A Formalization of the General Theory of Quaternions

Thaynara Arielly de Lima
Universidade Federal de Goiás, Brasil

André Luiz Galdino
Universidade Federal de Catalão, Brasil

Bruno Berto de Oliveira Ribeiro
Universidade de Brasília, Brasil

Mauricio Ayala-Rincón
Universidade de Brasília, Brasil

Abstract

This paper discusses the formalization of the theory of quaternions in the Prototype Verification System (PVS). The general approach in this mechanization allows for specification of arbitrary quaternion algebras parameterizing with the adequate field and constants. The theory includes characterizing algebraic properties that lead to constructing a quaternion structure that is a division ring. 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.

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.2024.69

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. Author partially funded by CNPq grant 313290/21-0.

Contents

Manuscript submitted to ITP 2024.
Editors: ITP 2024 PC chairs; Article No. 69; pp. 69:1–69:17
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

Quaternions is the theory of algebraic structures consisting of quadruples built over a field, $\langle \mathbb{F}, +_{\mathbb{F}}, *_{\mathbb{F}}, zero_{\mathbb{F}}, one_{\mathbb{F}} \rangle$ 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

$$(zero_{\mathbb{F}}, one_{\mathbb{F}}, zero_{\mathbb{F}}, zero_{\mathbb{F}})^2 = (a, zero_{\mathbb{F}}, zero_{\mathbb{F}}, zero_{\mathbb{F}})$$

$$(zero_{\mathbb{F}}, zero_{\mathbb{F}}, one_{\mathbb{F}}, zero_{\mathbb{F}})^2 = (b, zero_{\mathbb{F}}, zero_{\mathbb{F}}, zero_{\mathbb{F}})$$

$$(zero_{\mathbb{F}}, zero_{\mathbb{F}}, one_{\mathbb{F}}, zero_{\mathbb{F}}) * (zero_{\mathbb{F}}, one_{\mathbb{F}}, zero_{\mathbb{F}}, zero_{\mathbb{F}}) = (zero_{\mathbb{F}}, zero_{\mathbb{F}}, zero_{\mathbb{F}}, one_{\mathbb{F}})$$

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

$$\begin{array}{ll} 1 = (one_{\mathbb{F}}, zero_{\mathbb{F}}, zero_{\mathbb{F}}, zero_{\mathbb{F}}) & i = (zero_{\mathbb{F}}, one_{\mathbb{F}}, zero_{\mathbb{F}}, zero_{\mathbb{F}}) \\ j = (zero_{\mathbb{F}}, zero_{\mathbb{F}}, one_{\mathbb{F}}, zero_{\mathbb{F}}) & k = (zero_{\mathbb{F}}, zero_{\mathbb{F}}, zero_{\mathbb{F}}, one_{\mathbb{F}}) \end{array}$$

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

Hamilton's quaternions are the first introduced structure of quaternions [6]. 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. Although this, 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., [15]).

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 the field. The characterization is crucial to building multiplicative inverses for non-zero quaternions 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 parameters. Finally, we formalize a completeness theorem of Hamilton's quaternions to rotate any 3D vector.

As far as we know, there are two solid formalizations of the structure of Hamilton's quaternions, one of them in HOL Light [4], and the other in Isabelle/HOL [11]). In contrast, some elements of the general theory of quaternions built over any abstract field, as in our case, were developed as part of the Lean mathlib library [9].

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

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
```

are characterized as division rings (2.3). Section 3 is divided into two subsections presenting the parameterization to obtain the theory of quaternions (3.1), and the formalization of the completeness of Hamilton's quaternions 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 formalization, available as part of the PVS nasalib theory algebra.

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: $\langle \mathbb{F}, +_{\mathbb{F}}, *_{\mathbb{F}}, zero_{\mathbb{F}}, one_{\mathbb{F}}, a, b \rangle$.

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] -> T`, with constants `zero, one, a, b: T`.

Initially, in the theory defining the structure and type `quat`, quaternion_def, it is only assumed that `[T,+,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`. Also, `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,+,zero]` is a group, and each element of the quadruple has an additive inverse. Tuple addition and scalar multiplication are defined in Specification 1. Also, notice 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 : 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_distrl`), 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.

2.2 Inference of Quaternion's Algebraic Properties

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,+,*,zero,one]` is

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_distrl       :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
```

a field (specified in theory field_def). So, the type `T` with addition and `zero`, as well as, `T-{zero}` with multiplication and `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 `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 quaternions axioms, a series of auxiliary lemmas, including the previous ones mentioned, and others about the algebra of quaternions, such as lemmas for 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, `quat[T,+,*,zero,one,a,b]`, is a ring with unity as given in the Specification 5. The proof requires expanding the definition of field for `[T, +, *, zero, one]`, then using it is a commutative division ring, that is, a commutative group with unity. From this, and the algebraic properties inferred until this point, it is possible to prove that the structure of quaternions given as `[quat[T,+,*,zero,one,a,b], +, *, zero_q, one_q]` is indeed a ring with unity. The last is done expanding the notion of ring with

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 Unity

```
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)
```

unity, and proving that `[quat[T,+,*,zero,one,a,b], +, *, zero_q]` is a ring, and that `[quat[T,+,*,zero,one,a,b], *, 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, stating that for quaternions `q, u, conjugate(q * u) = conjugate(u) * 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. This required algebraic automation through the development of specialized PVS strategies since the PVS engine for algebraic simplification is not implemented for the structure of quaternions (as happens with each other non-numerical algebraic structure). 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.

```
-(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)
```

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 `red_norm(q) = q * 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, +, *, zero]` is different from two, i.e., there exists an element $x \in T$ such that $x + x \neq$ `zero`, the center of the structure built with the quaternions and its multiplication is exactly the subtype of all the scalar quaternions. The center of such structure is given by the quaternions that multiplicatively commute with all other quaternions: $\{$ `q | ∀ 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 `Tq(q:quat)(v:(pure_quat))` is specified, and crucial properties

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)
```

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.

2.3 Charaterization 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 `red_norm(q)` $\neq$ `zero_q`, using the characterization of `red_norm` in Specification 7, one has that the scalar component of ``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 `conjugate(q) *(y * one_q)`. The exhaustive job is once again related to the algebraic manipulation to prove that `q * (conjugate(q) *(y * one_q)) = 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`, states the equivalence between being the quaternion structure a division ring with the quaternion multiplication and having a reduced norm different from `zero_q`, for any non `zero_q` quaternion, `q`. Necessity is proved by contradiction from the existence of an inverse for `q`, say `y * q = one_q`, and expansion of the definition of reduced norm, `q * conjugate(q) = zero_q`. From these equations, by algebraic manipulations one obtains `y * (q * conjugate(q)) = one_q * conjugate(q)`, and then `zero_q = conjugate(q)`, which contradicts the assumption that `q` $\neq$ `zero_q`. The proof of sufficiency uses 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 `inv(q) = conjugate(q) * inv(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 `conjugate(q) * (red_norm(q))`$^{-1}$ is the inverse of `q`. This is proved showing that `q * (conjugate(q) * (red_norm(q))`$^{-1}$`) = one_q` and `(conjugate(q) * (red_norm(q))`$^{-1}$`) * q = one_q`. The former equation requires only associativity and expansion of the definition of `red_norm` to obtain the equation `(q * conjugate(q)) * (q * conjugate(q))`$^{-1}$ `= one_q`, from which one concludes. The latter equation requires the application of the previous lemma to obtain the multiplicative inverse of `red_norm(q)`, say `y`, such that `red_norm(q) * y = one_q`. Expanding the definition of `red_norm`, one obtains the equation `(q * conjugate(q)) * y = one_q`. In this manner, one obtains the equation `q * ((conjugate(q) * y) * q) = q * 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 = zero`, the type of `a` implies `-a` $\neq$ `zero`. For the case in which `t` $\neq$ `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 `zero`, one obtains objective equality `a*(y*y) + b * zero = one`. By replacing `a` with `t*t`, one obtains `(t*t)*(y*y) = one`. The formalization, as expected, requires simple field algebraic manipulations.

The fifth lemma, `quat_div_ring_aux2`, is another auxiliary result on fields. When `= zero`, one concludes by `b` type. 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` $\neq$ `zero`, allowing the use of the latter inverse. The second premise is then instantiated with `(one + a) * y1` and `(one - a) * y1 * y` giving the objective

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

Algebraic manipulation transforms the left-hand side of this equation into the term below, where for the integer k, k `t` abbreviates `t+t+`$\cdots$`+t` k times.

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

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

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

The third and last components are also eliminated:

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

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

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

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, +, *, zero] with field multiplication is different from two and the condition $\forall \mathtt{x}, \mathtt{y} \in \mathtt{T} : \mathtt{a} * \mathtt{x}^2 + \mathtt{b} * \mathtt{y}^2 \neq \mathtt{one}$, 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 red_norm(q) $\neq$ zero_q, for any q $\neq$ zero_q under these conditions.

On the one side, if there exists x, y in the field such that $\mathtt{a} * \mathtt{x}^2 + \mathtt{b} * \mathtt{y}^2 = \mathtt{one}$, one can select the quaternion element $\mathtt{q} = \mathtt{one}_\mathtt{q} + \mathtt{x} * \mathtt{i} + \mathtt{y} * \mathtt{j}$. So, q $\neq$ zero_q, and its reduced norm, $1 - \mathtt{a} * \mathtt{x}^2 - \mathtt{b} * \mathtt{y}^2$ 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 $\forall \mathtt{x}, \mathtt{y} \in \mathtt{T} : \mathtt{a} * \mathtt{x}^2 + \mathtt{b} * \mathtt{y}^2 \neq \mathtt{one}$ holds. Then, there exists q $\neq$ zero_q such that $\mathtt{red\_norm(q)} = \mathtt{q`x}^2 - \mathtt{a} * \mathtt{q`y}^2 - \mathtt{b} * \mathtt{q`z}^2 + \mathtt{a} * \mathtt{b} * \mathtt{q`t}^2 = \mathtt{zero\_q}$. For short, let this q be equal to (x,y,z,t).

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

$$\mathtt{x}^2 - \mathtt{a} * \mathtt{y}^2 - \mathtt{b} * \mathtt{z}^2 + \mathtt{a} * \mathtt{b} * \mathtt{t}^2 = \mathtt{zero} \tag{1}$$

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

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

From the last equation, one obtains

$$\mathtt{a} * (\mathtt{x} * \mathtt{t} + \mathtt{y} * \mathtt{z})^2 + \mathtt{b} * (\mathtt{z}^2 - \mathtt{a} * \mathtt{t}^2)^2 = (\mathtt{x} * \mathtt{z} + \mathtt{a} * \mathtt{y} * \mathtt{t})^2 \tag{2}$$

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

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

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

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

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

This completes the proof.

3 Parameterization of the Algebra of Hamilton's Quaternions

By parameterizing the theory quaternions as quaternions[real,+,*,0,1,-1,-1], 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., [15]). In this

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]))
```

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 $(\mathbb{H}, +_{\mathbb{H}}, zero_q, *_{\mathbb{R}})$, where $*_{\mathbb{R}}$ indicates the scalar product induced by the multiplication over real numbers, can be proved to be 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 $\mathbb{R}^3$ 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

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)
```

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 [1], and [12]). 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 [5]. 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 [5]. 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 = rot_quat(a,b)` such that the operator `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 $\texttt{rot\_quat}\left(\texttt{a}, \frac{|\texttt{a}|}{|\texttt{b}|}\texttt{b}\right)$ by the scalar $\sqrt{\frac{|\texttt{a}|}{|\texttt{b}|}}$, where $|\texttt{v}|$ denotes the usual norm of `v` in $\mathbb{R}^3$. In the following, we will highlight the main steps to formalize those theorems.

Initially, consider two pure quaternions `a` and `b` such that `va = Vector_part(a)` and `vb = Vector_part(b)` are linearly independent; i.e., such vectors are nonparallel and non-null. Let θ be the smallest angle between `va` and `vb` and consider $\texttt{n} = \frac{\texttt{va} \times \texttt{vb}}{|\texttt{va}||\texttt{vb}|}$, where $\texttt{va} \times \texttt{vb}$ denotes the usual cross product of vectors in $\mathbb{R}^3$. The idea is to consider `n` as the rotation

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)
```

Specification 12 Basic elements to built a rotation by quaternions

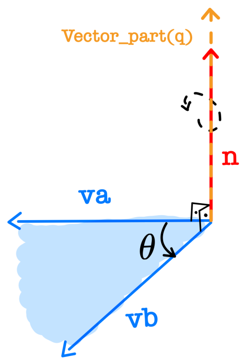
```
r_angle(a,b:(nzpure_quat)): nnreal_le_pi =
                              angle_between(Vector_part(a),Vector_part(b))

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 : nnreal_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)
```

axis and built the quaternion `q` that leads `a` into `b` from θ and `n`, as follows:

$$\mathtt{q} = \left(\cos\left(\frac{\theta}{2}\right), \mathtt{n'x} * \sin\left(\frac{\theta}{2}\right), \mathtt{n'y} * \sin\left(\frac{\theta}{2}\right), \mathtt{n'z} * \sin\left(\frac{\theta}{2}\right)\right)$$



The elements θ, `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(Vector_part(a),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)`.

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:

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

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 `Vector_part(q) * va = 0`. Consequently, the equation `(2 * (Vector_part(q) * va)) * 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 $(\texttt{va} \times \texttt{vb})$ and `va` are orthogonal. This is a consequence of the equalities $\texttt{Vector\_part(q)} = \texttt{sin}\left(\frac{\theta}{2}\right) * \texttt{n} = \frac{\texttt{sin}\left(\frac{\theta}{2}\right)}{|\texttt{va}||\texttt{vb}|} * (\texttt{va} \times \texttt{vb})$.

The lemma `Quat_Rot_Aux2` establishes the equality

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

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

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

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 $\texttt{cos}^2\left(\frac{\theta}{2}\right) - \texttt{sin}^2\left(\frac{\theta}{2}\right) = \texttt{cos}(\theta)$.

Finally, in the lemma `Quat_Rot_Aux3`, it is formalized that

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

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

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

Applying the lemmas `cross_cross` and `sin_2a`, specified in theories `vectors@cross_3D` and trig@trig_basic, respectively, one obtains the equality

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

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

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

Thus, by using the fact the `|va| = |vb|` and applying the identity $|\mathtt{va} \times \mathtt{vb}| = |\mathtt{va}||\mathtt{vb}|\sin(\theta)$, formalized in the lemma `norm_cross_charac_` of the theory `vectors`, one obtains the equality

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

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 $\mathtt{q} = \sqrt{\frac{|\mathtt{b}|}{|\mathtt{a}|}} * \mathtt{rot\_quat}\left(\mathtt{a}, \frac{|\mathtt{a}|}{|\mathtt{b}|}\mathtt{b}\right)$. In fact, using this `q` as argument of the transformation,

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

Then, applying the lemma `conj_product_quat_scalar`, behind some algebraic manipulations, it holds that

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

Finally, since $|\mathtt{Vector\_part(a)}| = \left|\mathtt{Vector\_part}\left(\frac{|\mathtt{a}|}{|\mathtt{b}|}\mathtt{b}\right)\right|$, the proof of the Theorem `Quaternions_Rotation_Deform` is completed instantiating `Quaternions_Rotation` with the pure quaternions `a` and $\frac{|\mathtt{a}|}{|\mathtt{b}|}\mathtt{b}$, which guarantees that

$$\mathtt{T\_q}\left(\mathtt{rot\_quat}\left(\mathtt{a}, \frac{|\mathtt{a}|}{|\mathtt{b}|}\mathtt{b}\right)\right)(\mathtt{a}) = \frac{|\mathtt{a}|}{|\mathtt{b}|}\mathtt{b},$$

and, consequently, that $\mathtt{T\_q(q)(a)} = \mathtt{b}$.

It is important to remark that only the crucial lemmas in 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 Parameterizations to Specify other Quaternion's Structures

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 quaternions 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 $M_2(\mathbb{F})$ [2]. An example is given by the quaternion built over the complex field: $\left(\dfrac{a,b}{\mathbb{C}}\right) \xrightarrow{\sim} M_2(\mathbb{C})$, in which not only, it splits for some values $a, b \in \mathbb{C} \setminus \{0\} = \mathbb{C}^{\times}$. On the other hand, all $\left(\dfrac{a,b}{\mathbb{F}}\right)$ 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 $\left(\dfrac{a,p}{\mathbb{Q}}\right)$, where p is an odd prime and a is a quadratic non-residue, or $\left(\dfrac{a,p}{\mathbb{Q}_p}\right)$, where $\mathbb{Q}_p$ are the p-adic numbers and a, p having the same restrictions [15].

The formalization of the general theory of quaternions constitutes a starting point to deal with other interesting applications of the theory of quaternions. Surveying only a few of the applications covered in Voight's book [15], 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 [8].

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 [15], 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 as a tool for proven theorems. This is a subring of the quaternions $\mathbb{H}$ and $\left(\dfrac{-1,-1}{\mathbb{Q}}\right)$, given by $H = \{\alpha\zeta + \beta i + \gamma j + \delta k \mid \alpha, \beta, \gamma, \delta \in \mathbb{Z}\}$, where $\zeta = \dfrac{1}{2}(1 + i + j + k)$. 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 an Euclidean ring.

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 `Red_norm(uv) = Red_norm(u) * 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:

$$c_0 = a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3 \qquad c_1 = a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2$$
$$c_2 = a_0 b_2 - a_1 b_3 + a_2 b_0 + a_3 b_1 \qquad c_3 = a_0 b_3 + a_1 b_2 - a_2 b_1 + a_3 b_0$$

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 [7].

Among the interesting applications in physics, it is possible to express using quaternion algebra, the gravity as part of a simple quaternion wave equation [14], the four Maxwell equations as a nonhomogeneous quaternion wave equation, as well as the Klein-Gordon equation as a quaternion simple harmonic oscillator [13]. Furthermore, under some restrictions, it is possible to express a quaternion analog to the Schrödinger equation, a 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 a vector of $\mathbb{R}^3$, denoted by $(\mathtt{s}, \tilde{\mathtt{V}})$, and write the quaternion in its polar form, namely:

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

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

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

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

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

$$\psi = \mathtt{e}^{(\mathtt{E}*\mathtt{t} - \tilde{\mathtt{R}}*\tilde{\mathtt{P}})*\mathtt{I}/\hbar},$$

where $\mathtt{I} = \frac{\mathtt{E} * \tilde{\mathtt{R}} + \tilde{\mathtt{P}} * \mathtt{t} + \tilde{\mathtt{R}} \times \tilde{\mathtt{P}}}{\|\mathtt{E} * \tilde{\mathtt{R}} + \tilde{\mathtt{P}} * \mathtt{t} + \tilde{\mathtt{R}} \times \tilde{\mathtt{P}}\|}$.

Now, differentiating ψ with respect to the time and the space we obtain, respectively:

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

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 ψ. Among these assumptions are, for example, the conservation of energy and momentum and the assumption that $\mathtt{E} * \mathtt{t} - \tilde{\mathtt{R}} * \tilde{\mathtt{P}} = \mathtt{0}$. Therefore,

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

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

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

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

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

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

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

Table 1 Quantitative information

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

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 [10] and di Vito in [3], among others. The availability of techniques to detect and cancel equal terms over algebraic theories as `field` and `quat` will surely make possible decreasing 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 theorem will require the adequate parameterization of the quaternion theory proving that Hurwitz substructure is indeed a ring and that is almost a Euclidian 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, mechanism of arithmetic manipulation for standard types as `int`, `nat`, and `reals` to abstract algebraic structures as `ring`, `field`, and `quat`.

References

1 Howard Anton and Chris Rorres. *Elementary Linear Algebra: Applications Version*. John Wiley & Sons. Inc., 10th edition, 2010.

2 Keith Conrad. Quaternion algebras. Accessed in March 13, 2024. URL: https://kconrad.math.uconn.edu/blurbs/ringtheory/quaternionalg.pdf.

3 Ben L. Di Vito. *Manip User's Guide, Version 1.3*, 2012.

4 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.

5 Gökmen Günaştı. Quaternions algebra, their applications in rotations and beyond quaternions. Technical report, Linnaeus University, Digitala Vetenskapliga Arkivet, 2012.

6 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.

7 Israel (Yitzchak) Nathan Herstein. *Topics in Algebra*. John Wiley and Sons, New York, Chichester, Brisbane, Toronto, Singapore, second edition, 1975.

8 David W. Lewis. Quaternion Algebras and the Algebraic Legacy of Hamilton's Quaternions. *Irish Math. Soc. Bulletin*, 57:41–64, 2006.

9 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.

10 César Muñoz and Micaela Mayero. Real Automation in the Field. Technical Report Interim report, No 39, NASA/ICASE, 2001.

11 Lawrence C. Paulson. Quaternions. *Arch. Formal Proofs*, 2018, 2018. URL: https://www.isa-afp.org/entries/Quaternions.html.

12 Logah Perumal. Euler angles: conversion of arbitrary rotation sequences to specific rotation sequence. *Comput. Animat. Virtual Worlds*, 25(5-6):521–529, 2014. URL: https://doi.org/10.1002/cav.1529, doi:10.1002/CAV.1529.

13 Douglas Sweetser. Doing Physics with Quaternions, 2005. Accessed in March 13, 2024. URL: https://theworld.com/~sweetser/quaternions/ps/book.pdf.

14 Douglas Sweetser. Three Roads to Quaternion Gravity. In *APS March Meeting Abstracts*, volume 2019 of *APS Meeting Abstracts*, page T70.008, January 2019.

15 John Voight. *Quaternion Algebras*, volume GTM 288 of *Graduate Texts in Mathematics*. Springer Cham, 2021. doi:https://doi.org/10.1007/978-3-030-56694-4.