automation in the Field. Technical Report Interim report, No 39, NASA/ICASE, 2001.
- 18 Lawrence C. Paulson. Quaternions. *Arch. Formal Proofs*, 2018. URL: <https://www.isa-afp.org/entries/Quaternions.html>.
- 19 Logah Perumal. Euler angles: conversion of arbitrary rotation sequences to specific rotation sequence. *Comput. Animat. Virtual Worlds*, 25(5-6):521–529, 2014. doi:10.1002/CAV.1529.
- 20 Douglas Sweetser. Doing Physics with Quaternions, 2005. Accessed in March 13, 2024. URL: <https://theworld.com/~sweetser/quaternions/ps/book.pdf>.
- 21 Douglas Sweetser. Three Roads to Quaternion Gravity. In *APS March Meeting Abstracts*, volume 2019 of *APS Meeting Abstracts*, page T70.008, January 2019.
- 22 John Voight. *Quaternion Algebras*, volume GTM 288 of *Graduate Texts in Mathematics*. Springer Cham, 2021. doi:10.1007/978-3-030-56694-4.