Formalizing Basic Complex Analysis

Dedicated to Andrzej Trybulec on the occasion of his 65th birthday

John Harrison

Intel Corporation, JF1-13
2111 NE 25th Avenue, Hillsboro OR 97124, USA
johnh@ichips.intel.com

Abstract. We describe the formalization of some of the basics of complex analysis in the HOL Light theorem prover. Besides being a beautiful area of mathematics, this has many potential applications, e.g. in analytic number theory. We have endeavoured to set up the kind of general analytic machinery that would make such applications feasible.

0 Mizar and me: some personal recollections

The first time I saw mention of the Mizar project was in a message from Bob Boyer to the QED mailing list in August 1993:[1]

> Indeed, there have been a good number of QED-like efforts spread over at least the last 27 years, both large scale and small. (I hear rumors that the Polish MIZAR effort may be the largest so far.)

At the time, even though Mizar had a large and thriving user community all over the world, I hadn't heard of it at all, so my curiosity was piqued. The following summer, the second QED Workshop was in Warsaw, and I had the opportunity to meet Andrzej Trybulec in person for the first time. This was a memorable experience in many ways, and immediately after the workshop a few participants travelled to Białystok where we had the opportunity to try out Mizar for ourselves with Andrzej's help.

I was impressed that Andrzej was willing to devote so much time to helping out some complete beginners. But I was equally impressed how little his help was needed! After a few hours, I was able to prove in Mizar the formula for the roots of a quadratic equation. To someone with no experience of proof assistants, that might seem an unspectacular accomplishment, but Mizar seemed to be dramatically easier to use than the other systems I'd tried, particularly HOL [3], with which I was most familiar.

Over the next few months, back in Cambridge (where I was supposed to be finishing my PhD) and in Turku/Åbo in Finland (where I was doing a postdoc under

[1] http://icml.stanford.edu/~uribe/mail/qed.messages/105.html

ISBN 978-83-7431-128-1 ISSN 0860–150X

the EU Human Capital and Mobility scheme), I often thought about why Mizar's proof language seemed much easier to use. I became convinced that Andrzej's design had many key features that we should emulate in other systems, and at the TPHOLs conference in 1996, I presented a paper [4] where I described a simple 'clone' of some features of the Mizar proof language built on top of my own HOL Light prover. During the discussion after my talk, Mike Gordon (the original inventor of HOL) coined the word *declarative* to describe the Mizar approach to proof, in contrast to the *procedural* approach of HOL and most other systems. Those terms, based on a natural analogy with declarative and procedural programming languages, seem to be very appropriate and have stuck.

Before I had even finished coding my 'Mizar Mode for HOL', Don Syme had attended a half-baked talk I gave on the subject in Cambridge and been inspired to write his own declarative prover. Many of the ideas about proof style that Don and I discussed found shape in a paper I gave at the TYPES meeting in Aussois in 1996 [5]. And next year, declarative proof had become a hot topic, with three papers by different people at the same conference [13, 14, 17].

Ironically, though I acted as a channel for Mizar's ideas, I have been little occupied with declarative over the subsequent decade. The most impressive line of work derived from Mizar is Markus Wenzel's "Isar" mode for the Isabelle prover [12]. This has even become Isabelle's default mode in place of the traditional ML tactic scripts, and the structured proof language seems to have contributed to a much wider usage of the Isabelle system. I have mostly continued to do proofs in the good old procedural way in HOL Light. This is partly inertia, but also partly a recognition that this approach has its advantages too. (Just as, for example, point-and-click interfaces and command lines have their place.) Perhaps the ultimate dream is a smooth combination of both procedural and declarative approaches [16].

As he approaches his 65th birthday, I hope Andrzej gains the deserved satisfaction from seeing his ideas spread not just through the user community of Mizar itself, but through the world of proof assistants generally. So far, the intellectual influence has mainly concerned the logical structure of the proof language, but I would not be surprised if other ideas from Mizar, such as its treatment of algebraic structures, begin to propagate into other systems. I would have liked to talk about some of these questions, but I lack the competence to do so. Instead, I draw inspiration from another of Andrzej's notable characteristics: while many people talk and dream about the formalization of mathematics, he and his colleagues really do it. In the same spirit, I want to describe some work I have done on the formalization of complex analysis using my HOL Light prover.

1 Topological and analytical basics

Instead of defining a special type of complex numbers, we use the type $\mathbb{R}^2$ directly, though we define `complex` as an accepted abbreviation for this type. In this way we instantly inherit all the topological and analytic apparatus described in [8], without needing explicit isomorphisms from one type to the other. Nevertheless, we add various special things for the complex numbers, e.g. the mappings `Re` and

`Im` for the real and imaginary components of a complex number, the conjugation mapping `cnj`, and multiplication and inversion of complex numbers. We have tried to keep notation compatible with an earlier theory [7]. Readers unfamiliar with a simple type system such as HOL will need to get used to seeing various type injections such as `&` : $\mathbb{N} \to \mathbb{R}$ and `Cx` : $\mathbb{R} \to \mathbb{C}$. Also, although the types $\mathbb{R}^2$ and $\mathbb{C}$ are synonymous, the types $\mathbb{R}$ and $\mathbb{R}^1$ are not, so we use bijections `lift` : $\mathbb{R} \to \mathbb{R}^1$ and `drop` : $\mathbb{R}^1 \to \mathbb{R}$.

More interestingly, we also define the key concept of complex differentiability. The general notion of differentiability for a function $\mathbb{R}^M \to \mathbb{R}^N$ is that there is a local linear approximation, which is also a function $\mathbb{R}^M \to \mathbb{R}^N$, e.g. for a simple limit at a point:

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

As discussed in [6], we formalize many such concepts in this relational style. For example, when proving things about limits we generally focus on assertions of the form $x_n \to a$ rather than the informal equivalent $\lim x_n = a$. In the HOL formalization these are not equivalent: $x_n \to a$ implies $\lim x_n = a$ but not conversely. The trouble is that because the limit function lim has some specific type, say $(\mathbb{N} \to \mathbb{R}^N) \to \mathbb{R}^N$, there is no way of encoding whether or not the limit exists; whether it does or not there will be *some* object $\lim x_n$ of type $\mathbb{R}^N$ and the equation $\lim x_n = a$ does not furnish any information about whether it's a "real" limit or just some other arbitrary value. (This problem is less severe in untyped frameworks or those with more flexible types like Mizar, since one can use subtyping to indicate definedness, e.g. setting lim to return something not in $\mathbb{R}^N$ when there is no limit.) Therefore, we quite consistently formalize limiting concepts in the relational fashion, as with complex differentiability and path integrability below.

Compared with general differentiability in $\mathbb{R}^N$, complex differentiability makes the more stringent assumption that the linear mapping just amounts to multiplication by a complex number:

```
|- (f has_complex_derivative f') net ⇔
       (f has_derivative (λx. f' * x)) net
```

It is easy to prove this equivalent to another natural characterization:

```
|- (f has_complex_derivative f') (at a) ⇔
     ((λx. (f(x) - f(a)) / (x - a)) --> f') (at a)
```

Equally, one can derive the Cauchy-Riemann characterization (though we have had no use for it so far):

```
|- f complex_differentiable (at z) ⇔
       f differentiable (at z) ∧
       jacobian f (at z)$1$1 = jacobian f (at z)$2$2 ∧
       jacobian f (at z)$1$2 = --(jacobian f (at z)$2$1)
```

where:

```
|- f complex_differentiable net ⇔
     ∃f'. (f has_complex_derivative f') net
```

We also define complex differentiability throughout a set. We use a restricted notion of limit considering points inside the set only. This is more in line with the general approach to limits within subspaces in topology, and in any case the distinction disappears when, as is usually done, we consider open sets. However, it is important to keep this in mind, since often analyticity on a set is taken to imply analyticity in an open set around each point. (Our motivation in taking the chosen course is that in the past we sometimes found it tedious handling such things as 1-sided limits at the endpoints of intervals with a separate argument.)

```
|- f analytic_on s ⇔
   ∀x. x ∈ s ⇒ ∃f'. (f has_complex_derivative f') (at x within s)
```

The usual theorems about composing limits and derivatives extend easily from general differentiability to this special case. Properties of complex multiplication are derived from general properties of bilinear mappings, though the complex inverse uses a more explicit and tedious argument. (Could this be avoided?)

We also define complex versions of the usual transcendental functions (starting with the Taylor expansion for the exponential function) and derive real versions from them. These are not much used in the first part of this development, but we do need the complex exponential function and its periodicity when we later come to talk about winding numbers. Note that HOL Light already has a theory of real analysis [6], but our long-term goal is to subsume it under this more general analytical theory in $\mathbb{R}^N$ and $\mathbb{C}$.

2 Paths

Cauchy's theorem and related results depend on integration of a complex function over a path (sometimes known as a line, road, curve or contour). A path is considered to be a mapping $\gamma : [0,1] \to \mathbb{C}$ out of some canonical real interval, and the path integral is then defined as

$$\int_\gamma f = \int_0^1 f(\gamma(t))\gamma'(t)\ dt$$

or in our HOL relational formulation:

```
|- (f has_path_integral i) g ⇔
   ((λx. f(g x) * vector_derivative g (at x)) has_integral i)
   (interval[vec 0,vec 1])
```

For most purposes, we want to forget the details of the parametrization using the arbitrary interval $[0,1]$, so we define various natural abbreviations:

```
|- pathstart g = g(vec 0)

|- pathfinish g = g vec 1)

|- closed_path g ⇔ pathstart g = pathfinish g

|- path_image g = IMAGE g (interval[vec 0,vec 1])
```

It's often convenient to stick together two new paths to make a new path. To retain the canonical parametrization we allocate the two intervals $[0, 1/2]$ and $[1/2, 1]$ to scaled versions of the the two components; formally:

```
|- g1 ++ g2 = (λx. if drop x <= &1 / &2
                  then g1(&2 % x)
                  else g2(&2 % x - vec 1))
```

where `vec` is a direct injection $\mathbb{N} \to \mathbb{R}^1$ and the infix operator '`%`' is scalar-vector multiplication. (We could have written '`Cx(&2) * x`' but the present definition is valid for any $\mathbb{R}^N$ as well as $\mathbb{C}$.) Similarly we often want to consider a path in reverse:

```
|- reversepath g = (λx. g(vec 1 - x))
```

For a path integral as defined above to exist, some restrictions on the functions allowed as paths are needed. The functions f we are concerned with are normally well-behaved, certainly continuous and usually analytic, so it is the nature of γ that is critical. The usual assumption in complex analysis texts is that a path γ should be piecewise continuously differentiable, which ensures that the path integral exists at least for any continuous f, since all piecewise continuous functions are integrable. However, our notion of validity is weaker, just piecewise differentiability:

```
|- valid_path f ⇔ f piecewise_differentiable_on interval[vec 0,vec 1]
```

where piecewise differentiability is continuity plus differentiability except on a finite set:

```
|- f piecewise_differentiable_on i ⇔
       f continuous_on i ∧
       (∃s. FINITE s ∧ (∀x. x ∈ i DIFF s ⇒ f differentiable at x))
```

This choice is influenced by the fact that our underlying theory of integration is the Kurzweil-Henstock theory [9, 10]. In contrast to the Riemann or Lebesgue theory (but in common with a simple notion based on antiderivatives), this can integrate all derivatives. Using the Riemann or Lebesgue theory we would be unable even to integrate a constant function along an exotic non-rectifiable path like $\gamma(t) = t + t^2 \sin(1/t^3)$, which is differentiable everywhere but with unbounded variation in a neighbourhood of 0, and so we could prove little of interest about general paths. With our integration theory, it is only when we need to consider bounds on integrals that we may need to impose stronger restrictions.

Of course, it is easy to establish various basic results about our combinators for paths, such as the following. Once these have been proved (often quite laborious, though intellectual trivial), one does not often have to return to the basic definition of path integral.

```
|- reversepath(reversepath g) = g

|- pathstart(reversepath g) = pathfinish g

|- valid_path(reversepath g) ⇔ valid_path g

|- pathfinish g1 = pathstart g2
   ⇒ (valid_path (g1 ++ g2) ⇔
       valid_path g1 ∧ valid_path g2)

|- (f has_path_integral i1) g1 ∧
   (f has_path_integral i2) g2 ∧
   valid_path g1 ∧ valid_path g2
   ⇒ (f has_path_integral (i1 + i2)) (g1 ++ g2)
```

Two particularly common paths that we use in what follows are a straight-line path from a to b:

```
|- linepath(a,b) = λx. (&1 - drop x) % a + drop x % b
```

and a circular path, traversed counterclockwise, with centre z and radius r (here `ii` denotes the imaginary unit i):

```
|- circlepath(z,r) = λx. z + Cx(r) * cexp(Cx(&2) * Cx pi * ii * Cx(drop x))
```

where `cexp` is the complex exponential function.

3 Cauchy's theorem

The cornerstone of the usual approach to complex analysis is the Cauchy-Goursat integral theorem, although there are ingenious approaches that avoid integration [15]. Our first step is a straightforward corollary combining the 1-dimensional Fundamental Theorem of Calculus and the general chain rule for composition of derivatives:

```
|- (∀x. x ∈ s ⇒ (f has_complex_derivative f'(x)) (at x within s)) ∧
   valid_path g ∧ (path_image g) SUBSET s
   ⇒ (f' has_path_integral (f(pathfinish g) - f(pathstart g))) g
```

This shows that if a function has a primitive (usual terminology for a complex antiderivative) within a set, the integral round any closed curve in that set is zero. Note that as when defining analyticity, we carefully consider limits within the set s, so this is a little sharper than the most common variant where the set s is assumed open.

```
|- (∀x. x ∈ s ⇒ (f has_complex_derivative f'(x)) (at x within s)) ∧
   valid_path g ∧ (path_image g) SUBSET s ∧
   pathfinish g = pathstart g
   ⇒ (f' has_path_integral Cx(&0)) g
```

In order to make progress, we need to establish the existence of line integrals for a more general class of functions. However, we only need to consider integrals along straight-line segments, and in this case the integrability of continuous functions follows from an analogous result for the reals:

```
|- f continuous_on segment(a,b) ⇒ f path_integrable_on (linepath(a,b))
```

Our goal is now to prove the Cauchy-Goursat theorem, which states that if a function is analytic in a set with suitable topological properties, its line integral round any closed path in that set is zero. For the time being, we just aim to prove this for a triangular path, on and inside which the function is analytic. The key argument is a quadrisection step, showing that if the integral were $\geq eK^2$ where K is a bound on the sides, then one of the four triangles obtained by joining all pairs of midpoints would have the same property, and the corresponding K would be halved. Note that we use the notion of convex hull as an easy way of talking about the inside and outside of the triangle.

```
|- f continuous_on (convex hull a,b,c) ∧
   dist (a,b) <= K ∧
   dist (b,c) <= K ∧
   dist (c,a) <= K ∧
   norm(path_integral(linepath(a,b)) f +
        path_integral(linepath(b,c)) f +
        path_integral(linepath(c,a)) f) >= e * K pow 2
   ⇒ ∃a' b' c'. a' ∈ convex hull a,b,c ∧
                b' ∈ convex hull a,b,c ∧
                c' ∈ convex hull a,b,c ∧
                dist(a',b') <= K / &2 ∧
                dist(b',c') <= K / &2 ∧
                dist(c',a') <= K / &2 ∧
                norm(path_integral(linepath(a',b')) f +
                     path_integral(linepath(b',c')) f +
                     path_integral(linepath(c',a')) f)
                 >= e * (K / &2) pow 2
```

This means that if the path integral round a triangle is nonzero, we could generate a decreasing nest of triangles, which by completeness must all contain a common point. (It is easy to see that there is exactly one.) But then from complex differentiability at that point, we obtain the following upper bound on the integral:

```
|- x ∈ s ∧ f continuous_on s ∧
   f complex_differentiable (at x within s) ∧
   &0 < e
   ⇒ ∃k. &0 < k ∧
         ∀a b c. dist(a,b) <= k ∧ dist(b,c) <= k ∧ dist(c,a) <= k ∧
                 x ∈ convex hull a,b,c ∧ convex hull a,b,c SUBSET s
                 ⇒ norm(path_integral(linepath(a,b)) f +
                        path_integral(linepath(b,c)) f +
                        path_integral(linepath(c,a)) f)
                   <= e * (dist(a,b) + dist(b,c) + dist(c,a)) pow 2
```

and for sufficiently small triangles, this is a contradiction, so we obtain our first version of Cauchy's theorem. We use the notion of integration on a 'chain', which is just a list of paths. We could express this directly using the path-combining operator '**++**', but this proof was designed before we introduced that combinator. It is a trivial corollary that the integral is zero round a closed path (a singleton chain).

```
|- f analytic_on (convex hull a,b,c)
   ⇒ (f has_chain_integral Cx(&0))
       [linepath (a,b); linepath(b,c); linepath(c,a)]
```

Before proceeding to more general regions, we generalize this in two directions. First, by a simple but slightly laborious limiting argument, we can see that the assumption of analyticity can be weakened to continuity on the boundary:

```
|- f continuous_on (convex hull a,b,c) ∧
   f analytic_on interior (convex hull a,b,c)
   ⇒ (f has_chain_integral Cx(&0))
       [linepath (a,b); linepath(b,c); linepath(c,a)]
```

and then we can permit a finite number of exceptional points inside, using a process of trisection at those points:

```
|- f continuous_on (convex hull a,b,c) ∧
   FINITE s ∧
   (∀x. x ∈ interior(convex hull a,b,c) DIFF s
        ⇒ f complex_differentiable (at x))
   ⇒ (f has_chain_integral Cx(&0))
       [linepath (a,b); linepath(b,c); linepath(c,a)]
```

We will eventually be able to show that in such a case the function is differentiable at these interior points anyway, but the weak hypothesis is useful to develop the machinery that will allow us to reach this result.

Now, given any convex set with f analytic on the interior except at a finite number of points, we can fix a point a of the set and define a function $g(x)$ by the line integral of f along $\mathrm{linepath}(a, x)$. Cauchy's theorem for a triangle is exactly what we need to show that this is a primitive for f, i.e. $g'(x) = f(x)$. For we have

$$g(x+h) - g(x) = \int_{\mathrm{linepath}(a,x+h)} f - \int_{\mathrm{linepath}(a,x)} f = \int_{\mathrm{linepath}(x,x+h)} f$$

and letting $h \to 0$ we see $(g(x+h) - g(x))/h \to f(x)$. So we can conclude that if a function is analytic at almost all interior points of a convex set, it has a primitive there:

```
|- convex s ∧ FINITE k ∧ f continuous_on s ∧
   (∀x. x ∈ interior(s) DIFF k ⇒ f complex_differentiable at x)
   ⇒ ∃g. ∀x. x ∈ s
             ⇒ (g has_complex_derivative f(x)) (at x within s)
```

Combining this with the first result for line integrals of a function with a primitive, we obtain our main version of Cauchy's theorem:

```
|- convex s ∧ FINITE k ∧ f continuous_on s ∧
   (∀x. x ∈ interior(s) DIFF k ⇒ f complex_differentiable at x) ∧
   valid_path g ∧ (path_image g) SUBSET s ∧
   pathfinish g = pathstart g
   ⇒ (f has_path_integral Cx(&0)) g
```

We can prove this under the slightly weaker assumption that the set is starlike, i.e. there is some point a such that for any x in the set, the line segment from a to x lies entirely in the set. However in that case we do seem to need the traditional hypothesis of openness. In any case, though this is far from the most topologically general version of Cauchy's theorem, it is enough to deduce many interesting and non-trivial results.

4 Winding numbers

So far, we haven't described results guaranteeing the existence of path integrals for a general path unless the function has a primitive throughout the path. (Of course, we can get results for the special case of paths that are continuously differentiable.) However, by chopping up the path sufficiently, it's easy to generalize this to require the existence only of a local primitive in a small neighbourhood of each point:

```
|- (∀x. x ∈ s
       ⇒ ∃d h. &0 < d ∧
                 ∀y. norm(y - x) < d
                     ⇒ (h has_complex_derivative f(y)) (at y within s)) ∧
   valid_path g ∧ (path_image g) SUBSET s
   ⇒ f path_integrable_on g
```

Thanks to our 'local' version of Cauchy's theorem, this implies that path integrals of analytic functions always exist:

```
|- open s ∧ f analytic_on s ∧ valid_path g ∧ path_image g SUBSET s
   ⇒ f path_integrable_on g
```

In particular, we can define the winding number by the usual integral $W(\gamma, z) = \frac{1}{2\pi i}\int_\gamma dw/(w-z)$, and deduce that this is welldefined provided z is not on the path γ:

```
|- valid_path g ∧ ¬(z ∈ path_image g)
   ⇒ ((λw. Cx(&1) / (w - z)) has_path_integral
        (Cx(&2) * Cx(pi) * ii * winding_number(g,z))) g
```

It follows immediately from our simple Cauchy theorem that if a path γ is inside a convex set, the winding number is zero about all points outside the set, because in that case $1/(w-z)$ is analytic throughout:

```
|- valid_path g ∧ convex s ∧ pathfinish g = pathstart g ∧
   ¬(z ∈ s) ∧ path_image g SUBSET s
   ⇒ winding_number(g,z) = Cx(&0)
```

and so in particular this means that the winding number must be zero for sufficiently large z:

```
|- valid_path g ∧ pathfinish g = pathstart g
   ⇒ ∃B. ∀z. B <= norm(z) ⇒ winding_number(g,z) = Cx(&0)
```

It is usual to consider the notion of winding number only in the case of closed paths. However, the definition does not preclude applying it to general paths, and we find this potentially useful. For example, we might want to compute winding numbers for composite paths using additivity:

```
|- valid_path g1 ∧ valid_path g2 ∧
   ¬(z ∈ path_image g1) ∧ ¬(z ∈ path_image g2)
   ⇒ winding_number(g1 ++ g2,z) =
      winding_number(g1,z) + winding_number(g2,z)
```

Of course, it is important to know that the winding number for a closed path is always an integer. The proof we use, apparently due to Ahlfors, is based on the observation that

$$e^{-\int_a^b \gamma'(t)/(\gamma(t)-z)\ dt}(\gamma(b)-z) = \gamma(a)-z$$

or in our formalization:

```
|- g piecewise_differentiable_on interval[a,b] ∧
   drop a <= drop b ∧ (∀x. x ∈ interval[a,b] ⇒ ¬(g x = z))
   ⇒  (λx. vector_derivative g (at x) / (g(x) - z))
      integrable_on interval[a,b] ∧
      cexp(--(integral (interval[a,b])
                       (λx. vector_derivative g (at x) / (g(x) - z)))) *
      (g(b) - z) = g(a) - z
```

The proof is fairly straightforward, although it needs some care because of the generality of our paths. At all points where γ is differentiable, the derivative of the expression $e^{-\int_a^y \gamma'(t)/(\gamma(t)-z)\ dt}(\gamma(y)-z)$ with respect to y is zero, using the Fundamental Theorem of Calculus. And at *all* points this is continuous as a function of y (the Kurzweil-Henstock integral in one dimension is always a continuous function of its upper limit whenever the integral exists). Therefore it is constant on the interval $[a,b]$ and so the values at a and b are equal; since $e^{-\int_a^a \gamma'(t)/(\gamma(t)-z)\ dt}(\gamma(a)-z) = e^0(\gamma(a)-z) = \gamma(a)-z$ the result follows. From this lemma, we can deduce as usual that if the path is closed, i.e. $\gamma(b)=\gamma(a)$, we must have $e^{-\int_a^b \gamma'(t)/(\gamma(t)-z)\ dt} = 1$, so $\int_a^b \gamma'(t)/(\gamma(t)-z)\ dt$ is a multiple of $2\pi i$ and thus the winding number is an integer. In fact, this equivalence works equally well in either direction: the winding number is an integer *if and only if* the path is closed:

```
|- valid_path g ∧ ¬(z ∈ path_image g)
   ⇒ (complex_integer(winding_number(g,z)) ⇔
       pathfinish g = pathstart g)
```

In what follows, we will often want to consider integrals round simple circular paths. It follows immediately from results above that the winding number is zero for points outside the circle. To show that it is 1 for points inside, the most satisfactory approach might be to prove it is clearly positive by considering the integrand, and must be at most 1 because the path is a *simple* curve. However, we haven't actually proved that the winding number cannot exceed 1 in magnitude for a simple closed curve, so we use a more direct approach. Explicit evaluation of the integral easily yields the winding number for a circle about the centre:

```
|- ¬(r = &0) ⇒ winding_number(circlepath(z,r),z) = Cx(&1)
```

Also, the winding number is a continuous function of the point, assuming it is off the curve. This could be proved for general paths, except that since we need to bound the integral, we may finally need to make a stronger assumption about our paths than piecewise differentiability. We just proved it for circles:

```
|- &0 < r ∧ ¬(norm(w - z) = r)
   ⇒ (λw. winding_number(circlepath(z,r),w)) continuous (at w)
```

Since the winding number is an integer, it must therefore be constant on connected components:

```
|- connected s ∧ (s INTER path_image (circlepath(z,r)) = ) ∧
   &0 < r ∧ w1 ∈ s ∧ w2 ∈ s
   ⇒ winding_number(circlepath(z,r),w1) =
       winding_number(circlepath(z,r),w2)
```

and so we deduce as we wanted:

```
|- norm(w - z) < r ⇒ winding_number(circlepath(z,r),w) = Cx(&1)
```

5 Cauchy's integral theorem

We deduce Cauchy's integral formula for a convex set by applying Cauchy's theorem to the function

$$g(w) = \begin{cases} \frac{f(w)-f(z)}{w-z} & \text{if } w \neq z \\ f'(z) & \text{if } w = z \end{cases}$$

Note that here it is useful to be able to assume only that g is *continuous* at z, while being analytic everywhere else. On the other hand, this result can eventually be used to deduce that in such a case the function is in fact differentiable at z anyway. (We have not actually proved such results about removable singularities yet, but this would be one natural next step.)

```
|- convex s ∧ FINITE k ∧ f continuous_on s ∧
   (∀x. x ∈ interior(s) DIFF k ⇒ f complex_differentiable at x) ∧
   z ∈ interior(s) DIFF k ∧
   valid_path g ∧ (path_image g) SUBSET (s DELETE z) ∧
   pathfinish g = pathstart g
   ⇒ ((λw. f(w) / (w - z)) has_path_integral
        (Cx(&2) * Cx(pi) * ii * winding_number(g,z) * f(z))) g
```

For a circular path and an analytic function, we have the simple instance:

```
|- convex s ∧ f analytic_on s ∧ z ∈ interior s ∧ &0 < r ∧
   path_image (circlepath(z,r)) SUBSET s
   ⇒ ((λw. f(w) / (w - z)) has_path_integral
        (Cx(&2) * Cx(pi) * ii * f(z))) (circlepath(z,r))
```

Even this is already enough to deduce a weak version of Liouville's theorem, that an entire function that tends to zero for all sufficiently large values of the argument must be zero everywhere. This is already enough to obtain an easy proof of the Fundamental Theorem of Algebra, by applying it to the inverse of a polynomial without a zero, though this is something which has already been proved by the more direct 'minimum modulus' proof [7].

```
|- f analytic_on (:complex) ∧ (f --> Cx(&0)) at_infinity
   ⇒ ∀z. f(z) = Cx(&0)
```

However, most further results depend on formulas for derivatives in terms of path integrals. The basic lemma that allows us to pass from an expression for values of a function g as an integral to a similar expression for its derivative g' is as follows. Note that we have two a priori different functions g and f, one defined in terms of a path integral of the other; this extra generality makes this quite a flexible lemma. (Here `pow` is the power function $\mathbb{C} \to \mathbb{N} \to \mathbb{C}$.)

```
|- ¬(k = 0) ∧
   (f continuous_on path_image(circlepath(z,r))) ∧
   (∀w. w ∈ ball(z,r)
        ⇒ ((λu. f(u) / (u - w) pow k) has_path_integral g w)
          (circlepath(z,r)))
   ⇒ ∀w. w ∈ ball(z,r)
         ⇒ (λu. f(u) / (u - w) pow (k + 1)) path_integrable_on
                   (circlepath(z,r)) ∧
             (g has_complex_derivative
              (Cx(&k) * path_integral(circlepath(z,r))
                        (λu. f(u) / (u - w) pow (k + 1))))
             (at w)
```

In particular, setting $k = 1$ and f and g to be the same, we obtain a formula for the first derivative:

```
|- f continuous_on cball(z,r) ∧
   f analytic_on ball(z,r) ∧
   w ∈ ball(z,r)
   ⇒ (λu. f(u) / (u - w) pow 2) path_integrable_on circlepath(z,r) ∧
       (f has_complex_derivative
           (Cx(&1) / (Cx(&2) * Cx(pi) * ii) *
            path_integral(circlepath(z,r)) (λu. f(u) / (u - w) pow 2)))
       (at w)
```

6 Consequences of the integral formula

Our versions of Cauchy's theorem and Cauchy's integral formula are restricted to convex sets. However, even this special case allows us to prove some significant consequences. First of all, the derivative formula immediately yields the existence of higher derivatives on an open set, since we can integrate round a sufficiently small circle:

```
|- open s ∧ f analytic_on s
   ⇒ (complex_derivative f) analytic_on s
```

Also, we easily obtain the full version of Liouville's theorem, because the integral $\int_\gamma f(w)/(w-z)^2\ dw$ must tend to zero as the size of the circle increases if f is bounded.

```
|- f analytic_on (:complex) ∧ bounded (IMAGE f (:complex))
   ⇒ ∃c. ∀z. f(z) = c
```

A slightly more involved application is Weierstrass's convergence theorem: if a sequence of analytic functions (f_n) with derivatives (f'_n) tends uniformly to a limit f, then the limit is also analytic and $f'_n \to f'$. Note that an analogous result fails for differentiability of a function $\mathbb{R}^M \to \mathbb{R}^N$ even for $M = N = 1$, where the series of

derivatives may not even converge. (For example, by the Weierstrass approximation theorem, every continuous function, not necessarily differentiable anywhere, is a uniform limit of analytic functions, viz. polynomials.) In our context, however, it is easy to see that the integral formulas defining higher derivatives converge, and we can conclude:

```
|- open s ∧
   (∀n x. x ∈ s ⇒ ((f n) has_complex_derivative f' n x) (at x)) ∧
   (∀x. x ∈ s
        ⇒ ∃d. &0 < d ∧ cball(x,d) SUBSET s ∧
                ∀e. &0 < e
                    ⇒ eventually (λn. ∀y. y ∈ cball(x,d)
                                          ⇒ norm(f n y - g y) < e)
                                 sequentially)
   ⇒ ∃g'. ∀x. x ∈ s ⇒ (g has_complex_derivative g'(x)) (at x) ∧
                       ((λn. f' n x) --> g'(x)) sequentially
```

This allows us to prove the following, which is a convenient 'one-stop-shop' for defining an analytic function in terms of a series (including but not limited to power series). If the sequence of functions (f_n) are all analytic on a set s with derivatives f'_n, and $|f_n(x)|$ is bounded on s by a summable real series h, then we can conclude that the series (f_n) converges to a function g and (f'_n) converges to its derivative, throughout f. (The set k restricts the terms of the infinite sum, e.g. to allow us to sum just from 1, only for even n or only for prime p.)

```
|- open s ∧
   (∀n x. n ∈ k ∧ x ∈ s ⇒ (f n has_complex_derivative f' n x) (at x)) ∧
   (∃l. (lift o h sums l) k) ∧
   (∃N. ∀n x. N <= n ∧ n ∈ k ∧ x ∈ s ⇒ norm(f n x) <= h n)
        ⇒ ∃g g'. ∀x. x ∈ s
                     ⇒ ((λn. f n x) sums g x) k ∧
                       ((λn. f' n x) sums g' x) k ∧
                       (g has_complex_derivative g' x) (at x)
```

7 Conclusions and future work

Generally, the sequence of results here have been developed without much difficulty, more or less following the usual informal plan. However, they rest on some other theories that were occasionally quite hard work to formalize. For example, even an *affine* change-of-variables theorem for the Kurzweil-Henstock integral (admittedly for integrals on $\mathbb{R}^N$ not just $\mathbb{R}^1$) was quite hard work to formalize, despite the straightforward underlying intuition that all the concepts like interval, partition, gauge and so on scale in an obvious way. We also found it very convenient to have a good library of results about convex sets to rely on, but it was occasionally remarkable how much work it was to prove complete trivialities. One amusing (or depressing) example is the following, which actually took many dozens of lines to prove!

```
|- ¬(a ∈ interior(convex hull a,b,c))
```

We have found it very convenient that HOL Light's programmability lets us set up quite powerful automated proof procedures for special tasks, e.g. a `COMPLEX_FIELD` rule for simple algebraic manipulations like the following, which would also be tedious by hand:

```
|- ¬(x = u) ∧ ¬(x = w)
   ⇒ Cx(&1) / (x - u) - Cx(&1) / (x - w) =
       (u - w) / ((x - u) * (x - w))
```

The most annoying gap in HOL Light's automation concerns 'triangle law' reasoning, which crops up all the time. We ended up proving a lot of trivial lemmas like the following:

```
|- abs(norm(w - z) - r) = d ∧
   norm(u - w) < d / &2 ∧
   norm(x - z) = r
   ⇒ d / &2 <= norm(x - u)
```

Thanks to a vector-space quantifier elimination procedure due to Bob Solovay [8], we can in principle prove such results automatically. In practice, using this method is not a complete answer because even linear problems like the above give rise to nonlinear problems over the reals, which though decidable are often quite slow. Recently we have observed that almost all the triangle law reasoning we use relies only on the basic norm properties and nothing specific to the Euclidean norm $|x| = \sqrt{x \cdot x}$. Using this fact, a more efficient decision procedure is possible, and it would have saved us some work if we'd come up with this sooner.

We have only scratched the surface of the extensive and beautiful theory of complex functions, and there are many future avenues to explore. One obvious idea would be to generalize Cauchy's theorem to simply connected regions and beyond, perhaps to a global version stated in terms of homotopy or homology of paths. Dixon's proof of the global Cauchy theorem [11] should be relatively easy to prove using the existing machinery.

Another interesting idea is to seek applications to other areas of mathematics. One notable possibility would be a proof of the Prime Number Theorem based on the usual complex-analytic machinery and the nonvanishing of the Riemann zeta function $\zeta(s)$ for $Re(s) \geq 1$. The "elementary" Erdös-Selberg proof has already been formalized [1], but Solovay has suggested the usual analytical proof as a significant challenge for formal verification. We hope to take up this challenge in a future paper.

References

1. J. Avigad, K. Donnelly, D. Gray, and P. Raff. A formally verified proof of the prime number theorem. To appear in the ACM Transactions on Computational Logic, 2006.
2. Y. Bertot, G. Dowek, A. Hirschowitz, C. Paulin, and L. Théry, editors. *Theorem Proving in Higher Order Logics: 12th International Conference, TPHOLs'99*, volume 1690 of *Lecture Notes in Computer Science*, Nice, France, 1999. Springer-Verlag.
3. M. J. C. Gordon and T. F. Melham. *Introduction to HOL: a theorem proving environment for higher order logic*. Cambridge University Press, 1993.
4. J. Harrison. A Mizar mode for HOL. In J. v. Wright, J. Grundy, and J. Harrison, editors, *Theorem Proving in Higher Order Logics: 9th International Conference, TPHOLs'96*, volume 1125 of *Lecture Notes in Computer Science*, pages 203–220, Turku, Finland, 1996. Springer-Verlag.

5. J. Harrison. Proof style. In E. Giménez and C. Paulin-Mohring, editors, *Types for Proofs and Programs: International Workshop TYPES'96*, volume 1512 of *Lecture Notes in Computer Science*, pages 154–172, Aussois, France, 1996. Springer-Verlag.
6. J. Harrison. *Theorem Proving with the Real Numbers*. Springer-Verlag, 1998. Revised version of author's PhD thesis.
7. J. Harrison. Complex quantifier elimination in HOL. In R. J. Boulton and P. B. Jackson, editors, *TPHOLs 2001: Supplemental Proceedings*, pages 159–174. Division of Informatics, University of Edinburgh, 2001. Published as Informatics Report Series EDI-INF-RR-0046. Available on the Web at `http://www.informatics.ed.ac.uk/publications/report/0046.html`.
8. J. Harrison. A HOL theory of Euclidean space. In J. Hurd and T. Melham, editors, *Theorem Proving in Higher Order Logics, 18th International Conference, TPHOLs 2005*, volume 3603 of *Lecture Notes in Computer Science*, pages 114–129, Oxford, UK, 2005. Springer-Verlag.
9. R. Henstock. A Riemann-type integral of Lebesgue power. *Canadian Journal of Mathematics*, 20:79–87, 1968.
10. J. Kurzweil. Generalized ordinary differential equations and continuous dependence on a parameter. *Czechoslovak Mathematics Journal*, 82:418–446, 1958.
11. S. Lang. *Complex Analysis*. Graduate Texts in Mathematics. Springer-Verlag, 3rd edition, 1993.
12. T. Nipkow, L. C. Paulson, and M. Wenzel. *Isabelle/HOL — A Proof Assistant for Higher-Order Logic*, volume 2283 of *Lecture Notes in Computer Science*. Springer-Verlag, 2002.
13. D. Syme. DECLARE: A prototype declarative proof system for higher order logic. Technical Report 416, University of Cambridge Computer Laboratory, New Museums Site, Pembroke Street, Cambridge, CB2 3QG, UK, 1997.
14. M. Wenzel. Isar - a generic interpretive approach to readable formal proof documents. In Bertot et al. [2], pages 167–183.
15. G. T. Whyburn. *Topological Analysis*, volume 23 of *Princeton Mathematical Series*. Princeton University Press, revised edition, 1964.
16. F. Wiedijk. Mizar light for HOL Light. In R. J. Boulton and P. B. Jackson, editors, *14th International Conference on Theorem Proving in Higher Order Logics: TPHOLs 2001*, volume 2152 of *Lecture Notes in Computer Science*, pages 378–394. Springer-Verlag, 2001.
17. V. Zammit. On the implementation of an extensible declarative proof language. In Bertot et al. [2], pages 185–202.