A certified proof of a theorem of Cartan

Gianni Ciolli   Graziano Gentili   Marco Maggesi

March 5, 2008

Abstract

In the present paper we present a machine-certified proof for a theorem of Cartan, using the HOL Light theorem prover by John Harrison.

1 Introduction

Teorema 1 (Cartan). *Let* $D = D(z_0, r) = \{z \in \mathbb{C} \mid |z - z_0| < r\}$, *and let* $f : D \to D$ *be holomorphic. Assume that* $f(z_0) = z_0$ *and* $f'(z_0) = 1$; *then* f *is the identity on* D.

2 How to run the proof

The HOL Light environment [Har08, Har96] is built on top of the Objective CAML (OCaml) programming language [OCA], using its powerful *inductive type definition* feature.

From a logical point of view, in HOL Light there are two main categories of objects:

- "term", which is any term in typed λ-calculus;
- "theorem", corresponding to terms of type `boolean` which are derived from other terms and theorems via the legitimate inference rules.

These two categories are implemented in OCaml by suitable type constructors, whose purpose is to mimick the standard inference rules of logic. In particular, the constructor for the "theorem" type implements the ten basic inference rules (see [Har06]) so that to construct a theorem (i. e., an object of type `thm`) there are only two ways:

- either derive it by any combination of the basic inference rules, some of which require pre-existing theorems;
- or declare it as an *axiom* (at any moment you can examine the list of current axioms by means of the `axioms()` function).

This means that, assuming that the computer and the OCaml implementation are not broken, any object of type `thm` is a proven statement, that is, it can be deducted formally from the axioms listed by the `axioms()` function.

At the present, the latest version of the HOL Light theorem prover (snapshot of the 19th february 2008) comes with many proved theorems, including some multivariate real and complex analysis; everything is built on top of the following three axioms (for a discussion of such axioms, see e. g. [Har06]):

- `INFINITY_AX`
  `|- ?f. ONE_ONE f /\ ~ONTO f`
- `SELECT_AX`
  `|- !P x. P x ==> P ((@) P)`
- `ETA_AX`
  `|- !t. (\x. t x) = t`

Hence, to verify that the proof in the `cartan.ml` file is correct, the following steps must be carried out:

1. install and compile HOL Light, snapshot of the 19th february 2008, as available from [Har08], following the instruction on that website;
2. put the file `cartan.ml` in the HOL Light directory;
3. run `hol` and type

   ```
   loadt "cartan.ml";;
   ```

4. after some time (on present-day personal computers, about half an hour) HOL Light stops writing

   ```
   val ( FIRST_CARTAN_THEOREM ) : thm =
     |- !f z r n m w.
            f holomorphic_on ball (z,r) /\
            f continuous_on cball (z,r) /\
            &0 < r /\
            f z = z /\
            (!w. w IN ball (z,r) ==> f w IN ball (z,r)) /\
            (!w. w IN cball (z,r) ==> f w IN cball (z,r)) /\
            complex_derivative f z = Cx (&1) /\
            w IN ball (z,r)
            ==> f w = w
   ```

   showing that the above term has type `thm`. As we have showed before, this means that the corresponding claim has a complete proof.

Nota 1. At the present our proof uses some new theorems available only in the 19th february 2008 snapshot; these features should become "permanent" in the subsequent stable release of HOL Light, which at the present has not been released. When that will happen, we will update the present document and remove this notice.

3 Proof of the theorem

In this section we sketch the structure of the proof.

1. We prove four additional assumptions:
   - $f : D \to D \implies f^{\circ m} : D \to D$
   - $f : \overline{D} \to \overline{D} \implies f^{\circ m} : \overline{D} \to \overline{D}$
   - $f^{\circ m}$ is holomorphic on D
   - $f^{\circ m}$ is continuous on $\overline{D}$
2. We reduce the goal to

   ```
   !n. higher_complex_derivative n f z = higher_complex_derivative n (\x. x) z
   ```

   using the following theorem:

   ```
   HOLOMORPHIC_FUN_EQ_ON_BALL;;
   val it : thm =
     |- !f g z r w.
            f holomorphic_on ball (z,r) /\
            g holomorphic_on ball (z,r) /\
            w IN ball (z,r) /\
            (!n. higher_complex_derivative n f z =
                 higher_complex_derivative n g z)
            ==> f w = g w
   ```

3. We assume $n > 1$, since:
   - If $n = 0$, the goal follows trivially via `ASM_REWRITE_TAC[higher_complex_derivative]`;
   - If $n = 1$, the goal follows trivially via `ASM_REWRITE_TAC[ONE;higher_complex_derivative;COMPLEX_DERIVATIVE_ID]`
4. Using the explicit form of the derivatives of the identity (`HIGHER_COMPLEX_DERIVATIVE_ID`) we reduce the goal to:

   ```
   higher_complex_derivative n f z = Cx (&0)
   ```

5. We use generalized induction on n, assuming the goal for each $m < n$.
6. The norm is injective on zero (`COMPLEX_NORM_ZERO`), so the goal is reduced to

   ```
   norm (higher_complex_derivative n f z) = &0
   ```

7. We reduce the goal via an "Archimedean" real theorem:

   ```
   REAL_ARCH_RDIV_EQ_0;;
   val it : thm =
     |- !x c. &0 <= x /\ &0 <= c /\ (!m. 0 < m ==> &m * x <= c) ==> x = &0
   ```

8. We supply $\frac{n!r}{r^n}$ as the correct value for c, so that the goal, after some integer arithmetic, is reduced to

```
!m. 0 < m
    ==> &m * norm (higher_complex_derivative n f z) <=
        &(FACT n) * r / r pow n
```

9. We prove that $mD^n f(z) = D^n(f^{\circ m})(z)$, using the following theorem specialized to the case where `s` is the open disc `ball(z,r)`:

```
HIGHER_COMPLEX_DERIVATIVE_ITER_TOP_LEMMA;;
val it : thm =
  |- !f s z n m.
         open s /\
         f holomorphic_on s /\
         (!w. w IN s ==> f w IN s) /\
         z IN s /\
         f z = z /\
         complex_derivative f z = Cx (&1) /\
         (!i. 1 < i /\ i < n ==> higher_complex_derivative i f z = Cx (&0)) /\
         1 < n
         ==> higher_complex_derivative n (ITER m f) z =
             Cx (&m) * higher_complex_derivative n f z
```

10. We reduce the goal using the following theorem:

```
CAUCHY_HIGHER_COMPLEX_DERIVATIVE_BOUND;;
val it : thm =
  |- !f z y r B0 n.
         &0 < r /\
         0 < n /\
         f holomorphic_on ball (z,r) /\
         f continuous_on cball (z,r) /\
         (!w. w IN ball (z,r) ==> f w IN ball (y,B0))
         ==> norm (higher_complex_derivative n f z) <=
             &(FACT n) * B0 / r pow n
```

11. The goal is now a straightforward consequence of the assumptions.

References

[Har96] John Harrison. HOL Light: A tutorial introduction. In Mandayam Srivas and Albert Camilleri, editors, *Proceedings of the First International Conference on Formal Methods in Computer-Aided Design (FMCAD'96)*, volume 1166 of *Lecture Notes in Computer Science*, pages 265–269. Springer-Verlag, 1996.

[Har06] John Harrison. HOL Light tutorial (for version 2.20). Freely available at `http://www.cl.cam.ac.uk/~jrh13/hol-light/tutorial_220.pdf`, 2006.

[Har08] John Harrison. The HOL Light theorem prover, snapshot of 19th february 2008. Freely available at `http://www.cl.cam.ac.uk/~jrh13/hol-light/`, 2008.

[OCA] The Objective CAML language. Freely available at `http://caml.inria.fr/ocaml/`.