Formalizing definition of the rotation number

Yury Kudryashov
DH-3021 3359 Mississauga Road
Mississauga, ON, L5L 1C6
yury.kudriashov@utoronto.ca

University of Toronto Mississauga

Abstract

Rotation number is the key numerical invariant of an orientation preserving circle homeomorphism. This paper describes the current state of an ongoing project with aim to formalize various facts about circle dynamics in Lean. Currently, the formalized material includes the definition and basic properties of the translation number of a lift of a circle homeomorphism to the real line. I also formalized a theorem by É. Ghys that says that two actions of a group on a circle by homeomorphisms are semi-conjugate provided that for some lifts of these actions to the real line, corresponding maps have equal translation numbers.

1 Introduction

Rotation number is an important invariant of a circle homeomorphism. Given an orientation preserving circle homeomorphism $f\colon S^1 \to S^1$, $S^1 = \mathbb{R}/\mathbb{Z}$, and its lift $\tilde{f}\colon \mathbb{R} \to \mathbb{R}$ to the real line, the *translation number* of $\tilde{f}$ is defined as the limit

$$\tau(\tilde{f}) = \lim_{n\to\infty} \frac{f^n(x) - x}{n}. \tag{1}$$

Here and below $f^n(x) = \underbrace{(f \circ \cdots \circ f)}_{n \text{ times}}(x)$. The limit exists for all x and does not depend on x. The *rotation number* of f is defined as $\tau(\tilde{f}) \mod \mathbb{Z}$. Here are a few properties of the rotation number:

- It is a topological invariant: if two homeomorphisms are (semi-)conjugate by a monotone circle map, then their rotation numbers are equal. Moreover, if two homeomorphisms have the same rotation number, then they are semi-conjugate.
- The rotation number $\tau(f)$ is rational if and only if f has a periodic point. More precisely, $\tau(\tilde{f}) = \frac{p}{q}$ if and only if $\tilde{f}^q(x) = x + p$ for some x.
- (Denjoy) If f is a C^2-smooth diffeomorphism of the circle and $\tau(f)$ is irrational, then f is conjugate to the pure rotation $x \mapsto x + \tau(f)$.
- (Hermann, Yoccoz) If f is a C^k-smooth diffeomorphism, $k \geq 3$, $f' > 0$, $\tau(f)$ satisfies the Diophantine condition of order δ, and $k > 2\delta + 1$, then for all $\varepsilon > 0$, f is $C^{k-1-\delta-\varepsilon}$-conjugate to the pure rotation $x \mapsto x + \tau(f)$.

In: A. Editor, B. Coeditor (eds.): Proceedings of the XYZ Workshop, Location, Country, DD-MMM-YYYY, published at http://ceur-ws.org

`Mathlib` [1, 3] is a project aimed to formalize lots of real-world mathematics in the Lean proof assistant (currently we use a community fork of Lean 3; we are working on migration to Lean 4). This paper describes an ongoing project that aims to add various facts about dynamical systems on the circle to `mathlib`. As a first milestone, I formalized the definition of the translation number and all lemmas from [2] that do not use homologies. In particular, I formalized the following theorem.

Theorem 1 ([2, Proposition 5.4]) *Let f_1 and f_2 be two actions of the same group G on the circle by orientation-preserving homeomorphisms. Let $\tilde{f}_1$ and $\tilde{f}_2$ be their lifts to actions on the real line. Suppose that for all $g \in G$ we have $\tau(\tilde{f}_1(g)) = \tau(\tilde{f}_2(g))$. Then these two actions are semi-conjugate: there exists a monotone map $h\colon \mathbb{R} \to \mathbb{R}$, $h(x+1) = h(x) + 1$, such that $h(f_1(g)(x)) = f_2(g)(h(x))$ for all x and g.*

As far as I know, this is the only available formalization of the translation number and its basic properties.

2 Design choices

There are many different ways to formalize the definition and basic properties of the translation number. In this section I describe some design choices I made while working on the project.

2.1 Do not require continuity

Classical texts define rotation number for a circle *homeomorphism*. However, sometimes it is convenient to deal with discontinuous and/or non-strictly monotone maps. E.g., if one takes the flow $\dot{x} = 1$, $\dot{y} = \sqrt{2}$ on the 2-torus, and performs a surgery that replaces a flow box with a Cherry cell, then the Poincaré map of the new flow will be discontinuous at one point, see **??**. It turns out that the definition is still correct and many basic properties are still true in these weaker settings.

2.2 Deal with lifts to the real line right away

While mathematical papers tend to formulate theorems in terms of homeomorphisms of the circle, many theorems actually deal with the lifts of these homeomorphisms to the real line anyway. So, I have decided to give all the basic definitions for a monotone map $f\colon \mathbb{R} \to \mathbb{R}$ such that $f(x+1) = f(x)+1$. This way one can avoid formalizing definitions of a circular order, of a monotone function $f\colon S^1 \to S^1$ etc.

Combined, these two decisions lead us to the main structure.

```
structure circle_deg1_lift : Type :=
(to_fun : ℝ → ℝ)
(monotone' : monotone to_fun)
(map_add_one' : ∀ x, to_fun (x + 1) = to_fun x + 1)
```

2.3 Homeomorphisms as units

The type `circle_deg1_map` is a monoid with multiplication given by composition. Invertible elements of this monoid are exactly orientation-preserving homeomorphisms, so I use `f : units circle_deg1_map` whenever I need `f` to be a lift of a circle homeomorphism. Probably, this decision will be changed in favor of a dedicated structure once more theorems that require continuity will be formalized.

2.4 DRY: dealing with $\leq$ and $\geq$

One of the basic lemmas about lifts of circle maps says that $f(x) \geq x+n$, $n \in \mathbb{Z}$, implies $f^k(x) \geq x + k * n$ for all $k \in \mathbb{N}$, and similarly for $\leq$. In order to avoid repeating the same proofs twice, most of these lemmas are proved for a pair of commuting maps $f, g\colon \alpha \to \alpha$, where α is any linear order, then specialized to the case $\alpha = \mathbb{R}$, $g(x) = x + 1$. This way we can reuse the proofs about $\geq$ in theorems about $\leq$. In mathlib it is done using the `order_dual` type tag: `order_dual` α is the type α with all inequalities reversed.

2.5 Definition of the translation number

The sequence (1) converges as $\sim \frac{1}{n}$, and the proof of the fact that it is a Cauchy sequence is a bit tricky. So, I first define $\tau(f)$ as the limit of the sequence $a_n = 2^{-n} f^{2^n}(0)$. It is easy to show that this sequence converges because f^{2^m} is an iterate of f^{2^n} for $m > n$. Then I prove that $\tau(f^n) = n * \tau(f)$ and $\tau(f) = \tau(g)$ whenever f is semiconjugate to g, and deduce that the sequence (1) converges to $\tau(f)$ for any x.

3 Proof of É. Ghys's theorem

As with many proofs in `mathlib`, Theorem 1 is formalized in more general settings than the original theorem. Namely, let α be a *conditionally complete lattice* (e.g., $\mathbb{R}$) and f_1, f_2 be two actions of a group G on α by order-preserving permutations. Suppose that each set $s(x) = \{ f_1(g)^{-1}(f_2(g)(x)) \mid g \in G \}$ is bounded above. Then the map $S(x) = \operatorname{Sup} s(x)$ semiconjugates each $f_2(g)$ to $f_1(g)$. This version is almost trivial.

In order to deduce the original version from this one, we show that the equality $\tau(f_1(g)) = \tau(f_2(g))$ implies that $f_1(g)^{-1}(f_2(g)(x)) \leq x + 2$ for all real x and all g. This inequality follows from basic properties of $\tau(f)$. The actual proof also needs several lines to jump between an action by `circle_deg1_lift`'s and an action by `order_iso`'s.

4 Future plans

4.1 Rotation number

While dealing with lifts of circle self-maps to the real line is a nice trick that allowed me to formalize quite a few properties of the translation number without proving that a map $f : S^1 \to S^1$ *can be lifted* to $\tilde{f} : \mathbb{R} \to \mathbb{R}$, I definitely have plans to formalize this fact (of course, for any covering, not only for $\mathbb{R} \to S^1$).

4.2 More theorems

While the currently formalized properties work as a proof-of-concept that this approach works, there are lots of classical theorems about dynamics on the circle that have to be formalized before one can say that we have a rich library about circle dynamics. Probably the most famous theorems are Denjoy's and Yoccoz's theorems mentioned in the introduction.

As for the *tools*, the next goal is to formalize the renormalization technique. This method is widely used to prove properties of circle diffeomorphisms, circle homeomorphisms with breaks, and circle critical maps. The idea is to take a point $p \in S^1$ and two consequents $\frac{p_{n-1}}{q_{n-1}}$, $\frac{p_n}{q_n}$ of the continued fraction for $\tau(f)$, then consider the first return map for f on $[f^{q_{n-1}}(p), f^{q_n}(p)]$ and rewrite it in the affine coordinate z such that $z(f^{q_{n-1}}(p)) = -1$, $z(p) = 0$. In many cases, the sequence of renormalized maps converges, and this convergence implies many properties of the original maps and of maps that conjugate two homeomorphisms.

References

[1] F. van Doorn, G. Ebner, and R. Lewis. "Maintaining a Library of Formal Mathematics". In: Intelligent Computer Mathematics, CICM 2020 (2020).

[2] É. Ghys. "Groupes d'homeomorphismes du cercle et cohomologie bornee". In: *The Lefschetz centennial conference* (Mexico City, 1984). .III. Contemp. Math. 58. Providence, RI: Amer. Math. Soc., 1987, pp. 81–106. DOI: 10.1090/conm/058.3/893858.

[3] The mathlib community. "The Lean mathematical library". In: *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020* (New Orleans, LA, USA, Jan. 20–21, 2020).