J Autom Reasoning (2013) 50:173–190
DOI 10.1007/s10817-012-9250-9

# The HOL Light Theory of Euclidean Space

**John Harrison**

Received: 1 September 2011 / Accepted: 3 April 2012 / Published online: 19 April 2012

**Abstract** We describe the library of theorems about N-dimensional Euclidean space that has been formalized in the HOL Light prover. This formalization was started in 2005 and has been extensively developed since then, partly in direct support of the Flyspeck project, partly out of a general desire to develop a well-rounded and comprehensive theory of basic analytical, geometrical and topological machinery. The library includes various 'big name' theorems (Brouwer's fixed point theorem, the Stone-Weierstrass theorem, the Tietze extension theorem), numerous non-trivial results that are useful in applications (second mean value theorem for integrals, power series for real and complex transcendental functions) and a host of supporting definitions and lemmas. It also includes some specialized automated proof tools. The library has as planned been applied to the Flyspeck project and has become the basis of a significant development of results in complex analysis, among others.

**Keywords** Formalized mathematics · Euclidean space · Vector space · HOL

## 1 Introduction

A library of formalized mathematics can be considered as the logical formalization of a suitably chosen compendium of proven theorems from textbooks and papers, together perhaps with tools for the automation of common patterns of reasoning. This paper gives a brief overview of the substantial library of results about $N$-dimensional Euclidean space formalized in HOL Light.

The initial impetus from our development came from the Flyspeck project to formalize the Kepler conjecture [3], where most of the reasoning is based in $\mathbb{R}^3$ or occasionally $\mathbb{R}^2$ or $\mathbb{R}$. While a few concepts such as vector cross products, are specific to $\mathbb{R}^3$, most of the theory has been developed for general $\mathbb{R}^N$ so as to be more

J. Harrison (✉)
Intel Corporation, RA2-451, 2501 NW 229th Avenue, Hillsboro, OR 97124, USA
e-mail: johnh@ichips.intel.com

widely applicable. Our theorem prover HOL Light [6] is based on a logic without dependent types, but we can still encode the index $N$ as a type (roughly, an arbitrary indexing type of size $N$), so theorems about specific sizes like 3 really are just type instantiations of theorems for general $N$ stated with polymorphic type variables. The basic setup is described in more detail and some initial results are presented in [8]. Since that paper was written, the library has been very substantially expanded into new areas, and the present paper gives a more up-to-date picture.

With some minimal exceptions noted later we do not generalize beyond $\mathbb{R}^N$ to, for example, analysis in arbitrary Banach or Hilbert spaces. This has the evident disadvantage that if some more general results are needed, our library cannot be used directly to derive them, though the proofs could certainly be generalized in a mechanical way. On the positive side, our theory copes well with a wide range of applications and the formalization is pleasingly direct and uncluttered. For example, we simply say that a function $f : \mathbb{R}^M \to \mathbb{R}^N$ is 'continuous on $S$' rather than 'continuous as a function from the subtopology over $S$ of the Euclidean topology on $\mathbb{R}^M$ into the Euclidean topology on $\mathbb{R}^N$'. Most such details, as well as more mundane ones like ensuring compatibility of dimensions in matrix multiplication, are taken care of by the HOL type system and are mostly inferred automatically.

## 1.1 Famous Theorems Versus Technical Results

It's natural to focus any discussion of such a library around the most famous or substantial-seeming results. However, a focus purely on this is apt to give a misleading impression either of the level of sophistication of the library or the hard work or ingenuity that went into its construction. First of all, in applications it is often less important to have powerful 'big name' theorems than to have a systematic development of modest-seeming technical results, and this can often take just as much or more hard work. For example, our theory proves the Tietze extension theorem that a function $f : \mathbb{R}^M \to \mathbb{R}^N$ continuous on a closed set $S \subseteq \mathbb{R}^M$ has a continuous extension to the whole of $\mathbb{R}^M$ (`TIETZE_UNBOUNDED`):

```
|- ∀f:real^M->real^N s.
      closed s ∧ f continuous_on s
      ⇒ ∃g. g continuous_on (:real^M) ∧ (∀x. x ∈ s ⇒ g x = f x)
```

the Brouwer fixed point theorem that a continuous function $f$ from a nonempty convex compact $S \subseteq \mathbb{R}^N$ to itself has a fixed point (`BROUWER`):

```
|- ∀f:real^N->real^N s.
      compact s ∧ convex s ∧ ¬(s = {}) ∧
      f continuous_on s ∧ IMAGE f s SUBSET s
      ⇒ ∃x. x ∈ s ∧ f x = x
```

the Krein–Milman theorem (which might better be called the Minkowski theorem in our setting of $\mathbb{R}^N$) that a convex compact set is the convex hull of its set of extreme points (`KREIN_MILMAN_MINKOWSKI`):

```
|- ∀s:real^N->bool.
      convex s ∧ compact s ⇒ s = convex hull {x | x extreme_point_of s}
```

and the Riemann Mapping Theorem that a nontrivial, open and simply connected subset of $\mathbb{C}$ is biholomorphic to the unit disc (RIEMANN_MAPPING_THEOREM):

```
|- ∀s:complex->bool.
     open s ∧ simply_connected s ⇔
     s = {} ∨
     s = (:complex) ∨
     ∃f g. f holomorphic_on s ∧
           g holomorphic_on ball(Cx(&0),&1) ∧
           (!z. z ∈ s ⇒ f z ∈ ball(Cx(&0),&1) ∧ g(f z) = z) ∧
           (!z. z ∈ ball(Cx(&0),&1) ⇒ g z ∈ s ∧ f(g z) = z
```

However, it is often just as important to have less famous and more technical results such as the fact that an indefinite integral is a continuous function of the upper limit of integration (INDEFINITE_INTEGRAL_CONTINUOUS_RIGHT):

```
|- ∀f:real^M->real^N a b.
      f integrable_on interval[a,b]
      ⇒ (λx. integral (interval[a,x]) f) continuous_on interval[a,b]
```

or that the relative interior of a polyhedron $S$ defined by the intersection of its affine hull and a set of halfspaces $\bigcap_i \{x \mid a_i \cdot x \le b\}$ that is irredundant is in fact $S \cap \bigcap_i \{x \mid a_i \cdot x < b\}$ (RELATIVE_INTERIOR_POLYHEDRON_EXPLICIT):

```
|- ∀s:real^N->bool f a b.
      FINITE f ∧
      s = affine hull s INTER INTERS f ∧
      (∀h. h ∈ f ⇒ ¬(a h = vec 0) ∧ h = {x | a h dot x <= b h}) ∧
      (∀f'. f' PSUBSET f ⇒ s PSUBSET affine hull s INTER INTERS f')
      ⇒ relative_interior s =
              {x | x ∈ s ∧ ∀h. h ∈ f ⇒ a h dot x < b h}
```

or that the winding number of a simple curve around a point inside it (implying that the curve must be closed) is ±1 (SIMPLE_CLOSED_PATH_NORM_WINDING_NUMBER_INSIDE):

```
|- ∀g z. simple_path g ∧ z ∈ inside(path_image g)
         ⇒ norm(winding_number(g,z)) = &1
```

or simply an accurate rational approximation to $\pi$ (PI_APPROX_32):

```
|- abs(pi - &13493037705 / &4294967296) <= inv(&2 pow 32)
```

And collectively, we feel sure that those four technical results took considerably more work to establish than their four more famous relatives.

### 1.2 Serious Theorems Versus Trivialities

A striking contrast between textbooks and formalized libraries is that the latter tend to record for later use many 'theorems' that seem so simple and obvious that a textbook would probably not even mention them except perhaps in a casual aside, and wouldn't dignify them even with the appellation 'Lemma n'. That such banalities are needed in formalized mathematics reflects the relatively limited power of automated theorem provers: these 'trivial' results would not usually be established unaided by the built-in automation, but must explicitly be proved somewhere. Once proved, they could still be deployed in a more automated way as background knowledge, but our own style is to keep tighter control over the lemmas used and keep proofs fairly explicit.

Often, such facts only sink into one's consciousness after proving them several times in the course of another proof. Even if such a result is so simple that it only takes a couple of lines and a moment's thought, it can become very tedious to interrupt the flow of a more interesting proof to produce such a result repeatedly. So when this happens, we try to recognize it as a lemma, prove it separately, give it a name and thereafter refer to it by that name. Still, there are degrees of triviality. Some theorems are so simple that a detailed formal proof falls into one's mind almost immediately as necessary:

- The number $\pi$ is strictly positive (PI_POS)

```
|- &0 < pi
```

- A 2-element set is collinear (COLLINEAR_2)

```
|- ∀x y. collinear {x, y}
```

- A convex hull is indeed convex (CONVEX_CONVEX_HULL)

```
|- ∀s. convex (convex hull s)
```

- An 'open halfspace' is indeed an open set (OPEN_HALFSPACE_LT)

```
|- ∀a b. open {x | a dot x < b}
```

- If $x$, $y$ and $z$ are in an affine set, so is $x + a(y - z)$ (IN_AFFINE_ADD_MUL_DIFF)

```
|- ∀s a x y z.
        affine s ∧ x ∈ s ∧ y ∈ s ∧ z ∈ s ⇒ x + a % (y - z) ∈ s
```

- A nonempty open set cannot have measure zero (OPEN_NOT_NEGLIGIBLE)

```
|- ∀s. open s ∧ ¬(s = {}) ⇒ ¬negligible s
```

Some apparently 'trivial' properties are a bit more interesting, in that they are still pretty obvious but one needs to think at least briefly to come up with a formal proof, e.g.

- If a connected set contains a point $x$ where $a \cdot x \leq b$ and a point $y$ where $a \cdot y \geq b$ then it contains a $z$ such that $a \cdot z = b$ (CONNECTED_IVT_HYPERPLANE):

```
|- ∀s x y a b.
        connected s ∧ x ∈ s ∧ y ∈ s ∧ a dot x <= b ∧ b <= a dot y
        ⇒ ∃z. z ∈ s ∧ a dot z = b
```

- If two hyperplanes $H = \{x : \mathbb{R}^N \mid a \cdot x = b\}$ and $H' = \{x : \mathbb{R}^N \mid a' \cdot x = b'\}$ are such that $H \subseteq H'$, then except in the degenerate cases of $H = \emptyset$ (i.e.

$a = 0,\ b \neq 0$) or $H' = \mathbb{R}^N$ (i.e. $a' = 0,\ b = 0$), we actually have $H = H'$ (SUBSET_HYPERPLANES)

```
|- ∀a b a′ b′.
        {x | a dot x = b} SUBSET {x | a′ dot x = b′} ⇔
        {x | a dot x = b} = {} ∨
        {x | a′ dot x = b′} = (:real^N) ∨
        {x | a dot x = b} = {x | a′ dot x = b′}
```

Of course, the dividing line is subjective, and at the high end these tend towards results that seem rather trifling but are nevertheless useful to know and might well be explicitly noted in a sufficiently careful informal treatment. For example, the following is actually Theorem 2.3.4 of [20] and leads to many interesting consequences.

- If $c$ is in the relative interior of a convex set $S$ and $x$ in its closure then the segment $[c, x)$ is in the relative interior (IN_RELATIVE_INTERIOR_CLOSURE_CONVEX_SHRINK)

```
|- ∀s e x c.
        convex s ∧ c ∈ relative_interior s ∧ x ∈ closure s ∧
        &0 < e ∧ e <= &1
        ⇒ x - e % (x - c) ∈ relative_interior s
```

Moreover, theorems whether interesting or uninteresting sometimes collect trivial side-conditions that one might forget in an informal proof. For example, notice how the result about hyperplanes above (SUBSET_HYPERPLANES) needed to take into account cases where the so-called ‘hyperplane’ $\{x \mid a \cdot x = b\}$ degenerates because $a = 0$. The complex transcendental functions are particularly rich in tricky conditions that one can forget, and it is quite valuable (if annoying) that the machine never does forget and can help to keep track of them. When a theorem holds anyway in various degenerate cases that one wouldn’t consider, it’s arguably worth the effort to prove it without unnecessary conditions, since those conditions would otherwise need to be checked each time the theorem is deployed. For example, consider the theorem that a continuous mapping $f$ from a sphere with center $a$ and radius $r$ to some other set $s$ is homotopic to some constant function $\lambda x.\, c$ iff it extends to a continuous $g$ defined on the whole of the corresponding closed ball (NULLHOMOTOPIC_SPHERE_EXTENSION):

```
|- ∀f:real^M->real^N s a r.
      (∃c. homotopic_with (λx. T) ({x | norm(x - a) = r},s) f (λx. c)) ⇔
      (∃g. g continuous_on cball(a,r) ∧ IMAGE g (cball(a,r)) SUBSET s ∧
           ∀x. x ∈ {x | norm(x - a) = r} ⇒ g x = f x
```

This theorem has no condition that the radius $r$ is positive, because the theorem turns out to be degenerately true if $r < 0$ or $r = 0$, and the requirement that $f$ be continuous is not made an explicit condition because it follows automatically from either side of the equivalence.

### 1.3 Orientation

The following table lists the files containing proof scripts, in their standard build order, with an indication of roughly what they contain and the number of bytes and lines (this is for revision 130 at the HOL Light download site http://code.google.com/p/hol-light/). The complete library, including the background material from the HOL Light core and other libraries, contains 9724 named formal theorems.

| File | Bytes | Lines | Contents |
|---|---:|---:|---|
| misc.ml | 20,611 | 492 | Background on suprema, hulls etc. |
| vectors.ml | 325,273 | 7,531 | Vectors in $\mathbb{R}^N$, matrices, linear algebra |
| determinants.ml | 105,718 | 2,243 | Determinants of $N \times N$ matrices |
| topology.ml | 604,696 | 13,111 | General topology, mainly on $\mathbb{R}^N$ |
| convex.ml | 877,880 | 18,055 | Affine and convex sets, convex functions |
| polytope.ml | 253,278 | 5,200 | Faces, extreme points, polytopes, polyhedra |
| dimension.ml | 259,851 | 5,275 | Brouwer, Jordan curve theorem |
| derivatives.ml | 119,474 | 2,466 | Fréchet derivatives, mean value theorem etc. |
| clifford.ml | 44,977 | 979 | Geometric (Clifford) algebra |
| integration.ml | 775,569 | 15,846 | Kurzweil–Henstock gauge integration in $\mathbb{R}^N$ |
| measure.ml | 384,253 | 7,830 | Lebesgue measure, measurable functions |
| complexes.ml | 73,182 | 1,911 | Complex numbers, arithmetic, conjugation etc. |
| canal.ml | 139,416 | 3,040 | Basic analysis over complex numbers |
| transcendentals.ml | 264,412 | 5,869 | Real and complex transcendental functions |
| realanalysis.ml | 616,694 | 13,340 | Analytical theorems in special case $\mathbb{R}$ |
| cauchy.ml | 758,016 | 14,997 | Cauchy integral theorem and consequences |
| All files | 5,623,300 | 118,185 | TOTAL |

The next section goes in more detail into the contents of most of these files. Since space is limited, we can only give a very brief sketch of each, and readers are encouraged to browse the formal proof scripts at the URL given above.

## 1.4 Authorship and Informal Models

This formalization was started by the present author, and the majority of the proof scripts are still by him, but others have made substantial direct contributions (not to mention the pervasive influence of the Flyspeck project). Lars Schewe contributed a significant part of the material on convex and affine sets, including basic theorems about affine dependence and Radon's theorem. The basic results on complex analysis developed by the present author were considerably extended by Marco Maggesi and his collaborators including Graziano Gentili and Gianni Ciolli (higher complex derivatives, the Cartan theorems) and Valentina Bruno (Cauchy's inequality, analytic continuation, maximum modulus principle, Schwartz's Lemma).

For most non-trivial results, the first step before creating a formal proof is to have a clearly understood informal proof in mind. We have not followed any one specific treatment of any large area of mathematics, but have always chosen what seemed the best proof from the available literature based on what results had already been formalized and our intuition about how easy certain informal proofs are to formalize. We would just mention two nice textbooks that we have found ourselves returning to over and over again, Webster's book on convexity [20] and Yee and Vyborny's book on the Kurzweil–Henstock integral [22].

## 2 A Tour of the Library

Here we will systematically go through the files listed above giving a slightly more detailed idea of their content. To save space, we will omit most of the complex analysis files, a fairly detailed description of the initial development of which can be found elsewhere [9].

### 2.1 misc.ml

This file does not yet talk about vectors in $\mathbb{R}^N$ but contains some auxiliary material that is used when we do. For example, it contains additional lemmas about suprema and infima like this one (`SUP_FINITE`):

```
|- ∀s. FINITE s ∧ ¬(s = {}) ⇒ sup s ∈ s ∧ (∀x. x ∈ s ⇒ x <= sup s)
```

It also contains a general '`hull`' operation, written infix, which given a predicate *P* and a set *s* yields the intersection of all supersets of *s* satisfying *P*:

```
|- ∀P s. P hull s = INTERS {t | P t ∧ s SUBSET t}
```

This is used in several places later, most notably 'convex hull' and 'affine hull', and it is attractive that some of the general properties can be deduced without special knowledge of *P*, for examples this one (`HULL_MINIMAL`)

```
HULL_MINIMAL = |- ∀P s t. s SUBSET t ∧ P t ⇒ (P hull s) SUBSET t
```

### 2.2 vectors.ml

This is where the basic operations on vectors in $\mathbb{R}^N$ are defined, for example addition (using overloading of the conventional '+' symbol) and scalar-vector multiplication (using the distinct symbol '%'). We also define the usual `dot` (inner) product, in a way quite close to the informal notation $x \cdot y = \sum_{i=1}^{N} x_i y_i$, except that since our `N` is a *type*, we need to convert it to a number by applying `dimindex` to its universe set:

```
|- (x:real^N) dot (y:real^N) =
      sum(1..dimindex(:N)) (λi. x$i * y$i)
```

We then also define the usual Euclidean norm `norm` and distance `dist` functions.

```
|- norm x = sqrt(x dot x)
```

```
|- dist(x,y) = norm(x - y)
```

Among other theorems, we prove the triangle law `NORM_TRIANGLE` and the Cauchy–Schwarz inequality `NORM_CAUCHY_SCHWARZ`:

```
|- ∀x y. norm(x + y) <= norm(x) + norm(y)
```

```
|- ∀x y. abs(x dot y) <= norm(x) * norm(y)
```

Other vectorial concepts formalized include orthogonality, between-ness and collinearity. Here is a typical theorem (`COLLINEAR_BETWEEN_CASES`) relating the last two concepts:

```
|- ∀a b c:real^N.
       collinear {a,b,c} ⇔
       between a (b,c) ∨ between b (c,a) ∨ between c (a,b)
```

Next we define the notion of `linear` function $\mathbb{R}^M \to \mathbb{R}^N$

```
|- linear (f:real^M->real^N) ⇔
       (∀x y. f(x + y) = f(x) + f(y)) ∧
       (∀c x. f(c % x) = c % f(x))
```

and also operations on matrices, treating matrices as vectors of vectors in a uniform way. We then proceed to develop a body of basic linear algebra theorems, standard fare about spans, subspaces, bases, dimension and rank. For example, this theorem relates the dimension of a space of sums to the intersection and its constituents (`DIM_SUMS_INTER`):

```
|- ∀s t:real^N->bool.
       subspace s ∧ subspace t
       ⇒ dim {x + y | x ∈ s ∧ y ∈ t} + dim(s INTER t) = dim(s) + dim(t)
```

We often want to switch between the types $\mathbb{R}^1$ and $\mathbb{R}$, which are formally different, and we do this via mutually inverse functions `lift` : $\mathbb{R} \to \mathbb{R}^1$ and `drop` : $\mathbb{R}^1 \to \mathbb{R}$.

### 2.3 determinants.ml

Here we define the determinant of an $N \times N$ matrix (`det`):

```
|- det(A:real^N^N) =
       sum { p | p permutes 1..dimindex(:N) }
           (λp. sign(p) * product (1..dimindex(:N)) (λi. A$i$(p i)))
```

and deduce various standard properties from this very explicit definition, such as the product formula (`DET_MUL`). The double star used for matrix multiplication here is also overloaded for vector-matrix and matrix-vector multiplication:

```
|- ∀A B:real^N^N. det(A ** B) = det(A) * det(B)
```

We also prove Cramer's rule (CRAMER), which is stated using the 'lambda' function used to construct a vector (including a vector of vectors, which is our representation of a matrix) componentwise:

```
|- ∀A:real^N^N x b.
       ¬(det(A) = &0)
       ⇒ (A ** x = b ⇔
            x = lambda k.
                  det((lambda i j. if j = k then b$i else A$i$j):real^N^N) /
                  det(A))
```

In this file we also define orthogonal transformations and various theorems associated with them.

### 2.4 topology.ml

Here we start with a somewhat rudimentary development of general topological spaces, defining concepts like open_in, whether a set is open in a particular topology. But this fairly general material is brief and only exploited to define relative interiors (with respect to a set's affine hull). Most of the time we work with respect to the standard Euclidean topology, and here we define the usual topological concepts like open, compact, connected, limit_point_of (which asserts that a point is a limit point of a set), interior, closure and frontier (boundary). Here, for example, is the Heine-Borel theorem that a set is compact iff every open cover has a finite subcover (COMPACT_EQ_HEINE_BOREL):

```
|- compact s ⇔
   ∀f. (∀t. t ∈ f ⇒ open t) ∧ s SUBSET (UNIONS f)
       ⇒ ∃f'. f' SUBSET f ∧ FINITE f' ∧ s SUBSET (UNIONS f')
```

We include some properties that might not strictly be considered topological, such as boundedness (bounded) and completeness (complete), the latter being used, for example, in the Banach fixed point theorem:

```
|- ∀f s c. complete s ∧ ¬(s = {}) ∧
           &0 <= c ∧ c < &1 ∧
           (IMAGE f s) SUBSET s ∧
           (∀x y. x ∈ s ∧ y ∈ s ⇒ dist(f(x),f(y)) <= c * dist(x,y))
           ⇒ ∃!x:real^N. x ∈ s ∧ (f x = x)
```

Also in this file we define a reasonably general notion of limit (something close to Smith–Moore convergence nets). We pay particular attention to convergence at a point (possibly approached within a set) and convergence of a sequence, which can be characterized in the standard way even though the actual definitions are more technical (LIM_WITHIN and LIM_SEQUENTIALLY):

```
|- (f --> l) (at a within s) ⇔
       ∀e. &0 < e
           ⇒ ∃d. &0 < d ∧
                 ∀x. x ∈ s ∧ &0 < dist(x,a) ∧ dist(x,a) < d
                 ⇒ dist(f(x),l) < e

|- (s --> l) sequentially ⇔
       ∀e. &0 < e ⇒ ∃N. ∀n. N <= n ⇒ dist(s(n),l) < e
```

We prove various routine combining theorems about limits, most of which are independent of the particular kind of limit, such as the following (LIM_SUB):

```
|- ∀net f g l m.
   (f --> l) net ∧ (g --> m) net ⇒ ((λx. f(x) - g(x)) --> l - m) net
```

We also define uniform convergence, continuity and uniform continuity and a slew of similar routine combining theorems, and set up notation for open and closed intervals and segments using an overloading trick to approximate the common convention of using $[a, b]$ for the closed version and $(a, b)$ for the open. Thus for example, the intervals written `interval[a,b]` and `interval(a,b)` are respectively the set of points $x$ such that $a_i \leq x_i \leq b_i$ or $a_i < x_i < b_i$ for each coordinate. Note that these are $N$-dimensional intervals, so we might have chosen to call them ‘boxes’ or ‘rectangles’ to avoid misleading one-dimensional connotations of the name.

### 2.5 convex.ml

This file starts by defining the notions of convex and affine set, which are used constantly in more geometrical reasoning:

```
|- affine s ⇔ ∀x y u v. x ∈ s ∧ y ∈ s ∧ u + v = &1
                         ⇒ (u % x + v % y) ∈ s

|- convex s ⇔
   ∀x y u v. x ∈ s ∧ y ∈ s ∧ &0 <= u ∧ &0 <= v ∧ u + v = &1
             ⇒ (u % x + v % y) ∈ s
```

In particular, we develop properties of the affine and convex hulls of a set, and also define the notion of affine dimension (`aff_dim`), which is similar to `dim` except that the origin is not privileged and we define it as an integer rather than a natural number so that we can maintain the usual convention that the affine dimension of the empty set is $-1$. Using the general notion of affine dependence we also define the special case of coplanarity and more about collinearity, and we define the concept of relative interior and prove several important properties. Among the more interesting theorems proved here are Radon’s theorem that an affinely dependent set can be partitioned into two parts whose convex hulls overlap (RADON):

```
|- ∀c. affine_dependent c
       ⇒ ∃(m:real^N->bool) (p:real^N->bool).
              m SUBSET c ∧ p SUBSET c ∧ DISJOINT m p ∧
              ¬(DISJOINT (convex hull m) (convex hull p))
```

and various classic results about separating convex sets from each other by hyperplanes, e.g. this result (SEPARATING_HYPERPLANE_COMPACT_CLOSED):

```
|- ∀s t. convex s ∧ compact s ∧ ¬(s = {}) ∧
         convex t ∧ closed t ∧ DISJOINT s t
         ⇒ ∃a b. (∀x. x ∈ s ⇒ a dot x < b) ∧
                 (∀x. x ∈ t ⇒ a dot x > b)
```

A few additional notions like continuous paths (`path`) and the special case of arcs (`arc`) are defined here because it is more convenient to have some of the theorems about convex sets available for various lemmas. We also derive some theorems about connectedness as trivial consequences of theorems about convexity, even though they could have been proved earlier with little extra effort. Sometimes there is a trade-off between finding the simplest and most natural proof and putting related proofs together. Similarly, results on homotopy of continuous functions and contractibility and simple connectedness of topological spaces also end up here. (These are used extensively in complex analysis.) Since this material has grown significantly it should probably be separated out into its own file.

### 2.6 polytope.ml

Here we start by defining ‘extreme points’ and ‘faces’ of a convex set, e.g.

```
|- t face_of s ⇔
      t SUBSET s ∧ convex t ∧
      ∀a b x. a ∈ s ∧ b ∈ s ∧ x ∈ t ∧ x ∈ segment(a,b)
              ⇒ a ∈ t ∧ b ∈ t
```

We develop a number of properties of faces and extreme points in general, notably the Krein–Milman theorem that we have mentioned above, and various others such as the following (`FACE_OF_FACE`, `FACE_OF_TRANS` and `FACE_OF_SING`):

```
|- ∀f s t. t face_of s ⇒ (f face_of t ⇔ f face_of s ∧ f SUBSET t)

|- ∀s t u. s face_of t ∧ t face_of u ⇒ s face_of u‘,

|- ∀x s. {x} face_of s ⇔ x extreme_point_of s
```

Most of the file is concerned with polytopes, which are convex hulls of finite sets, and polyhedra, which are finite intersections of halfspaces:

```
|- polytope s ⇔ ∃v. FINITE v ∧ s = convex hull v

|- polyhedron s ⇔
       ∃f. FINITE f ∧
           s = INTERS f ∧
           (∀h. h ∈ f ⇒ ∃a b. ¬(a = vec 0) ∧ h = {x | a dot x <= b})
```

After a fairly long development of technical lemmas (one example of which was mentioned above), we end up with some relatively simple properties such as the characterization of polytopes as bounded polyhedra (`POLYTOPE_EQ_BOUNDED_POLYHEDRON`):

```
|- ∀s. polytope s ⇔ polyhedron s ∧ bounded s
```

### 2.7 dimension.ml

This file contains a small number of deeper theorems about the topology of $\mathbb{R}^N$, most significantly the Brouwer fixed point theorem (see `BROUWER` above), which is proved using a combinatorial lemma following Kuhn [15]. This is somewhat analogous to the “Sperner’s Lemma” proof often found in books, but trades a more complex combinatorial lemma for a simpler subdivision of a large cube into cubes rather than a simplex into simplices.

Brouwer's theorem is immediately applied to a useful lemma sometimes called the 'Fashoda meet theorem', that if one continuous path goes from top to bottom of a rectangle in $\mathbb{R}^2$ and another goes from left to right, then they must cross (FASHODA):

```
|- ∀f g a b:real^2.
        path f ∧ path g ∧
        path_image f SUBSET interval[a,b] ∧
        path_image g SUBSET interval[a,b] ∧
        (pathstart f)$1 = a$1 ∧ (pathfinish f)$1 = b$1 ∧
        (pathstart g)$2 = a$2 ∧ (pathfinish g)$2 = b$2
        ⇒ ∃z. z ∈ path_image f ∧ z ∈ path_image g
```

This in its turn is used as a major lemma in the proof of the Jordan Curve Theorem (JORDAN_CURVE_THEOREM), which had already been proved by Hales using a somewhat different proof [4].

```
|- ∀c:real^1->real^2.
        simple_path c ∧ pathfinish c = pathstart c
        ⇒ ∃ins out.
                ¬(ins = {}) ∧ open ins ∧ connected ins ∧
                ¬(out = {}) ∧ open out ∧ connected out ∧
                bounded ins ∧ ¬bounded out ∧
                ins INTER out = {} ∧
                ins UNION out = (:real^2) DIFF path_image c ∧
                frontier ins = path_image c ∧
                frontier out = path_image c
```

### 2.8 derivatives.ml

Here we define the traditional Frechet derivative of a function, meaning essentially a local linear approximation

```
|- (f has_derivative f') (at x) ⇔
        linear f' ∧
        ((λy. inv(norm(y - x)) % (f(y) - (f(x) + f'(y - x)))) --> vec 0)
        (at x)
```

All the usual results such as derivatives of sums are easy to prove:

```
|- (f has_derivative f') net ∧ (g has_derivative g') net
       ⇒ ((λx. f(x) + g(x)) has_derivative (λh. f'(h) + g'(h))) net
```

and the 'chain rule' is also reasonably straightforward:

```
|- (f has_derivative f') (at x) ∧
   (g has_derivative g') (at (f x))
   ⇒ ((g o f) has_derivative (g' o f')) (at x)
```

We also prove a somewhat unusual version of the inverse function theorem, which does not a priori require continuity of the derivative [19].

```
|- open s ∧ f continuous_on s ∧
   x ∈ s ∧ (f has_derivative f') (at x) ∧ linear g' ∧ (f' o g' = I)
   ⇒ ∀t. t SUBSET s ∧ x ∈ interior(t)
          ⇒ f(x) ∈ interior(IMAGE f t)
```

### 2.9 clifford.ml

This file is a development of some of the basics of geometric algebra. Because it is not used in what follows and is somewhat experimental (though we anticipate using it to develop a theory of differential forms) we will not discuss it further.

### 2.10 integration.ml

This file is a development of integration in a quite general context, of functions $\mathbb{R}^M \to \mathbb{R}^N$ over an arbitrary subset $s \subseteq \mathbb{R}^M$. The definition is based on the Kurzweil–Henstock gauge integral. We will not go through the somewhat technical definitions, but the basic concept defined is `(f has_integral y) s`, meaning that $\int_s f = y$ and that integral is defined. There are numerous simple manipulative theorems proved, including the composition with a linear function (`HAS_INTEGRAL_LINEAR`):

```
|- ∀f:real^M->real^N y s h:real^N->real^P.
        (f has_integral y) s ∧ linear h ⇒ ((h o f) has_integral h(y)) s
```

and the integrability of uniform limits (`INTEGRABLE_UNIFORM_LIMIT`)

```
|- ∀f a b. (∀e. &0 < e
                ⇒ ∃g. (∀x. x ∈ interval[a,b] ⇒ norm(f x - g x) <= e) ∧
                        g integrable_on interval[a,b])
            ⇒ (f:real^M->real^N) integrable_on interval[a,b]
```

There are also many deeper results such as the powerful monotone and dominated convergence theorems, the latter (`DOMINATED_CONVERGENCE`) looking like this:

```
|- ∀f:num->real^M->real^N g h s.
      (∀k. (f k) integrable_on s) ∧ h integrable_on s ∧
      (∀k x. x ∈ s ⇒ norm(f k x) <= drop(h x)) ∧
      (∀x. x ∈ s ⇒ ((λk. f k x) --> g x) sequentially)
     ⇒ g integrable_on s ∧
          ((λk. integral s (f k)) --> integral s g) sequentially
```

The gauge integral is a ‘nonabsolute’ generalization of the Lebesgue integral on Euclidean space, but we define the following notion that turns out to be exactly equivalent to Lebesgue integration as traditionally defined:

```
|- f absolutely_integrable_on s ⇔
        f integrable_on s ∧ (λx. lift(norm(f x))) integrable_on s
```

### 2.11 measure.ml

In this file we define two variants of measurability. One, `lebesgue_measurable`, is defined in a more traditional way based on a theory of measurable functions, while the other `measurable` is defined directly in terms of integration of characteristic functions. The latter corresponds to measurability with a bounded measure, which is returned by a function `measure`. We also have a concept of a null set, `negligible`, which corresponds to having measure zero. We prove various routine closure properties (these are called MEASURE_NEGLIGIBLE_UNION and MEASURABLE_INTER):

```
|- ∀s t. measurable s ∧ measurable t ∧ negligible(s INTER t)
         ⇒ measure(s UNION t) = measure s + measure t

|- ∀s t. measurable s ∧ measurable t ⇒ measurable (s INTER t)
```

as well as the measurability of various well-behaved sets (these are MEASURABLE_COMPACT and LEBESGUE_MEASURABLE_OPEN)

```
|- ∀s. compact s ⇒ measurable s

|- ∀s. open s ⇒ lebesgue_measurable s
```

and conversely, the fact that measurable sets can be approximated by well-behaved ones (this is MEASURABLE_OUTER_OPEN):

```
|- ∀s e. measurable s ∧ &0 < e
         ⇒ ∃t. open t ∧ s SUBSET t ∧
               measurable t ∧ measure t < measure s + e
```

A slightly more exotic theorem is Steinhaus's that if a set has strictly positive measure then its set of differences has nonempty interior (STEINHAUS):

```
|- ∀s. measurable s ∧ &0 < measure s
       ⇒ ∃d. &0 < d ∧ ball(vec 0,d) SUBSET {x - y | x ∈ s ∧ y ∈ s}
```

### 2.12 transcendentals.ml

This file defines transcendental functions over the complex numbers and the real numbers. Generally speaking we derive the complex variants as basic and then deduce properties of the real functions from those. For example, the complex exponential function is defined by its power series:

```
|- cexp z = infsum (from 0) (λn. z pow n / Cx(&(FACT n)))
```

and the real version defined in terms of that

```
|- exp(x) = Re(cexp(Cx x))
```

We prove a number of standard ‘algebraic’ facts, e.g SIN_ADD:

```
|- ∀x y. sin(x + y) = sin(x) * cos(y) + cos(x) * sin(y)
```

as well as continuity and differentiability properties, e.g. the following for continuity of the complex arctangent:

```
|- ∀s. (∀z. z ∈ s ∧ Re z = &0 ⇒ abs(Im z) < &1) ⇒ catn continuous_on s
```

### 2.13 realanalysis.ml

In this file we deduce a slew of real analytical theorems from their counterparts either over $\mathbb{R}^1$ or $\mathbb{C}$. Most of these proofs are entirely routine, even though it is somewhat tedious to have to redefine essentially equivalent notions over the reals instead of vectors (e.g. `has_real_integral` instead of `has_integral`. Some theorems that were proved earlier reach their cleanest and most natural form here, such as the fundamental theorem of calculus, including this slightly generalized form

```
|- ∀f f’ s a b.
        FINITE s ∧
        a <= b ∧ f real_continuous_on real_interval[a,b] ∧
        (∀x. x ∈ real_interval(a,b) DIFF s
             ⇒ (f has_real_derivative f’(x)) (atreal x))
        ⇒ (f’ has_real_integral (f(b) - f(a))) (real_interval[a,b])
```

and the integral Second Mean Value Theorem (`REAL_SECOND_MEAN_VALUE_THEOREM`):

```
|- ∀f g a b.
        ¬(real_interval[a,b] = {}) ∧
        f real_integrable_on real_interval[a,b] ∧
        (∀x y. x ∈ real_interval[a,b] ∧ y ∈ real_interval[a,b] ∧ x <= y
               ⇒ g x <= g y)
        ⇒ ∃c. c ∈ real_interval[a,b] ∧
               real_integral (real_interval[a,b]) (λx. g x * f x) =
                 g(a) * real_integral (real_interval[a,c]) f +
                 g(b) * real_integral (real_interval[c,b]) f
```

This file often acts as a confluence of earlier threads that are brought together in a number of non-trivial theorems including the Stone-Weierstrass theorem and invariance of domain and dimension, e.g. `INVARIANCE_OF_DOMAIN`:

```
|- ∀f:real^N->real^N s.
        f continuous_on s ∧ open s ∧
        (∀x y. x ∈ s ∧ y ∈ s ∧ f x = f y ⇒ x = y)
        ⇒ open(IMAGE f s)
```

## 3 Additional Inference Rules

As well as theorems, we have defined several convenient inference rules to improve the level of automation. These include tools for automatically ‘differentiating by proof’ expressions involving real and complex transcendental functions, or for proving that they are continuous, by automatically recursing through combining theorems like the chain rule. While valuable, there is not much novelty since the idea already appears in much older work [7].

We have also implemented a simple tool for proving routine algebraic properties of vector expressions by reducing them to componentwise real operations. A more interesting one decides the universal additive theory of normed spaces, which is very useful for intricate ‘triangle law’ reasoning. This is a simple case of one of the decision procedures discussed in [18].

Another interesting and unusual tool supports the common style of picking convenient coordinate axes ‘without loss of generality’ by exploiting translation, scaling and orthogonal transformation. It works by automatically using a database of theorems asserting invariances of various properties under such transformations [10]. This is invaluable for more intricate results in geometry, where a convenient choice of frame can make the eventual algebraic reduct of a geometrical problem dramatically easier.

## 4 Related Work

The formalization of properties of real numbers in theorem provers goes back at least to Jutting [13]. Since this pioneering work, many people have worked on formalizations in various theorem provers of real and complex analysis, topology, measure theory etc. that have significant overlap with our work [2, 4, 7, 12, 16]. In some cases this work is more limited in scope, in that it only tackles properties of $\mathbb{R}$ or $\mathbb{R}^2$ rather than the significantly richer domain of $\mathbb{R}^N$ for arbitrary $N$. In other cases it is actually more general, for example covering arbitrary measure spaces instead of just Lebesgue measure in $\mathbb{R}^N$, though this generality can come at the cost of more intricate statements that are more difficult to apply in concrete cases.

By most measures the largest and most systematically developed library of formalized mathematics is the Mizar Mathematical Library; according to [21] a recent version contains approximately 2 million lines of proof scripts, covering a wide range of mathematical domains. This includes quite a lot of results that are similar to those in our formalization. There are too many individual articles for us to summarize them all here, but the reader is encouraged to browse the table of contents at http://mizar.org/fm/. However, it has been developed in a more piecemeal way by many authors, and not motivated as clearly by a real application like Flyspeck, so there is not yet such a systematic feel to this collection of results.

## 5 Conclusions and Future Work

After about 7 years of development, this theory is becoming quite a comprehensive compendium of results about Euclidean space, and we continue to extend it all the time, partly driven by applications. By far the most significant application is Flyspeck [5], but we have also recently been experimenting with formalization of $L_p$ spaces and Fourier series, Pick's theorem and Euler's polyhedron formula. With each new application we find some fundamental results missing, but the gaps are getting less and less significant over time, and the library is attaining the feel of a satisfying whole.

Occasionally the restriction to $\mathbb{R}^N$ is a hindrance, and we wish that some parts of the work had been done more generally. Even with the restriction to $\mathbb{R}^N$ accepted, the technical details of representing this space in the limited HOL type system cause some complications. In particular, proofs by induction over dimension are usually done in a somewhat intricate style by mapping $\mathbb{R}^M$ for $M \leq N$ into $\mathbb{R}^N$ as a subset, since we cannot directly perform induction on the size of types. But for the most part we are satisfied with the uncluttered feel of the library and its easy applicability to a wide range of interesting problems including Flyspeck.

One glaring omission is any serious machinery for algebraic topology, which might provide a more natural route to some of our existing results and to new ones like the

Borsuk-Ulam theorem. We do have various basic results about homotopy including what are in effect the 'fundamental group' properties, and we have sufficient material on polyhedra to support the definition of homology groups, but none of this algebraic machinery has actually been set up. The results on multiple integrals and change of variable in integrals are rudimentary, with only fairly weak Fubini-like results. There is also currently no material on differential forms or differentiable manifolds, though eventually we hope our geometric algebra development will provide a suitable basis for such formalizations.

There is certainly scope for more automation, since many of the current proofs are quite long and technical. HOL Light has a built-in first-order prover `MESON` which can help to bridge simple logical gaps. There has been considerable work going back at least to [11] on exploiting more powerful 'off-the-shelf' first-order provers. This kind of support would certainly enable larger gaps to be bridged and make it possible to omit explicit references to lemmas to be used since the prover is capable of determining useful lemmas itself; experience indicates that this can be quite productive [17]. Nevertheless, first-order logic only covers a relatively small part of the proofs here, which often involve higher-order reasoning, arithmetic and algebra. Combining all these in an effective way is not easy. One common and slightly tedious pattern is the need to instantiate index variables for coordinates before being able to use purely automated arithmetic or algebraic reasoning, e.g. to deduce from $\forall i.\ 1 \leq i \leq n \Rightarrow x_i \geq 0$ and $\forall i.\ 1 \leq i \leq n \Rightarrow y_i \geq 0$ that $\forall i.\ 1 \leq i \leq n \Rightarrow x_i + y_i \geq 0$. We believe that this can be substantially automated using ideas from [1], and this might be a useful step.

Given the large investment of time and effort put into this formalization, it would be appealing if the work could be re-used in other systems. For example, it might be possible to extend the work on importing HOL Light into Coq [14] to cover this domain of mathematics. Moreover, if we or somebody else did want a more general formalization in HOL Light (e.g. in the setting of arbitrary normed spaces), many proofs are 'morally the same' and it would be appealing to be able to use similar technology to generalize the proofs in a mechanical way. This should be possible, but we are not aware of any actual work in this area.

**Acknowledgements** The author is grateful to everyone who has helped with the development of the library (most of whom have been named above), and to the anonymous reviewers for their useful comments on the first version of this paper.

## References

1. Fontaine, P.: Techniques for verification of concurrent systems with invariants. Ph.D. thesis, Institut Montefiore, Université de Liège (2004)
2. Geuvers, H., Wiedijk, F., Zwanenburg, J.: A constructive proof of the fundamental theorem of algebra without using the rationals. In: Callaghan, P., Luo, Z., McKinna, J., Pollack, R. (eds.) Types for Proofs and Programs, Proceedings of the International Workshop, TYPES 2000. Lecture Notes in Computer Science, vol. 2277, pp. 96–111. Springer (2001)
3. Hales, T.C.: Introduction to the Flyspeck project. In: Coquand, T., Lombardi, H., Roy, M.-F. (eds.) Mathematics, Algorithms, Proofs. Dagstuhl Seminar Proceedings, vol. 05021. Internationales Begegnungs- und Forschungszentrum fuer Informatik (IBFI), Schloss Dagstuhl, Germany (2006)
4. Hales, T.C.: The Jordan curve theorem, formally and informally. Am. Math. Mon. **114**, 882–894 (2007)

5. Hales, T.C., Harrison, J., McLaughlin, S., Nipkow, T., Obua, S., Zumkeller, R.: A revision of the proof of the Kepler conjecture. Discrete Comput. Geom. **44**, 1–34 (2010)
6. Harrison, J.: HOL light: a tutorial introduction. In: Srivas, M., Camilleri, A. (eds.) Proceedings of the First International Conference on Formal Methods in Computer-Aided Design (FM-CAD'96), Lecture Notes in Computer Science, vol. 1166, pp. 265–269. Springer (1996)
7. Harrison, J.: Theorem Proving with the Real Numbers. Springer (1998). Revised version of author's Ph.D. thesis
8. 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, Oxford, UK (2005)
9. 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)
10. Harrison, J.: Without loss of generality. In: Berghofer, S., Nipkow, T., Urban, C., Wenzel, M. (eds.) Proceedings of the 22nd International Conference on Theorem Proving in Higher Order Logics, TPHOLs 2009. Lecture Notes in Computer Science, vol. 5674, pp. 43–59. Springer, Munich, Germany (2009)
11. Hurd, J.: Integrating Gandalf and HOL. In: Bertot, Y., Dowek, G., Hirschowitz, A., Paulin, C., Théry, L. (eds.) Theorem Proving in Higher Order Logics: 12th International Conference, TPHOLs'99. Lecture Notes in Computer Science, vol. 1690, pp. 311–321. Springer, Nice, France (1999)
12. Hurd, J.: Formal verification of probabilistic algorithms. Ph.D. thesis, University of Cambridge (2001)
13. Jutting, L.S.v.B.: Checking Landau's "Grundlagen" in the AUTOMATH system. Ph.D. thesis, Eindhoven University of Technology (1977). Useful summary in Nederpelt, R.P., Geuvers, J.H., Vrijer, R.C.d. (eds.) Selected Papers on Automath. Studies in Logic and the Foundations of Mathematics, vol. 133, pp. 701–732. North-Holland (1994)
14. Keller, C., Werner, B.: Importing HOL light into Coq. In: Kaufmann, M., Paulson, L.C. (eds.) First International Conference on Interactive Theorem Proving, ITP 2010. Lecture Notes in Computer Science, vol. 6172, pp. 307–322. Springer, Edinburgh, UK (2010)
15. Kuhn, H.W.: Some combinatorial lemmas in topology. IBM J. Res. Dev. **4**, 518–524 (1960)
16. Milewski, R.: Fundamental theorem of algebra. J. Formal. Math. **12** (2000). http://mizar.org/JFM/Vol12/polynom5.html
17. Paulson, L.C., Blanchette, J.C.: Three years of experience with Sledgehammer, a practical link between automatic and interactive theorem provers. In: Sutcliffe, G., Ternovska, E., Schulz, S. (eds.) Proceedings of the 8th International Workshop on the Implementation of Logics, pp. 1–11 (2010)
18. Solovay, R.M., Arthan, R., Harrison, J.: Some new results on decidability for elementary algebra and geometry. ArXiV preprint 0904.3482. Submitted to Ann. Pure Appl. Logic. Available at http://arxiv.org/abs/0904.3482 (2009)
19. Sussmann, H.J.: Multidifferential calculus: chain rule, open mapping and transversal intersection theorems. In: Hager, W.W., Pardalos, P.M. (eds.) Optimal Control: Theory, Algorithms, and Applications, pp. 436–487. Kluwer (1998)
20. Webster, R.: Convexity. Oxford University Press (1995)
21. Wiedijk, F.: Statistics on digital libraries of mathematics. In: Grabowski, A., Naumowicz, A. (eds.) Computer Reconstruction of the Body of Mathematics. Studies in Logic, Grammar and Rhetoric, vol. 18(31). University of Białystok (2009)
22. Yee, L.-P., Výborný, R.: The Integral: An Easy Approach After Kurzweil and Henstock. Australian Mathematical Society Lecture Series. Cambridge University Press (2000)