Formalizing basic quaternionic analysis

Andrea Gabrielli[1] and Marco Maggesi[2] *

[1] University of Florence, Italy
andrea.gabrielli@unifi.it
[2] University of Florence, Italy
marco.maggesi@unifi.it
http://www.math.unifi.it/~maggesi/

Abstract We present a computer formalization of quaternions in the HOL Light theorem prover. We give an introduction to our library for potential users and we discuss some implementation choices.
As an application, we formalize some basic parts of two recently developed mathematical theories, namely, slice regular functions and Pythagorean-Hodograph curves.

1 Introduction

Quaternions are a well-known and elegant mathematical structure which lies at the intersection of algebra, analysis and geometry. They have a wide range of theoretical and practical applications from mathematics and physics to CAD, computer animations, robotics, signal processing and avionics.

Arguably, a computer formalization of quaternions can be useful, or even essential, for further developments in pure mathematics or for a wide class of applications in formal methods.

In this paper, we present a formalization of quaternions in the HOL Light theorem prover. Our aim is to give a quick introduction of our library to potential users and to discuss some implementation choices.

Our code is available from a public Git repository[3] and a significant part of it has been included in the HOL Light library.

The paper is divided into two main parts. The first one (Section 3), we describe the core of our library, which is already available in the HOL Light distribution.

Next, in the second part, we outline two applications to recently developed mathematical theories which should serve as further examples and as a testbed for our work. More precisely, we give the definition and some basic theorems about slice regular quaternionic functions (Section 4) and Pythagorean-Hodograph curves (Section 5).

We thank Graziano Gentili, Carlotta Giannelli and Caterina Stoppato for many enlightening discussions.

---

* This work has been supported by GNSAGA-INdAM and MIUR.

[3] Reachable from the url https://bitbucket.org/maggesi/quaternions/ .

2 Related work

The HOL Light theorem prover furnishes an extensive library about multivariate analysis [7] and complex analysis [8], which has been constantly and steadily extended over the years by Harrison, the main author of the system.

Our objective is to try to further improve this work by adding contributions in (hyper)complex analysis. One previous work along this line was the proof of the Cartan fixed point theorems [1] by Ciolli, Gentili and the second author of this paper.

In a broader context, quaternions are one of the simplest examples of geometric algebra (technically, real Clifford algebra). In this respect, we mention two recent related efforts. Fuchs and Théry [4] devised an elegant inductive data structure for formalizing geometric algebra. More recently, Ma et al. [9], provided a formalization in HOL Light of Conformal Geometric Algebra. In principle, these contributions can be integrated with our work, but at the present stage, we have focused entirely on the specific case of quaternions.

3 The core library

Quaternions were "invented" by Hamilton in 1843. From their very inception, they was meant to represent, in an unified form, both scalar and vector quantities. Informally, a quaternion q is expressed as a formal combination

$$q = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{H} \qquad a, b, c, d \in \mathbb{R},$$

where $\mathbf{i}, \mathbf{j}, \mathbf{k}$ are *imaginary units*. The following identities

$$\begin{aligned} \mathbf{ij} &= \mathbf{k} = -\mathbf{ji} \\ \mathbf{jk} &= \mathbf{i} = -\mathbf{kj} \\ \mathbf{ki} &= \mathbf{j} = -\mathbf{ik} \\ \mathbf{i}^2 &= \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1 \end{aligned}$$

together with the distributive law, induce a product that turns the set $\mathbb{H}$ of quaternions into a skew field.

It is useful to consider a number of different possible decompositions for a quaternion q, as briefly sketched in the following schema (here $\mathbb{I} = \mathbb{R}^3$ can be interpreted, depending on the context, as the imaginary part of $\mathbb{H}$ or the 3-dimensional space):

$$\begin{aligned} q &= \underbrace{a}_{\operatorname{Re} q} + \underbrace{b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}}_{\operatorname{Im} q} && \in \mathbb{H} = \mathbb{R} \oplus \mathbb{I} \\ &= \underbrace{a}_{\text{scalar}} + \underbrace{b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}}_{\text{3d-vector}} && \in \mathbb{R}^4 = \mathbb{R} \oplus \mathbb{R}^3 \\ &= \underbrace{a + b\,\mathbf{i}}_{z \in \mathbb{C}} + \underbrace{(c + d\,\mathbf{i})}_{w \in \mathbb{C}}\,\mathbf{j} && \in \mathbb{H} \simeq \mathbb{C} \oplus \mathbb{C} \end{aligned}$$

3.1 The definition of quaternion

For the sake of consistency, whenever possible, our development mimics the formalization of complex numbers, due to Harrison, that is present in the HOL Light standard library [8]. Following this path, we define the data type `‘:quat‘` of quaternions as an alias for the type of 4-dimensional vectors `‘:real^4‘`. This approach has the fundamental advantage that we inherit immediately from the general theory of Euclidean spaces the appropriate metric, topology and real-vector space structure.

A set of auxiliary constants for constructing and destructing quaternions is defined to setup a suitable *abstraction barrier*. They are listed in the following table.

Table 1. Basic notations for the `‘:quat‘` datatype

Constant name	Type	Description
`Hx`	`:real->quat`	Embedding $\mathbb{R} \to \mathbb{H}$
`ii`, `jj`, `kk`	`:quat`	Imaginary units $\mathbf{i}, \mathbf{j}, \mathbf{k}$
`quat`	`:real#real#real#real->quat`	Generic constructor
`Hv`	`:real^3->quat`	Embedding $\mathbb{R}^3 \to \mathbb{H}$
`Re`	`:quat->real`	Real component
`Im1`, `Im2`, `Im3`	`:quat->real`	Imaginary components
`HIm`	`:quat->real^3`	Imaginary part
`cnj`	`:quat->quat`	Conjugation

This is summarized in the following theorem

```
QUAT_EXPAND
|- !q. q = Hx(Re q) + ii*Hx(Im1 q) + jj*Hx(Im2 q) + kk*Hx(Im3 q)
```

With these notations in place, the multiplicative structure can be expressed with an explicit formula

```
let quat_mul = new_definition
  ‘p * q =
   quat
   (Re p *  Re q - Im1 p * Im1 q - Im2 p * Im2 q - Im3 p * Im3 q,
    Re p * Im1 q + Im1 p *  Re q + Im2 p * Im3 q - Im3 p * Im2 q,
    Re p * Im2 q - Im1 p * Im3 q + Im2 p *  Re q + Im3 p * Im1 q,
    Re p * Im3 q + Im1 p * Im2 q - Im2 p * Im1 q + Im3 p *  Re q)‘;;
```

and the inverse of a quaternion is defined analogously. Moreover, we also provide auxiliary theorems that express in the same notation the already defined additive and metric structures, e.g.,

```
quat_add
|- p + q =
   quat(Re p + Re q,Im1 p + Im1 q,Im2 p + Im2 q,Im3 p + Im3 q)
```

```
quat_norm
|- norm q =
   sqrt(Re q pow 2 + Im1 q pow 2 + Im2 q pow 2 + Im3 q pow 2)
```

Notice that several notations (Re, ii, cnj, ...) overlap in the complex and quaternionic case and, more generally, with the ones of other number systems (+, *, ...). HOL Light features an overloading mechanism that uses type inference to select the right constant associated to a given notation.

3.2 Computing with quaternions

After settling the basic definitions, we supply a simple automated procedure for proving quaternionic algebraic identities. It consists of just two steps: (1) rewriting the given identity in real components, (2) using an automated procedure for the real field (essentially one involving polynomial normalization, elimination of fractions and Gröbner Basis):

```
let SIMPLE_QUAT_ARITH_TAC =
  REWRITE_TAC[QUAT_EQ; QUAT_COMPONENTS; HX_DEF;
              quat_add; quat_neg; quat_sub; quat_mul;
              quat_inv] THEN
  CONV_TAC REAL_FIELD;;
```

This approach, although very crude, allows us to prove directly nearly 60 basic identities, e.g.,

```
let QUAT_MUL_ASSOC = prove
 (`!x y z:quat. x * (y * z) = (x * y) * z`,
  SIMPLE_QUAT_ARITH_TAC);;
```

and it is also occasionally useful to prove ad hoc identities in the middle of more complex proofs. In this way, we quickly bootstrap a small library with the essential algebraic results that are needed for building more complex procedures and theorems.

Next, we provide a conversion RATIONAL_QUAT_CONV for evaluating literal algebraic expressions. This is easily assembled from elementary conversions for each basic algebraic operation (RATIONAL_ADD_CONV, RATIONAL_MUL_CONV, ...) using the HOL mechanism of higher-order conversionals. For instance, the computation

$$\left(1+2\mathbf{i}-\frac{1}{2}\mathbf{k}\right)^3 = -\frac{47}{4}-\frac{5}{2}\mathbf{i}+\frac{5}{8}\mathbf{k}$$

is performed with the command

```
# RATIONAL_QUAT_CONV
  `(Hx(&1) + Hx(&2) * ii - Hx(&1 / &2) * kk) pow 3`;;
val it : thm =
  |- (Hx(&1) + Hx(&2) * ii - Hx(&1 / &2) * kk) pow 3 =
     -- Hx(&47 / &4) - Hx(&5 / &2) * ii + Hx(&5 / &8) * kk
```

Finally, we implement a procedure for simplifying quaternionic polynomial expressions. HOL Light provides a general procedure for polynomial normalization, which unfortunately works only for commutative rings. Hence we are forced to code our own solution. In principle, our procedure can be generalized to work with arbitrary (non-commutative) rings. However, at the present stage, it is hardwired to the specific case of quaternions. To give an example, the computation

$$(p+q)^3 = p^3 + q^3 + pq^2 + p^2q + pqp + qp^2 + qpq + q^2p$$

can be done with the command

```
# QUAT_POLY_CONV `(x + y) pow 3`;;
val it : thm =
  |- (p + q) pow 3 =
     p pow 3 + q pow 3 + p * q pow 2 + p pow 2 * q +
     p * q * p + q * p pow 2 + q * p * q + q pow 2 * p
```

3.3 The geometry of quaternions

One simple fact, which makes quaternions useful in several physical and geometrical applications, is that the quaternionic product encodes both the scalar and the vector product. More precisely, if p and q are purely imaginary quaternions then we have

$$pq = -\underbrace{\langle p, q\rangle}_{\substack{\text{scalar}\\\text{product}}} + \underbrace{p \wedge q}_{\substack{\text{vector}\\\text{product}}} \in \mathbb{R} \oplus \mathbb{I},$$

which can be easily verified by direct computation.

Moreover, it is possible to use quaternions to encode orthogonal transformations. We briefly recall the essential mathematical construction. For $q \neq 0$, the conjugation map is defined as

$$c_q : \mathbb{H} \longrightarrow \mathbb{H}$$
$$c_q(x) := q^{-1}\, x\, q$$

and we have

$$c_{q_1} \circ c_{q_2} = c_{q_1 q_2}, \qquad c_q^{-1} = c_{q^{-1}}.$$

One important special case is when q is unitary, i.e., $\|q\| = 1$ for which we have $q^{-1} = \bar{q}$ (the conjugate) and thus $c_q(x) = \bar{q}\, x\, q$.

Now, we are ready to state some basic results, which we have formalized in our framework (see file `Quaternions/qisom.hl` in the HOL Light distribution).

Proposition 1. *If v is a non-zero purely imaginary quaternion, then $-c_v : \mathbb{R}^3 \to \mathbb{R}^3$ is the reflection with respect to the subspace of $\mathbb{R}^3$ orthogonal to v.*

Here is the corresponding statement proved in HOL Light

```
REFLECT_ALONG_EQ_QUAT_CONJUGATION
|- !v. ~(v = vec 0)
       ==> reflect_along v = \x. --HIm (inv (Hv v) * Hv x * Hv v)
```

The theorem of Cartan-Dieudonné asserts that any orthogonal transformation $f\colon \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is the composition of at most n reflections. Using this and the previous proposition we get the following result.

Proposition 2. *Any orthogonal transformation $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ is of the form*

$$f = c_q \quad \textit{or} \quad f = -c_q, \qquad \|q\| = 1.$$

The corresponding formalization is the following

```
ORTHOGONAL_TRANSFORMATION_AS_QUAT_CONJUGATION
|- !f. orthogonal_transformation f
         ==> (?q. norm q = &1 /\
                  ((!x. f x = HIm (inv q * Hv x * q)) \/
                   (!x. f x = --HIm (inv q * Hv x * q))))
```

3.4 Elementary quaternionic analysis

Passing from algebra to analysis, we need to prove a series of technical results about the analytical behaviour of the algebraic operations. Following the HOL Light practice, we use the formalism of net topology to express limits and continuity. To give an idea, here we report the theorem that states the uniform continuity of the quaternionic inverse $q \mapsto q^{-1}$

```
UNIFORM_LIM_QUAT_INV
|- !net P f l b.
     (!e. &0 < e
          ==> eventually (\x. !n. P n ==> norm (f n x - l n) < e)
                         net) /\
     &0 < b /\ eventually (\x. !n. P n ==> b <= norm (l n)) net
     ==> (!e. &0 < e
              ==> eventually
                  (\x. !n. P n
                           ==> norm (inv (f n x) - inv (l n)) < e)
                  net)
```

We conducted a systematic formalization of the behaviour of algebraic operations from the point of view of limits and continuity, which brought us to prove more than fifty such theorems overall. Some of them are indeed trivial. For instance, the uniform continuity of the product is a direct consequence of a more general result already available on bilinear maps. Some are less immediate and forced us to dive into a technical $\epsilon\delta$-reasoning.

Next, we considered the differential structure. Given a function $f : \mathbb{R}^n \to \mathbb{R}^m$ we denote by $\mathrm{D}f_{x_0}(v)$ or $\frac{\mathrm{d}}{\mathrm{d}x} f(x)|_{x_0}(v)$ the (Frechét) *derivative* of f at x_0 applied to the vector v. When the derivative exists, it is the linear function from $\mathbb{R}^n$ to $\mathbb{R}^m$ that "best" approximates the variation of f in a neighborhood of x_0, i.e.,

$$f(x) - f(x_0) \approx \mathrm{D}f_{x_0}(x - x_0).$$

In HOL Light, the ternary predicate `(f has_derivative f') (at x0)` is used to assert that f is (Frechét) differentiable at x_0 and $f' = \mathrm{D}f_{x_0}$

We compute the derivative of the basic quaternionic operations. Notice that, if f is a quaternionic valued function, the derivative $\mathrm{D}f_{q_0}(x)$ is a quaternion (in the modern language of Differential Geometry this is the natural identification of the tangent space $T_{f(q_0)}\mathbb{H} \simeq \mathbb{H}$). For instance, given two differentiable functions $f(q)$ and $g(q)$, the derivative of their product at q_0 is

$$\frac{\mathrm{d}\big(f(q)g(q)\big)}{\mathrm{d}q}|_{q_0}(x) = f(q_0)\,\mathrm{D}g_{q_0}(x) + \mathrm{D}f_{q_0}(x)g(q_0).$$

In our formalism, the previous formula becomes the following theorem:

```
QUAT_HAS_DERIVATIVE_MUL_AT
|- !f f' g g' q.
     (f has_derivative f') (at q) /\ (g has_derivative g') (at q)
     ==> ((\x. f x * g x) has_derivative
          (\x. f q * g' x + f' x * g q)) (at q)
```

Another consequence that will be useful later, is the following formula for the power:

$$\frac{\mathrm{d}q^n}{\mathrm{d}q}|_{q_0}(x) = \sum_{i=1}^{n} q_0^{n-i} x q_0^{i-1},$$

that is, the HOL theorem

```
QUAT_HAS_DERIVATIVE_POW
|- !q0 n.
     ((\q. q pow n) has_derivative
      (\h. vsum (1..n) (\i. q0 pow (n - i) * h * q0 pow (i - 1))))
     (at q0)
```

which is easily proven by induction using the derivative of the product.

4 Slice regular functions

Complex holomorphic functions play a central role in mathematics. Given the deep link and the evident analogy between complex numbers and quaternions, it is natural to seek for a theory of *quaternionic holomorphic functions*. A more careful investigation shows that the situation is less simple than expected. Naive attempts to generalize the complex theory to the quaternionic case fail because they lead to conditions which are either too strong or too weak and do not produce *interesting* classes of functions.

Fueter in the 1920s, proposed a definition of *regular* quaternionic function which is now well-known to the experts and has been extensively studied and developed. Fueter's regular functions have significant applications to physics and engineering, but present also some undesirable aspects. For instance, the identity function and the polynomials $P(q) = a_0 + a_1 q + \ldots + a_n q^n$, $a_i \in \mathbb{H}$ are not Fueter-regular. A more detailed discussion on this subject is far beyond the goal of the present work. To the interested reader we recommend Sudbery's excellent survey [11].

In this setting, a novel promising approach has been recently proposed by Gentili and Struppa in their seminal paper in 2006 [6], where they introduce the definition of *slice regular* functions and prove that they expand into power series near the origin. Slice regular functions are now a stimulating and active subject of research for several mathematicians worldwide. A comprehensive introduction on the foundation of this new theory can be found in the book of Gentili, Stoppato and Struppa [5].

In this section, we use our quaternionic framework presented in the previous section to formalize the basics of the theory of slice regular functions.

4.1 The definition of slice regular function

A real 2-dimensional subspace $L \subset \mathbb{H}$ containing the real line is called a *slice* (or *Cullen slice*) of $\mathbb{H}$. The key fact is that the quaternionic product becomes commutative when it is restricted on a slice, that is if p, q are in the same slice L, then $pq = qp$. In other terms, each slice L can be seen as a copy of the complex field $\mathbb{C}$. More precisely, if I is a quaternionic imaginary unit (i.e., an unitary imaginary quaternion), then $L_I = \text{Span}\{1, I\} = \mathbb{R} \oplus \mathbb{R}I$ is a slice and the injection $j_I \colon \mathbb{C} \to L_I \subset \mathbb{H}$, defined by

$$j_I \colon x + y\mathbf{i} \mapsto x + yI,$$

is a field homomorphism. Its formal counterpart is

```
let cullen_inc = new_definition
  `cullen_inc i z = Hx(Re z) + Hx(Im z) * i`;;
```

We can now introduce the definition of Gentili and Struppa:

Definition 1 (Slice regular function). *Given a domain (i.e., an open, connected set) $\Omega \subset \mathbb{H}$ a function $f \colon \Omega \to \mathbb{H}$ is* slice regular *if it is holomorphic (in the complex sense) on each slice, that is, the restricted function $f_{L_I} \colon \Omega \cap L_I \to \mathbb{H}$ satisfies the condition*

$$\frac{1}{2}\left(\frac{\partial}{\partial x} + I\frac{\partial}{\partial y}\right) f_{L_I}(x + yI) = 0$$

for each $q = x + yI$ in $\Omega \cap L_I$, for every imaginary unit I. In that case, we define the slice derivative *of f in q to be the quaternion*

$$f'(q) = \frac{1}{2}\left(\frac{\partial}{\partial x} - I\frac{\partial}{\partial y}\right) f_{L_I}(x + yI).$$

Our first task is to code the previous definition within our formalism. One problem is the notation for partial derivatives, which is notorious for being occasionally opaque and potentially misleading. When it has to be rendered in a formal language, its translation might be tricky or at least cumbersome. This is essentially due to the fact that it is a convention that induces us to use the same name for different functions, depending on the name of the arguments.[4]

We decided that the best way to avoid potential problems in our development was to systematically replace partial derivatives with (Frechét) derivatives. This leads to an alternative, and equivalent, definition of slice regular function which could be interesting in its own.

The basic idea is the following. A complex function f is holomorphic in z_0 precisely when its derivative $\mathrm{D}f_{z_0}$ is $\mathbb{C}$-linear. Hence, by analogy, a quaternionic function should be slice regular if its derivative is $\mathbb{H}$-linear on slices in a suitable sense. This is indeed the case: consider $f : \Omega \to \mathbb{H}$ as before and a quaternion $q_0 \in \Omega$. Let L be a slice containing q_0 and denote by f_L the restriction of f to $\Omega \cap L$. Then we have

Proposition 3. *The function f is slice regular in q_0 if and only if the derivative of f_L is right-$\mathbb{H}$-linear, that is, there exists a quaternion c such that*

$$\mathrm{D}(f_L)_{q_0}(p) = pc.$$

In that case, c is the slice derivative $f'(q_0)$.

We then take the alternative formulation given by the above Proposition as the definition of slice regular function in our developement. The resulting formalization in HOL is the following

```
let has_slice_derivative = new_definition
  `!f (f':quat) net.
     (f has_slice_derivative f') net <=>
     (!l. subspace l /\ dim l = 2 /\ Hx(&1) IN l /\
          netlimit net IN l
          ==> (f has_derivative (\q. q * f')) (net within l))`;;
```

Notice that the predicate `has_slice_derivative` formalizes at the same time the notion of slice regular function and the notion of slice derivative. The domain Ω does not appear in the definition because functions in HOL are total and, in any case, the notion of slice derivative is local.

Our formalization of slice derivative is slightly more general than the one of Proposition 3 for the fact that we use HOL nets. The reader who is not

[4] Spivak, in his book *Calculus on manifolds* [10, p. 65], notices that if $f(u, v)$ is a function and $u = g(x, y)$ and $v = h(x, y)$, then the chain rule is often written

$$\frac{\partial f}{\partial x} = \frac{\partial f}{\partial u}\frac{\partial u}{\partial x} + \frac{\partial f}{\partial v}\frac{\partial v}{\partial x},$$

where f denotes two different functions on the left- and right-hand of the equation.

accustomed to the use of nets can simply think the variable `net` as a denoting the limit $q \to q_0$ and `netlimit net` as the limit point q_0. Other than that, these details about nets are largely irrelevant in the rest of the paper.

We formally proved Proposition 3 in HOL Light. Here is the statement for the case when $q_0 = x + yI$ is not real.

```
HAS_SLICE_DERIVATIVE
|- !f f' i x y.
     i pow 2 = -- Hx(&1) /\ ~(y = &0) /\
     f differentiable at (Hx x + Hx y * i)
     ==> ((f has_slice_derivative f') (at (Hx x + Hx y * i)) <=>
          (?fx fy.
            ((\a. f(Hx(drop a) + Hx y*i)) has_vector_derivative fx)
              (at(lift x)) /\
            ((\b. f(Hx x + Hx(drop b)*i)) has_vector_derivative fy)
              (at(lift y)) /\
            fx + i * fy = Hx(&0) /\ f' = fx /\ f' = --(i * fy)))
```

Since any slice L can be obtained as the image of j_I for any imaginary unit $I \in L$, then we also have the following useful reformulation

```
HAS_SLICE_DERIVATIVE_CULLEN_INC
|- !i f f' z0.
     i pow 2 = --Hx(&1)
     ==> ((f has_slice_derivative f')
          (at (cullen_inc i z) within cullen_slice i) <=>
          (f o cullen_inc i has_derivative
           (\z. cullen_inc i z * f')) (at z0))
```

After the definition, we provided a series of lemmas that allow us to compute the slice derivative of algebraic expressions. In particular, the powers q^n are slice regular and, if $f(q)$ and $g(q)$ are slice regular functions and c is a quaternion, then $f(q) + g(q)$ and $f(q)c$ are slice regular. It follows that *right* polynomials (i.e., polynomials with coefficients on the right)

$$c_0 + qc_1 + q^2c_2 + \cdots + q^nc_n$$

are all slice regular functions. Most of these results are easy consequences of those discussed in Section 3.4.

We should stress that the product $f(q)g(q)$, including left multiplication $cf(q)$ and arbitrary polynomials of the form

$$c_0 + c_{1,1}q + c_{2,0}qc_{2,1}qc_{2,2} + c_{3,0}qc_{3,1}qc_{3,2}qc_{3,3} + \cdots,$$

is not slice regular in general.

A more explicit link between slice regular functions and complex holomorphic functions is given by the *splitting lemma*, which is a fundamental tool for several subsequent results. Given two imaginary units I, J orthogonal to one other, every quaternion can be *split*, in an unique way, into a sum $q = z + wJ$ with $z, w \in L_I$. Now, given a function $f\colon \Omega \to \mathbb{H}$ we can split its restriction f_{L_I} as

$$f_{L_I}(z) = F(z) + G(z)J$$

with $F, G\colon \Omega \cap L_I \to L_I$. Then we have

Lemma 1 (Splitting Lemma). *The function f is slice regular at $q_0 \in L_I$ if and only if the functions F and G are holomorphic at q_0.*

Notice that, in the above statement, the two functions F, G are 'complex holomorphic' with respect to the implicit identification $\mathbb{C} \simeq L_I$ given by $j_I\colon x + y\mathbf{i} \mapsto x + yI$. This has been made explicit in the following formal statement using our injection `cullen_inc`:

```
QUAT_SPLITTING_LEMMA
|- !f s i j.
     open s /\ i pow 2 = --Hx (&1) /\ j pow 2 = --Hx (&1) /\
     orthogonal i j
     ==> (?g h.
            (!z. f (cullen_inc i z) =
                 cullen_inc i (g z) + cullen_inc i (h z) * j) /\
            (!g' h' z.
               z IN s
               ==> ((g has_complex_derivative g') (at z) /\
                    (h has_complex_derivative h') (at z) <=>
                    (f o cullen_inc i has_derivative
                     (\z. cullen_inc i z *
                          (cullen_inc i g' + cullen_inc i h' * j)))
                    (at z))) /\
            (g holomorphic_on s /\ h holomorphic_on s <=>
             (f slice_regular_on s) i))
```

4.2 Power expansions of slice regular functions

We now approach power series expansions of slice regular functions at the origin, which is one of the corner stone for the development of the whole theory. While the HOL Light library has a rather complete support for sequences and series in general, at the beginning of our work it was still lacking the proof of various theorems that were important prerequisites for our task.

We undertake a systematic formalization of the missing theory, including

1. the definition of limit superior and inferior and their basic properties;
2. the root test for series;
3. the Cauchy-Hadamard formula for the radius of convergence.

We avoid discussing this part of the work in detail in this paper. All these preliminaries have been recently included in the HOL Light standard library.[5]

[5] Commit on Apr 10, 2017, HOL Light GitHub repository.

Theorem 1 (Abel's Theorem for slice regular functions). *The quaternionic power series*

$$\sum_{n\in\mathbb{N}} q^n a_n \tag{1}$$

is absolutely convergent in the ball $B = B\big(0, 1/\limsup_{n\to+\infty} \sqrt[n]{|a_n|}\big)$ *and uniformly convergent on any compact subset of* B*. Moreover, its sum defines a slice regular function on* B*.*

The corresponding formalization is split into several theorems. As for the convergence, we have three statements, one for each kind of convergence (pointwise, absolute, uniform). As an example, we include the statement for the uniform convergence:

```
QUAT_UNIFORM_CONV_POWER_SERIES
|- !a b s k.
     ((\n. root n (norm (a n))) has_limsup b)
      (sequentially within k) /\
     compact s /\
     (!q. q IN s ==> b * norm q < &1)
     ==> ((\i q. q pow i * a i) uniformly_summable_on s) k
```

The predicate `uniformly_summable_on` is a compact notation for uniform convergence for series. Note that the hypothesis `b * norm q < &1` allows a correct representation of the domain of convergence also in the case of infinite radius (case $b = 0$).

With a little extra effort we proved the same results for the formal derivative of the series (1).

Finally, from the previous results, and the fact that derivative distributes over uniformly convergent series, we proved that right quaternionic power series are slice regular functions on any compact subsets of their domain of convergence

```
QUAT_HAS_SLICE_DERIVATIVE_POWER_SERIES_COMPACT
|- !a b k q0 s.
     ((\n. root n (norm (a n))) has_limsup b)
      (sequentially within k) /\
     compact s /\ s SUBSET {q | b * norm q < &1} /\
     ~(s = {}) /\ q0 IN s
     ==> ((\q. infsum k (\n. q pow n * a n)) has_slice_derivative
          infsum k (\n. q0 pow (n - 1) * Hx (&n) * a n)) (at q0)
```

which completes the formalization of Theorem 1.

Next, from the Splitting Lemma 1, we can derive the existence of the power series expansion of a slice regular function f from the analyticity of its holomorphic components F and G.

Theorem 2. *Let $f : B(0, R) \to \mathbb{H}$ be a slice regular function. Then*

$$f(q) = \sum_{n\in\mathbb{N}} q^n \frac{1}{n!} f^{(n)}(0),$$

where $f^{(n)}$ is the n-th slice derivative of f.

The resulting formalization is the following

```
SLICE_REGULAR_SERIES_EXPANSION
|- !r q f.
     &0 < r /\ q IN ball (Hx(&0),r) /\
     (!i. (f slice_regular_on ball (Cx(&0),r)) i)
     ==> (?z i.
            i pow 2 = --Hx(&1) /\ q = cullen_inc i z /\
            f q =
            infsum (:num)
            (\n. cullen_inc i z pow n *
                 cullen_inc i (inv (Cx(&(FACT n)))) *
                 higher_slice_derivative i n f (Hx(&0))))
```

5 Pythagorean-Hodograph curves

The *hodograph* of a parametric curve $\mathbf{r}(t)$ in $\mathbb{R}^n$ is just its derivative $\mathbf{r}'(t)$, regarded as a parametric curve in its own right. A parametric polynomial curve $\mathbf{r}(t)$ is said to be a *Pythagorean-Hodograph* curve if it satisfies the *Pythagorean condition*, i.e., there exists a polynomial $\sigma(t)$ such that

$$\left\|\mathbf{r}'(t)\right\|^2 = x_1^2(t) + \cdots + x_n^2(t) = \sigma^2(t), \tag{2}$$

that is, the parametric speed $\left\|\mathbf{r}'(t)\right\|$ is polynomial.

Pythagorean-Hodograph curves (PH curves) were introduced by Farouki and Sakkalis in 1990. They have significant computational advantages when used for computer-aided design (CAD) and robotics applications since, among other things, their arc length can be computed precisely, i.e., without numerical quadrature, and their offsets are rational curves. Farouki's book [3] offers a fairly complete and self-contained exposition of this theory.

5.1 Formalization of PH curves and Hermite interpolation problem

The formal definition of PH curve in HOL Light is straightforward:

```
let pythagorean_hodograph = new_definition
 `pythagorean_hodograph r <=>
  vector_polynomial_function r /\
  real_polynomial_function
    (\t. norm (vector_derivative r (at t)))`;;
```

In our work, we deal with spacial PH curves which can be succinctly and profitably expressed in terms of the algebra of quaternions, and thus, are a natural application of our formalization of quaternionic algebra.

It turns out that, regarding $\mathbf{r}(t) = x(t)\mathbf{i} + y(t)\mathbf{j} + z(t)\mathbf{k}$ as a pure vector in $\mathbb{R}^3 \subset \mathbb{H}$, condition (2) holds if and only if exists a quaternionic polynomial $A(t)$ such that

$$\mathbf{r}'(t) = A(t)\mathbf{u}\bar{A}(t) \tag{3}$$

where $\mathbf{u}$ is any fixed unit vector and $\bar{A}(t)$ is the usual quaternionic conjugate of $A(t)$. We proved formally that the definition (2) follows from the previous condition.

```
QUAT_PH_CURVE
|- !r A u.
     u pow 2 = --Hx (&1) /\
     vector_polynomial_function A /\
     (!t. (r has_vector_derivative A t * u * cnj (A t)) (at t))
     ==> pythagorean_hodograph r
```

One basic question, with many practical applications, is whether there exists a PH curve with prescribed conditions on its endpoints.

Problem 1 (Hermite Interpolation Problem). Given the initial and final point $\{\mathbf{p}_i, \mathbf{p}_f\}$ and derivatives $\{\mathbf{d}_i, \mathbf{d}_f\}$, find a PH interpolation for this data set.

Following the work of Farouki et al. [2], here we treat only the case of cubic and quintic solutions of the above problem.

From condition (3) the problem can be reduced to finding a quaternionic polynomial $A(t)$, of degree 1 (for cubics) or 2 (for quintics), such that the curve $\mathbf{r}(t)$ obtained by integrating (3) satisfies $\mathbf{r}(0) = \mathbf{p_i}$, $\mathbf{r}(1) = \mathbf{p_f}$ and $\mathbf{r}'(0) = \mathbf{d_i}$, $\mathbf{r}'(1) = \mathbf{d_f}$.

5.2 PH cubic and quintic interpolant

As is well-known, for a given initial data set $\{\mathbf{p}_i, \mathbf{p}_f, \mathbf{d}_i, \mathbf{d}_f\}$, there is a unique "ordinary" cubic interpolant [3]. It turns out that such a curve is PH if and only if the data set satisfies specific conditions [2, Section 5], namely:

$$\mathbf{w} \cdot (\delta_i - \delta_f) = 0$$
$$\left(\mathbf{w} \cdot \frac{\delta_i + \delta_f}{|\delta_i + \delta_f|}\right)^2 + \frac{(\mathbf{w} \cdot \mathbf{z})^2}{|\mathbf{z}|^4} = |\mathbf{d}_i||\mathbf{d}_f|$$

where $\mathbf{w} = 3(\mathbf{p}_f - \mathbf{p}_i) - (\mathbf{d}_i + \mathbf{d}_f)$, $\delta_i = \frac{\mathbf{d}_i}{|\mathbf{d}_i|}$, $\delta_f = \frac{\mathbf{d}_f}{|\mathbf{d}_f|}$ and $\mathbf{z} = \frac{\delta_i \wedge \delta_f}{|\delta_i \wedge \delta_f|}$.

We formalized only one implication of this result, i.e., the sufficient condition for the "ordinary" cubic interpolant to be PH. The HOL theorem is

```
PH_CUBIC_INTERPOLANT_EXISTS
|- !Pf Pi di df:quat.
     let w = Hx(&3) * (Pf - Pi) - (di + df) in
     let n = \v. Hx(inv(norm v)) * v in
     let z = Hx(inv (norm (n di + n df))) *
             Hv(HIm(n di) cross HIm(n df)) in
     let r = \t. bernstein 3 0 (drop t) % Pi +
                 bernstein 3 1 (drop t) % (Pi + Hx(&1 / &3) * di) +
                 bernstein 3 2 (drop t) % (Pf - Hx(&1 / &3) * df) +
                 bernstein 3 3 (drop t) % Pf in
     Re Pf = &0 /\ Re Pi = &0 /\ Re di = &0 /\ Re df = &0 /\
     ~(Hx(&0) = di) /\ ~(Hx(&0) = df) /\ (!a. ~(n di = Hx a * df))
     ==>
     pathstart r = Pi /\ pathfinish r = Pf /\
     pathstart (\t. vector_derivative r (at t)) = di /\
     pathfinish (\t. vector_derivative r (at t)) = df /\
     (w dot (n di - n df) = &0 /\
      (w dot (n (n di + n df))) pow 2 +
      inv(norm z) pow 4 * (w dot z) pow 2 =
      norm di * norm df
      ==> pythagorean_hodograph r)`
```

where the curve $\mathbf{r}(t)$ is expressed in the Bernstein form.

We also formalized the analogous result for quintics. In this case the theory shows several differences, since, for instance, an Hermite PH quintic interpolant can be found for every initial data set. Actually, there is a two-parameter family of such interpolants [2, Section 6] and the algebraic expression of $\mathbf{r}(t)$ is substantially more complex with respect to the case of cubics. The formal statement of the theorem is about 40 lines of code and thus cannot be included here for lack of space (see theorem `PH_QUINTIC_INTERPOLANT` in file `ph_curve.hl` in our online repository).

Both of the aforementioned proofs consist essentially in algebraic manipulation on quaternions, so our formal framework has been very useful to automate many calculations that were implicit in the original paper [2, Section 6].

6 Conclusions

We laid the foundations for quaternionic calculus in the HOL Light theorem prover, which might be of general interest for developing further formalization in pure mathematics, physics, and for several possible applications in formal methods.

We also presented two applications. First, a formalization of quaternionic analysis with a focus on the theory of slice regular functions, as proposed by Gentili and Struppa. Secondly, the computer verified solutions to the Hermite interpolation problem for cubic and quintic PH curves.

Along the way, we provided a few extensions of the HOL Light library about multivariate and complex analysis, comprising limit superior and inferior, root test for series, Cauchy-Hadamard formula for the radius of convergence and some basic theorems about derivatives.

Overall, our contribution takes about 10,000 lines of code and consists in about 600 theorems, of which more than 350 have been included in the HOL Light library.

This work is open to a wide range of possible improvements and extensions. The most obvious line of developement would be to formalize further mathematical results about quaternions; there is an endless list of potential interesting candidates within reach from the present state of art.

For the core formalization of quaternions, we only provided basic procedures for algebraic simplification. They were somehow sufficient for automating several computations occurring in our development, but it surely would be interesting to implement more powerful decision procedures. Some of them would probably involve advanced techniques from non-commutative algebra.

References

1. Ciolli, G., Gentili, G., Maggesi, M.: A certified proof of the cartan fixed point theorems. Journal of Automated Reasoning 47(3), 319–336 (2011)
2. Farouki, R.T., Giannelli, C., Manni, C., Sestini, A.: Identification of spatial ph quintic hermite interpolants with near-optimal shape measures. Computer Aided Geometric Design 25(4), 274 – 297 (2008)
3. Farouki, R.: Pythagorean-Hodograph Curves: Algebra and Geometry Inseparable. Geometry and Computing, Springer Berlin Heidelberg (2009)
4. Fuchs, L., Théry, L.: Implementing geometric algebra products with binary trees. Advances in Applied Clifford Algebras 24(2), 589–611 (2014)
5. Gentili, G., Stoppato, C., Struppa, D.: Regular Functions of a Quaternionic Variable. Springer Monographs in Mathematics, Springer Berlin Heidelberg (2013)
6. Gentili, G., Struppa, D.C.: A new approach to cullen-regular functions of a quaternionic variable. Comptes Rendus Mathematique 342(10), 741 – 744 (2006)
7. Harrison, J.: A HOL theory of Euclidean space. In: Hurd, J., Melham, T. (eds.) Theorem Proving in Higher Order Logics, 18th International Conference, TPHOLs 2005. Lecture Notes in Computer Science, vol. 3603, pp. 114–129. Springer-Verlag, Oxford, UK (August 2005)
8. Harrison, J.: Formalizing basic complex analysis. In: Matuszewski, R., Zalewska, A. (eds.) From Insight to Proof: Festschrift in Honour of Andrzej Trybulec. Studies in Logic, Grammar and Rhetoric, vol. 10(23), pp. 151–165. University of Białystok (2007), http://mizar.org/trybulec65/
9. Ma, S., Shi, Z., Shao, Z., Guan, Y., Li, L., Li, Y.: Higher-order logic formalization of conformal geometric algebra and its application in verifying a robotic manipulation algorithm. Advances in Applied Clifford Algebras 26(4), 1305–1330 (2016)
10. Spivak, M.: Calculus on Manifolds: A Modern Approach to Classical Theorems of Advanced Calculus. Advanced book program, Avalon Publishing (1965)
11. Sudbery, A.: Quaternionic analysis. Mathematical Proceedings of the Cambridge Philosophical Society 85(02), 199–225 (3 1979)