Non-constructive complex analysis in Coq

Aloïs Brunel

Université Paris 13, Sorbonne Paris Cité, Laboratoire d'Informatique de Paris-Nord (LIPN), CNRS, UMR 7030, F-93430, Villetaneuse, France.
alois.brunel@ens-lyon.org

Abstract

Winding numbers are fundamental objects arising in algebraic topology, with many applications in non-constructive complex analysis. We present a formalization in Coq of the winding numbers and their main properties. As an application of this development, we also give non-constructive proofs of the following theorems: the Fundamental Theorem of Algebra, the 2-dimensional Brouwer Fixed-Point theorem and the 2-dimensional Borsuk-Ulam theorem.

1998 ACM Subject Classification F.4.1 Mathematical Logic

Keywords and phrases Coq, complex analysis, winding numbers

Digital Object Identifier 10.4230/LIPIcs.TYPES.2011.1

1 Introduction

In this paper we present a formalization in Coq of several results in complex analysis. More precisely, we have formalized non-constructive proofs of the following theorems: the two-dimensional Brouwer Fixed Point theorem, the two-dimensional Borsuk-Ulam theorem and the Fundamental Theorem of Algebra. The particularity of these proofs, besides their classical nature (in the logical sense), is that they all rely on the notion of winding number, which is an invariant of homotopy. The winding number around a point $z \in \mathbb{C}$ of a closed curve γ basically counts how many time γ *turns* counterclockwise around z. They constitute an important notion in algebraic topology and have applications in many domains of mathematics and physics, including complex analysis but also differential geometry and string theory. This wide range of applications has decided us to start the formalization of this notion in Coq, along with examples of important applications.

Finally, we are also interested in organizing our development in a reusable set of libraries on top of Coq Standard Library. There is still some cleaning and organizing work to do on our development, but we think the presented work is close to that goal.

Contributions

To establish these results, we had to develop a whole library on top of the Coq Standard Library. It includes a general purpose library for metric spaces, defined using type classes [12], that generalize several results of the Coq Standard Library of reals. We have formalized some properties of Euclidean spaces, including the characterization of compact sets as the bounded closed sets. Our formalization also provides definitions and various results about the complex plane: the definition and the continuity of common functions, the existence of a complex logarithm and a continuous lifting theorem. Finally, a crucial part of the formalization concerns the definition of the winding number of a closed path and its main properties, culminating in proving that the winding number is an homotopy invariant. Results about line integrals have also been formalised but they are just briefly discussed in this paper. To

18th International Workshop on Types for Proofs and Programs (TYPES 2011).
Editors: Nils Anders Danielsson, Bengt Nordström; pp. 1–15

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

define winding numbers, we have followed [11]. The proofs of the three mentioned theorems we have formalised can be found in [5].

The classical nature of the proofs presented here is twofold. First, we decisively use the reasoning by contradiction to obtain the different results from the homotopy invariance theorem (although it is not used to define winding numbers or to prove the homotopy invariance of the winding number). Secondly, the standard library of reals of Coq is a classical axiomatization of the field of reals.

Related work

C-CoRN Project — A constructive proof of the Fundamental Theorem of Algebra has been formalized as part as the C-CoRN project [2]. Its proof [6] relies on elementary properties of $\mathbb{R}$ and $\mathbb{C}$ (mostly the existence of k-th roots in $\mathbb{C}$, an intermediate value theorem for polynomials and some basic polynomial arithmetic). The constructive nature and the careful design of the proof makes it particularly suitable for extraction [3]. In contrast, we were interested in formalizing classical mathematics, which makes our two works completely different in nature. Yet, it does not mean we completely give up on the possibility of extraction, as discussed in the conclusion.

Coqtail Project — Coqtail [4] is a project intended to extend the standard Coq library by providing clean, reusable libraries for various domains of undergraduate mathematics: arithmetic, reals, basic complex analysis, basic topology. It has been used to formalize a proof of Lagrange's four square theorem, to formalize power series and solve some differential equations [1]. It seems that many of the basic definitions about complex numbers and functions coincide in both our works, and so it is likely that the developments described here could easily be integrated in their library.

Other proof assistants — Numerous developments based on complex analysis, euclidean spaces or topology have been formalized in other proof assistants. One can cite Harrison's works in HOL Light [8, 7] on the theory of Euclidean spaces (including a proof of the general Brouwer Fixed-Point theorem, using combinatorial arguments) and on a complex-analytic proof of the prime number theorem.

Outline

Basic definitions and notations are described in section 2. We then present in section 3 the metric spaces and euclidean spaces libraries. Section 4 introduces the existence of a complex logarithm, the continuous lifting theorem and finally the definition of the winding number and the formalization of some of its main properties. We present the non-constructive proof of the main theorems along with their formalization in section 5. Section 6 finally concludes this work.

2 Basic notations and definitions

We give here the basic notations and definitions, relative to the complex plane and the euclidean spaces in general, needed to understand the Coq statements of the next sections.

2.1 Complex plane

We begin with the definition of the complex plane. We remind that the underlying theory of reals that we use is the one of the Coq Standard Library. It is based on an axiomatic definition of the field of reals. It has to be noted that this axiomatic definition of reals is fundamentally classical.

The set $\mathbb{C}$ is defined as $\mathbb{R}^2$, the imaginary and real parts being respectively the first and second projections.

```
Definition C : Set := prod R R.
Definition CRe (c : C) : R := match c with ( a, _) => a end.
Definition CIm (c : C) : R := match c with ( _, b) => b end.
```

`co : R*R -> C` denotes the trivial coercion from `R*R` to `C`, so that `co a b` represents the complex number $a + ib$. A coercion from `R` to `C` is defined and noted `IRC`.

```
Definition IRC (r : R) : C := co r 0.
Coercion IRC : R >-> C.
```

It also possible to define a complex number by its polar form.

```
Definition polar_form (r: R) (t : R) :=  co (r*cos t) (r*sin t).
```

We declare distinguished elements of `C`, noted `0`, `1`, `Ci` representing respectively 0, 1 and the purely imaginary number i. We endow `C` with operations noted as in `R`, `+`, `-`, `*` and `/`. `C` then defines a ring and a field, and is declared as such, permitting to use the `ring` and `field` tactic families. The absolut value and the conjugation operations are noted respectively `Cmod` and `Cconj`. The complex exponential is defined using the real exponential already defined in the standard library and the polar form:

```
Definition Cexp (c : C) := polar_form (exp (CRe c)) (CIm c).
```

The circle of radius `r` can then be parametrized as follows.

```
Definition C_circle_par (r : R) (theta : R) : C :=  r * Cexp (0,theta).
```

2.2 Euclidean space

We also define the euclidean space $\mathbb{R}^n$, using an inductive product of set.

```
Fixpoint prod_n (E: Set) (n:nat) : Set :=
  match n with
   | O => unit
   | S n => prod (prod_n E n) E
  end.
```

Hence `prod_n R n` represents the set $\mathbb{R}^n$. We define usual operations on $\mathbb{R}^n$: `[+]`, `[-]`, `[.]` and an element `[0]` implementing respectively the addition, the substraction, the inner product and the element $(0, \ldots, 0)$.

2.3 Domains

We define useful subsets of $\mathbb{R}$ and $\mathbb{C}$.

```
Definition CUnit_Disk : C -> Prop := fun x => Cmod x <= 1.
Definition CUnit_Circle : C -> Prop := fun x => Cmod x = 1.
Definition RDom_Int (a b : R) : R -> Prop := fun x => a <= x <= b.
Definition CRect (a b c d : R) : C -> Prop := fun c => a <= CRe c <= b
/\ d <= CIm c <= e.
```

We define the notion of star shaped subset of $\mathbb{C}$.

```
Definition CDom_Star (K : C -> Prop) :=
  forall x y : C, K x -> K y ->
  forall lam : R, 0 <= lam <= 1 -> K (lam * x + (1 - IRC lam) * y).
```

3 Metric spaces

To prove sophisticated complex analysis results, we need elementary regularity properties of functions on $\mathbb{R}^n$, which are consequences of the metric space structure of $\mathbb{R}^n$, such as Heine theorem (continuity on a compact implies uniform continuity). There are also properties we need for $\mathbb{R}, \mathbb{R}^2$ and $\mathbb{R}^3$, which are true for all euclidean spaces $\mathbb{R}^n$. Instead of reproving these results each time we consider a different set, we do it in the general case. Hence, we provide libraries for metric spaces and euclidean spaces, which are presented in this section.

3.1 Metric spaces

We define metric spaces and of top of them, the notions of continuity, uniform continuity, open set, closed set, and so on. We mostly follow the definitions and naming already present in Coq reals library. Our choice has been to define metric spaces as a type class [12], hence benefiting of features like notation overloading, parametrized instances and generalized type-class binders. The definition is as follows:

```
Class MetrSpace (E: Set) :=
{
  d : E -> E -> R;
  pr_pos : forall x y : E, 0 <= d x y;
  pr_sym : forall x y : E, (d x y) = (d y x);
  pr_sep : forall x y : E, (d x y = 0) <-> x = y;
  pr_tri : forall x y z : E, d x y <= (d x z) + (d z y);
  pt  : E
}.
```

▶ Remark. Notice that we define *pointed* metric spaces, that is a metric space together with a distinguished element `pt` of the base set. This is just a convenient choice that simplifies a bit some proofs abound bounded sets and the writing of some tactics about continuity (that we don't mention in this paper).

Different instances of the class `MetrSpace` are declared, like $\mathbb{R}$ and $\mathbb{C}$. We also define the product metric space of two metric spaces as a parametrized instance:

```
Instance prod_MetrSpace `(EM : MetrSpace E, FM: MetrSpace F) :
                                    MetrSpace (E * F).
```

This allows to declare the n-dimensional euclidean space $\mathbb{R}^n$ as a metric space.

In the definition of limits and continuity between two metric spaces, the latter are introduced via generalized type-class binders, which allows to write statements and proofs in a natural way.

```
Definition Metr_limit_in `{EM: MetrSpace E, FM: MetrSpace F}
  (f : E -> F) (D : E -> Prop) (a : E) (l : F) :=
  forall eps : posreal -> exists eta : posreal /\
   (forall x, D x -> d x a < eta -> d (f x) l < eps).

Definition MS_continue_in `{EM : MetrSpace E, FM : MetrSpace F}
  (f : E -> F) (D : E -> Prop) (a : E) : Prop :=
    Metr_limit_in f D a (f a).

Definition MS_uniform_continuity `{EM : MetrSpace E, FM : MetrSpace F}
  (f : E -> F) (D : E -> Prop) : Prop :=
  forall eps : posreal, exists delta : posreal,
      (forall x y: E, D x -> D y ->
       d x y < delta -> d (f x) (f y) < eps).
```

▶ **Example 1.** As an example, the statement that the function $x \in \mathbb{R} \mapsto x + 1$ is uniformly continuous on $\mathbb{R}$ is simply written in Coq:

```
MS_uniform_continuity (fun x => x + R1) (fun x => True)
```

The notation is light: there is no need to specify the base set nor the metric space used here, since the type-class constraint system permits to retrieve the previously declared metric space on $\mathbb{R}$.

The definition of compact set is adapted from the one used in the Coq Reals library. It is however a notion of compactness with respect to a set of open sets $\mathcal{O}$.

```
Definition MS_compact_base `{EM: MetrSpace E}
  (X: E -> Prop) (O: (E->Prop)->Prop) : Prop :=
  forall I : Type, forall IM: MetrSpace I, forall f : MS_family I E,
    MS_covering_open_set X f -> MS_family_base f O ->
     exists D : I -> Prop, MS_covering_finite X (MS_subfamily f D).
```

This amounts to say that a set X is compact if whenever we have a cover $\mathcal{C}$ of X constituted by open sets of $\mathcal{O}$, we can find a finite subset $\mathcal{C}' \subseteq \mathcal{C}$ which is still a cover of X. The usual compactness property is just an alias for compactness with respect to all open sets.

```
Definition MS_compact `{EM: MetrSpace E}  (X: E -> Prop) : Prop :=
  MS_compact_base X (fun _ => True).
```

In the Real library, a cover is represented by a family of open sets $(O_i)_{i\in\mathbb{R}}$ indexed by $\mathbb{R}$. Here, we can use any element of `Type` as a set of indexes. This is indeed necessary to prove a crucial result: compactness is equivalent to compactness with respect to an open set basis.

```
Theorem MS_compact_basis `{EM : MetrSpace E}:
  forall X : E -> Prop, forall O : (E -> Prop) -> Prop,
  forall Ho: MS_open_basis O, MS_compact_base O X -> MS_compact X.
```

Here, `MS_open_basis O` denotes the fact that a set $\mathcal{O}$ of open sets is such that any open set G can be written $G = \bigcup_{X \in O \wedge X \subseteq G} X$. To prove this theorem, we *need* to have an index set of type `Type`. Indeed, from an original cover C_i, we build the cover $C_{(i,U)}$ where U is an open set such that $U \subseteq C_i$ and $U \in \mathcal{O}$. This amounts to use `prod I (E -> Prop)` as a type for indexes, which justifies the use of `Type`.

▶ **Example 2.** As an example of a theorem already proved for $\mathbb{R}$ in the standard library, the Heine theorem is now available for all metric spaces. It states that every continuous function on a compact set is also uniformly continuous.

```
Theorem MS_Heine :
  forall (f:E -> F) (D:E -> Prop),
    MS_compact D -> MS_continue_on f D -> MS_uniform_continuity f X.
```

3.2 Euclidean spaces

Rather than defining directly euclidean spaces with the particular canonical euclidean scalar product, we define them axiomatically as a type class:

```
Class Euclidean (dim : nat) :=
{
  scal : prod_n R dim -> prod_n R dim -> R;
  scal_sym : forall x y : prod_n R dim, scal x y = scal y x;
  scal_pos : forall x : prod_n R dim, 0 <= scal x x;
  scal_def : forall x  : prod_n R dim, scal x x = R0 -> x = Rn_zero;
  scal_add1 : forall x y z : prod_n R dim, scal (Rn_plus x y) z =
                        scal x z + scal y z;
  scal_add2 : forall x y z : prod_n R dim, scal x (Rn_plus y z)  =
                        scal x y + scal x z;
  scal_lam1 : forall x y lam, scal (Rn_dot  x lam) y= lam * scal x y;
  scal_lam2 : forall x y lam, scal x (Rn_dot  y lam)= lam * scal x y
}.
```

Each instance of an euclidean space then defines an euclidean norm, defined as follows:

```
Definition Eucl_norm `{E : Euclidean n} :=
  fun x : prod_n R n => sqrt (scal x x).
```

We define two notations for the unit disk and the unit circle of dimension n.

```
Definition RnUnit_Disk `{E : Euclidean n} :=
    fun x : prod_n R n => Eucl_norm x <= 1.
Definition RnUnit_Circle `{E : Euclidean n} :=
    fun x : prod_n R n => Eucl_norm x = 1.
```

From these axioms, we derive several useful properties, like the Cauchy-Schwarz inequality.

```
Lemma Eucl_CauchySchwartz `{E: Euclidean n}:
 forall x y, Rabs (scal x y) <= Eucl_norm x * Eucl_norm y.
```

Using the euclidean norm to define a distance, we can show that each euclidean space $\mathbb{R}^n$ defines a metric space instance.

```
Instance Rn_MetrSpace {n : nat} : MetrSpace (prod_n R n).
```

An important step in our development is the Borel-Lebesgue theorem, which states that in $\mathbb{R}^n$, the compact sets (defined in terms of covering) are exactly those sets which are both closed and bounded.

```
Theorem Eucl_Borel_Lebesgue:
  forall n : nat, forall X : prod_n R n -> Prop,
    (MS_compact X <-> MS_closed_set X /\ MS_bounded X).
```

In particular, to show that a closed and bounded set is compact, we reason by induction and use the fact that a product of compacts is compact. That is where we need the equivalence between compactness and compactness on the product basis (which, for the product metric space, is the set of product of open sets) stated in the previous subsection.

4 Winding number theory

There are many ways to define the winding number. Mostly, two approaches are possible: by using path integral or by proving a lifting theorem. We have formalised both definitions, but we focus only on the latter, since it is more general and presents many advantages, as advocated in subsection 4.4 In this section, we present the following results: the existence of a complex logarithm, a continuous lifting theorem, and finally the notion of winding numbers.

4.1 Complex logarithm

A complex logarithm is an *inverse* of the complex exponential function, similarly to the case of the real-valued functions ln and e^x. However, the situation is more complicated on $\mathbb{C}$ than on $\mathbb{R}$. Indeed, the complex exponential is not injective (just consider the identity $e^x = e^{x+2i\pi}$) and hence cannot have an inverse function. This problem is usually solved by restricting the domain of the exponential to a subset on which it is injective. In our case, we restrict it to $\mathbb{R}\times]-\pi,\pi]$, and hence the logarithm will be defined only on the domain $\mathbb{C}\setminus\mathbb{R}_-$, which is defined in Coq as:

```
Definition CLog_D0 := fun c => forall x : R, x <= 0 -> c <> IRC x.
```

We first show that every point z of this domain has a logarithm. To prove that it suffices to notice that by the domain restriction, the polar decomposition of $z = re^{i\theta}$ is unique. This fact is equivalent to the following statement.

```
Lemma CLog_1:
  forall z, CLog_D0 z ->
    exists r, exists theta,  0 < r /\ -PI < theta <= PI /\
      (IRC r) * Cexp (co 0 theta) = z.
```

Hence, its logarithm can be defined by $Log(z) = ln(r) + i\theta$. We can then prove the *existence* of a logarithm function on the domain `CLog_D0`. This function is necessarily continuous.

```
Lemma CLog_ex_continuous :
  exists log : C -> C, log C1  = C0 /\
  (forall z, CLog_D0 z ->
     -PI <= CIm (log z) <= PI /\ Cexp (log z) = z /\ MS_continue_in log z).
```

To prove this theorem, we crucially need the axiom of choice in its functional form:

```
Axiom choice :
 forall (A B : Type) (R : A->B->Prop),
   (forall x : A, exists y : B, R x y) ->
    exists f : A->B, (forall x : A, R x (f x)).
```

We could obtain an actual function `log : C -> C` by using the principle of constructive indefinite description.

```
Axiom constructive_indefinite_description :
  forall (A : Type) (P : A->Prop),
    (exists x, P x) -> { x : A | P x }.
```

This principle is stronger than the axiom of choice. In fact, we never need to obtain a logarithm function: the statement of its existence is enough.

4.2 Complex lifting

Given a function $f : \mathbb{C} \to \mathbb{C}$ continuous on K, we say that $\Phi : K \to \mathbb{C}$ is a continuous lifting of f if Φ is continuous and $\forall x \in K, f(x) = \|f(x)\|e^{\Phi(x)}$. We can state the existence of such a lifting for any set K, which is both compact and star-shaped.

```
Theorem Complex_Lifting:
  forall F : C -> C, forall K : C -> Prop,
  MS_compact K ->  CDom_Star K -> MS_continue_on F K ->
  (forall x, K x -> F x <> C0) -> exists Phi : C -> C,
      (forall x : C, K x -> F x = IRC (Cmod (F x)) * Cexp (Phi x)) /\
      MS_continue_on Phi K.
```

The proof, which we don't detail, crucially relies on the uniform continuity of the function, and hence on Heine theorem.

4.3 Winding numbers

A *path* is a continuous function $\gamma : [a, b] \to \mathbb{C}$. We moreover say it is a *closed path* if $\gamma(a) = \gamma(b)$. From now on, we only consider closed path γ such that $\forall x \in [a, b], \gamma(x) \neq 0$. In Coq, a closed path is represented as a record containing its domain together with a proof of its continuity.

```
Record C_lace : Type := mklace {
  gam :> R -> C;
  a : R;
  b : R;
  ab_pr: a <= b;
  gam_lace : gam a = gam b;
  gam_cont: forall x, RDom_Int a b x -> MS_continue_in gam (RDom_Int a b) x
}.
```

Given a closed path g, we say that $\psi : [a, b] \to \mathbb{C}$ is an argument of g if ψ is continuous and if $\forall x \in [a, b], g(x) = \|g(x)\|e^{\psi(x)}$. This property is denoted in Coq by

```
Definition cont_arg_choice (a b : R) (F : R -> C) (psi : R -> C) :=
   (forall x, RDom_Int a b x -> F x = IRC(Cmod(F x))*(Cexp (psi x)))
/\ (forall x, RDom_Int a b x -> MS_continue_in psi (RDom_Int a b) x).
```

If γ is nowhere vanishing (meaning it never takes the value 0 on its domain) and H is an argument of γ, we can define its *winding number* (around 0) by:

```
Definition lace_WN_param (g : C_lace) (psi : R -> C) : C :=
  (psi (b g) - psi (a g))/(co 0 (2*PI)).
```

Moreover, we prove that whatever the choice of argument we have made, the winding number is the same.

```
Lemma lace_WN_param_equal:
  forall g, (forall x, RDom_Int (a g) (b g) x -> g x <> C0) ->
  forall psi1 psi2,
    cont_arg_choice (a g) (b g) g psi1 ->
    cont_arg_choice (a g) (b g) g psi2 ->
       lace_WN_param g psi1  = lace_WN_param g psi2.
```

▶ Remark. Usually, because the winding number is invariant by the choice of argument, it is defined as an actual number using a specific continuous argument ψ obtained by the complex lifting theorem.

$$n(\gamma, 0) = \frac{\psi(b) - \psi(a)}{2i\pi}$$

We choose not to do that since it would mean using the principle of constructive indefinite description to obtain an argument, which can be avoided. Instead, we will always carry an assumption of the existence of a continuous argument.

An important property is that the winding number of a closed path is always an integer.

```
Lemma lace_WN_param_Z:
  forall g psi,
    (forall x, RDom_Int (a g) (b g) x -> g x <> C0) ->
    cont_arg_choice (a g) (b g) g psi ->
    exists z : Z, lace_WN_param g psi = IRC (IZR z).
```

To obtain this result, we make use of trigonometry results contained in the standard library. Here is an informal proof.

Proof. Suppose that for every x, $\gamma(x)$ is in the unit disk. Let Φ be a lifting of γ: $\gamma(x) = |\gamma(x)|e^{\Phi(x)}$. Then, $e^{\Phi(b)-\Phi(a)} = 1$ (since $\gamma(a) = \gamma(b)$. Hence, there exists some $k \in \mathbb{Z}$ such that $\Phi(b) - \Phi(a) = 2i(k\pi)$. Hence $n(\gamma, 0) = \frac{\Phi(b)-\Phi(a)}{2i\pi} = k \in \mathbb{Z}$. ◀

▶ **Example 3.** As an example, we can compute the winding number of the unit circle.

```
Definition C_circ_unit : R -> C := fun t => Cexp (co 0 (2*PI*t)).
```

The winding number of the corresponding path `C_circ_lace` between 0 and 1 is equal to 1. This fits the intuition of the path turning one time around the point 0.

```
Lemma C_circ_fact2:
  forall psi, cont_arg_choice 0  1 (C_circ_lace) psi ->
    lace_WN_param C_circ_lace psi  = C1.
```

The final and important theorem is the *invariance of the winding number by homotopy*. Formally, supposing two closed paths `g0, g1 : C_lace` are *homotopically equivalent*, that is there exists a continuous function `H : C -> C` such that:

```
Definition CHomotopyEqu (g0 g1 : C_lace) (H : C -> C) :=
  a g0 = a g1 /\ b g0 = b g1 /\
  (forall x, a g0 <= x <= b g0 -> H(0,x) = g0 x) /\
  (forall x, a g1 <= x <= b g1 -> H(1,x) = g1 x) /\
  (MS_continue_on H (CRect 0 1 (a g0) (b g0))) /\
  (forall x, RDom_Int 0 1 x -> H(u, a g0) = H(u, b g0)).
```

And if moreover, `H` never equals to `0` (which ensures that neither `g0` nor `g1` do), then the winding numbers of `g0` and `g1` are equal. This is summarized in the following theorem:

```
Theorem Clace_WN_homotopy_invariant:
  forall g0 g1 : C_lace, forall H : C -> C,
  (forall c, (CRect 0 1 (a g0) (b g0) c) -> H c <> C0) ->
  CHomotopyEqu g0 g1 H ->
  forall psi0 psi1 : R -> C,
    cont_arg_choice (a g0) (b g0) g0 psi0 ->
    cont_arg_choice (a g1) (b g1) g1 psi1 ->
      lace_WN_param g0 psi0 = lace_WN_param g1 psi1.
```

▶ Remark. Notice that here again, the theorem is stated without fixing a choice of argument for the closed paths.

4.4 Winding numbers: path integral versus continuous lifting

We have presented here a definition of winding number of a closed path by using a choice of argument for it. It is however often defined using line integrals. We can indeed define the winding number of a closed path $\gamma : [a, b] \to \mathbb{C}$ around a point c as:

$$n(\gamma, c) = \frac{1}{2i\pi} \oint_\gamma \frac{dz}{z - c}$$

where the line integral is defined using

$$\oint_\gamma f(z)dz = \int_a^b f(\gamma(t))\gamma'(t)dt$$

We have also formalized this alternative definition and proved that it yields the same result as the other. It has shown several disadvantages over the definition we have presented:

- To define path integrals, we need a good definition of integration for complex valued functions over $\mathbb{R}$. We have experimented using the Riemann integral from the Standard Library of Coq. It allows one to define winding numbers without the path lifting theorem, but always reasoning on integrals rather than in terms of complex exponentials and logarithms is definitely more difficult.
- The main problem is that because we use path integrals, we also need the path γ to be differentiable (it can be then extended for continuous paths, but it involves sophisticated results about complex analysis we have not formalised). This is indeed a severe restriction, since we could prove the Fundamental Theorem of Algebra, but not the Brouwer Fixed-Point theorem or the Borsuk-Ulam theorem, which are stated for continuous functions. In contrast, coupled with the continuous lifting theorem, our definition immediately only requires continuity of γ.

5 Applications of the winding number homotopy invariance

We now detail the proofs we have formalized of the Fundamental Theorem of Algebra, the Brouwer Fixed-Point theorem and finally of the Borsuk-Ulam theorem. All these proofs rely on corollaries of the invariance by homotopy of the winding number and classical principles.

5.1 Prerequisites

We briefly give the statements and sketch the proofs of two fundamental lemmas needed for the proofs of the Borsuk-Ulam and Brouwer Fixed Point theorems.

▶ **Lemma 4.** *Suppose $f : \mathbb{C} \to \mathbb{C}$ is continuous and nowhere vanishing on the unit disk. Then if $\gamma(t) = f(e^{2i\pi t})$, we have $n(\gamma, 0) = 0$.*

Proof. The path γ is homotopically equivalent to the constant path $t \mapsto f(0)$. Indeed, $H(u,t) = f(u * e^{2i\pi t})$ is such that $H(0,t) = f(0)$ and $H(1,t) = \gamma(t)$. It is moreover continuous because f is, and vanishes nowhere. Hence, because any constant path has a winding number equal to 0, we conclude by homotopy invariance of the winding number. ◀

▶ **Lemma 5.** *There does not exist a map $f : \mathbb{C} \to \mathbb{C}$ which is continuous, odd (that is $f(-x) = -f(x)$) and nowhere vanishing on the unit disk.*

Proof. We will prove that if such a map f exists, then if we pose the lace $\gamma(t) = f(e^{i\pi t})$, there exists $k \in \mathbb{Z}$ such that $n(\gamma, 0) = 2k + 1$ (we skip the proof here, but it only involves simple calculations). Hence, because of Lemma 4, it leads to a contradiction. ◀

5.2 Fundamental Theorem of Algebra

The first application is a classical proof of the Fundamental Theorem of Algebra, which states that any complex polynomial has a root. A complex polynomial is represented as a list of complex coefficients, begining with the coefficient of higher degree and ending with the one of degree 0.

```
Definition C_polynom : Set := Clist.
Definition C_polynom_deg (P : C_polynom) := pred (Clength P).
```

But of course, we need to remove the extra elements equals to `C0` in order to be able to calculate the true degree of the polynomial. This is the job of the function `C_polynom_without_zero` which has the type `C_polynom -> C_polynom`. The evaluation of a polynomial is done inductively by the function `C_polynom_eval : C_polynom -> C`. We now prove the following statement.

```
Theorem FTA: forall P : C_polynom,
   (1 <= C_polynom_deg (C_polynom_without_zero a)) ->
   exists x : C, C_polynom_eval P x = C0.
```

So suppose the existence of a polynomial `P` of degree `n` (and we note its dominating coefficient $a_n \neq 0$) such that

```
Variable pr_deg : n >= 1.
Variable pr_root: forall x, C_polynom_eval a x <> C0.
```

We then define the lace `Gamma_circle r` whose underlying function is the parametrization of the circle of radius `r` deformed by the polynomial `P` (and by hypothesis `pr_root`, it makes sense to speak of its winding number):

```
fun theta : R => C_polynom_eval P (C_circle_par r theta)
```

Now if `R1` is big enough, the polynomial becomes dominated by its coefficient of larger degree `C_polynom_domcoeff P`, and then the winding number is the same wether or not you consider the other coefficients:

```
Definition nu (r : R) (theta : R) : C :=
  C_polynom_domcoeff P * IRC (r^n) * Cexp (co 0 ((INR n)*theta)).

Lemma Alembert_theo5:
  exists M : R, 0 < M /\ forall R1,  forall pr : 0 < R1,
  forall pr2 : M < R1, forall psi1 psi2 : R -> C,
  cont_arg_choice 0 2*PI (nu_path R1 pr) psi1 ->
  cont_arg_choice 0 2*PI (Gamma_circle R1) psi2 ->
  lace_WN_param (nu_path R1 pr) psi1 = lace_WN_param (Gamma_circle R1) psi2.
```

But the winding number of $\nu(\theta) = a_n r^n e^{in\theta}$ can be shown by a simple calculation to be equal to n. When the circle is of radius 0, the obtained path `Gamma_circle 0` is constant and hence its winding number is equal to 0. On the other hand, we can show that whatever the positive reals `R1 R2 : R`, the paths `Gamma_circle R1` and `Gamma_circle R2` are homotopically equivalent, and so have the same winding number.

```
Lemma Alembert_theo3:
  forall R1, 0 <= R1 -> forall R2, 0 <= R2 ->
    (forall psi1 psi2 : R -> C,
       cont_arg_choice 0 2*PI (Gamma_circle R1) psi1 ->
       cont_arg_choice 0 2*PI (Gamma_circle R2) psi2 ->
         forall Arg: R -> (R -> C), forall Harg: (forall r,
           Rmin R1 R2 <= r <= Rmax R1 R2 ->
           cont_arg_choice 0 2*PI (Gamma_circle r) (Arg r)),
lace_WN_param (Gamma_circle R1) psi1 = lace_WN_param (Gamma_circle R2) psi2.
```

The contradiction comes immediately, since when going from `0` to a real `R` big enough, the winding number changes from `0` to `n` (by Lemma `Alembert_theo5`). This is contradicted by the previous lemma `Alembert_theo3` and because `1 <= n`.

5.3 Brouwer Fixed-point theorem

We now prove the 2-dimensional version of the celebrated Brouwer Fixed-Point theorem. It is a classical (in the sense of classical reasoning) corollary of the following no retraction theorem.

```
Theorem No_Retraction:
 ~(exists r : C -> C,
   (forall x, CUnit_Disk x -> CUnit_Disk (r x)) /\
   (forall x, CUnit_Circle x -> r x = x)    /\
   (forall x, CUnit_Disk x -> MS_continue_in r CUnit_Disk x)).
```

Proof. Suppose by contradiction that we have such a retraction r. By hypothesis, for every x in the unit disk, $r(x) \neq 0$, and r is continuous. Hence, by Lemma 4, the lace $\gamma : t \mapsto r(e^{2i\pi t})$ is such that $n(\gamma, 0) = 0$. But, $\gamma(t) = e^{2i\pi t}$ since r is the identity on the unit circle. By Lemma 5, however, we have $n(\gamma, 0) \neq 0$, which is contradictory. ◀

We are now able to formalize a proof of the Brouwer Fixed-Point theorem, which is stated as follows.

```
Theorem BrouwerFixedPoint:
  forall f : C -> C, (forall x, CUnit_Disk x -> CUnit_Disk (f x)) ->
    MS_continue_on f CUnit_Disk ->
    exists x, CUnit_Disk x /\ f x = x.
```

The key point is to reason classicaly by supposing the existence of a map which has no fixpoint and build a retract `CUnit_Disk` to `CUnit_Circle` out of it, which will lead to a contradiction by the no retraction theorem.

Proof. The proof is carried using the following classical principle

```
not_all_not_ex: forall P:U->Prop, ~(forall n:U, ~P n) -> exists n:U, P n.
```

We suppose that `f : C -> C` is continuous on the unit disk and has no fixpoint, and derive a contradiction.

```
Hypothesis Br_H1: forall x, CUnit_Disk x -> CUnit_Disk (f x).
Hypothesis Br_H2: forall x, CUnit_Disk x -> MS_continue_in f CUnit_Disk x.
Hypothesis Br_H3: forall x, CUnit_Disk x -> f x <> x .
```

We want to define a continuous retract `brouwer_retract : C -> C` from the unit disk to the circle. Informally, consider a point `z` of the unit disk and its image `f(z)`. Since we have supposed that `f(z) <> z`, we can continue the segment that joins `f(z)` to `z` until it reaches the unit circle. `brouwer_retract z` is this intersection point. Formally, given two distinct points `x0` and `x` of the unit disk, we need to solve the equation

$$(E) \quad x_0 + \lambda(x - x_0) \quad = \quad 1$$

Finding λ amounts to solve a second degree (real) polynomial, which can be done using the standard Coq library. Given a polynomial aX^2+bX+c, if its discriminant b^2-4ac is positive, the two roots (which are possibly equal) are given by `sol_x1 a b c` and `sol_x2 a b c`. We use this to obtain a function `LC_lambda x x0 : x <> x0 -> R` that calculates the λ of Equation (E).

```
Lemma line_circle_intersect (x0 x : C) (H : x <> x0) :
  CUnit_Disk x0 ->
    Cmod (x0 + IRC (LC_lambda x x0 H) * (x - x0)) = 1 /\
    Cmod x = 1 -> LC_lambda x x0 = 1.
```

The map `brouwer_retract` is then defined, and if `z` is in the unit disk (we have a proof `Hunit : CUnit_Disk z`), it is equal to

```
f z + IRC (LC_lambda z (f z) (Br_H3 z Hunit)) * (z - f z)
```

To conclude, we need to show that `brouwer_retract` is indeed a continuous retract, which amounts to prove the three following lemmas. The first one is the continuity of `brouwer_retract` on the unit disk. This proof involves a lot of bureaucracy, since we have to show that `LC_lambda` is continuous on $\mathbb{C}^*$.

```
Lemma Br_retract_continue : MS_continue_on brouwer_retract CUnit_Disk.
```

Secondly, restricted to the circle, `brouwer_retract` is the identity.

```
Lemma Br_retract_circle :
  forall z : C, CUnit_Circle z -> brouwer_retract z = z.
```

And finally `brouwer_retract` is actually a map from the unit disk to the unit circle.

```
Lemma Br_retract_unit :
  forall z : C, CUnit_Disk z -> CUnit_Circle (brouwer_retract z).
```

These two last lemmas are direct consequences of the lemma `line_circle_intersect`. Under these hypothesis, we conclude to a contradiction.

```
Lemma BrouwerNoFix : False.
```

◀

5.4 Borsuk-Ulam theorem

The last application is the Borsuk-Ulam theorem, which states that for any continuous complex-valued function f on the unit sphere, there exists a point x such that $f(x) = f(-x)$.

```
Theorem BorsukUlam:
  forall f : Rcube -> C, MS_continue_on f RnUnit_disk ->
  exists x, RnUnit_disk x /\ f (-x) = f x.
```

The proof of this theorem will be a consequence of the following intermediate lemma.

```
Lemma BU_lemma2:                #(AC)
  forall f : Rcube -> C, MS_continue_on f RnUnit_disk ->
  (forall x, BU_disk x -> f([-]x) = - f(x)) ->
  exists p, RnUnit_circle p /\ f p = 0.
```

Proof. Here again, we reason by contradiction using `not_all_not_ex`. So we suppose having a map f which is odd, continuous and nowhere vanishing. Then consider the following map (where $\mathcal{S}^2$ is the 2-sphere):

$$\begin{array}{rcl} \phi_h & : & \mathbb{R}^2 \to \mathcal{S}^2 \\ \phi_h(x,y) & = & (x, y, \sqrt{1-x^2-y^2}) \end{array}$$

Now, it is clear that if we pose $\gamma(t) = f(e^{2i\pi t}, 0)$, then $\gamma(t) = (f \circ \phi_h)(e^{2i\pi t})$. We know by hypothesis that $f \circ \phi_h$ never vanishes on $\mathbb{C}$ and is continuous. Hence, by Lemma 4, we have $n(\gamma, 0) = 0$. But by Lemma 5, because $f \circ \phi_h$ is nowhere vanishing, odd and continuous, we have $n(\gamma, 0) \neq 0$ which is contradictory. ◀

Given this last lemma, we obtain Borsuk-Ulam Theorem.

Proof of Borsuk-Ulam Theorem. We reason classicaly by supposing the existence of a function $f : \mathbb{R}^3 \to \mathbb{C}$, continuous on the unit ball and such that for every point x of the unit ball, $f(x) \neq f(-x)$. Then, consider the map

$$F(x) = \frac{f(x) - f(-x)}{\|f(x) - f(-x)\|}$$

Then F is well-defined and continuous by hypothesis, and F is clearly odd. Hence, using `BU_lemma2`, there exists x in the unit sphere such that $F(x) = 0$, which contradicts the hypothesis since it means $f(x) = f(-x)$. ◀

6 Conclusion and remarks

We have described in this paper a library implementing metric spaces, euclidean spaces and winding numbers, and we have employed it to prove sophisticated results in classical complex analysis. One future direction of research is the generalization of the results in arbitrary dimension. In this development, we have only proved the 2-dimensional version of Brouwer Fixed-Point and Borsuk-Ulam theorems, but their n-dimensional versions still can be proved. The proofs are quite similar to those we have briefly sketched here. However, it requires to use a generalization of the notion of winding number: the *degree* of a continuous mapping. It can be defined for maps from $\mathbb{R}^n$ to $\mathbb{R}^n$ (which is sufficient) but also for continuous mapping between oriented compact manifolds of the same dimension. To do this, one would need to formalize some parts of classical homotopy theory.

References

1 G. Allais. Using reflection to solve some differential equations. *3rd Coq workshop*, 2011.

2 Luís Cruz-Filipe, Herman Geuvers, and Freek Wiedijk. C-CoRN, the constructive Coq repository at Nijmegen. In Andrea Asperti, Grzegorz Bancerek, and Andrzej Trybulec, editors, *Mathematical Knowledge Management*, volume 3119 of *Lecture Notes in Computer Science*, pages 88–103. Springer Berlin Heidelberg, 2004.

3 Luís Cruz-Filipe and Bas Spitters. Program extraction from large proof developments. In David Basin and Burkhart Wolff, editors, *Theorem Proving in Higher Order Logics*, volume 2758 of *Lecture Notes in Computer Science*, pages 205–220. Springer Berlin Heidelberg, 2003.

4 Coqtail development team. http://coqtail.sourceforge.net.

5 W. Fulton. *Algebraic topology: a first course*. Springer, 1995.

6 Herman Geuvers, Freek Wiedijk, and Jan Zwanenburg. A constructive proof of the fundamental theorem of algebra without using the rationals. In Paul Callaghan, Zhaohui Luo, James McKinna, Robert Pollack, and Robert Pollack, editors, *Types for Proofs and Programs*, volume 2277 of *Lecture Notes in Computer Science*, pages 96–111. Springer Berlin Heidelberg, 2002.

7 J. Harrison. Formalizing an analytic proof of the prime number theorem. *Journal of Automated Reasoning*, 43(3):243–261, 2009.

8 John Harrison. A HOL theory of euclidean space. In Joe Hurd and Tom Melham, editors, *Theorem Proving in Higher Order Logics*, volume 3603 of *Lecture Notes in Computer Science*, pages 114–129. Springer Berlin Heidelberg, 2005.

9 J.L. Krivine. Realizability in classical logic. *Panoramas et synthèses*, 27:197–229, 2009.

10 Alexandre Miquel. Classical program extraction in the calculus of constructions. In Jacques Duparc and Thomas A. Henzinger, editors, *Computer Science Logic*, volume 4646 of *Lecture Notes in Computer Science*, pages 313–327. Springer Berlin Heidelberg, 2007.

11 M. Rao and H. Stetkaer. *Complex analysis: an invitation: a concise introduction to complex function theory*. World Scientific, 1991.

12 Matthieu Sozeau and Nicolas Oury. First-class type classes. In OtmaneAit Mohamed, César Muñoz, and Sofiène Tahar, editors, *Theorem Proving in Higher Order Logics*, volume 5170 of *Lecture Notes in Computer Science*, pages 278–293. Springer Berlin Heidelberg, 2008.