EasyChair Preprint

№ 6168

Formalizing Rotation Number and Its Properties in Lean

Yury Kudryashov

July 27, 2021

Formalizing rotation number and its properties in Lean

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 gives a necessary and sufficient condition for two actions of a group on the circle by homeomorphism to be semiconjugate to each other.

1 Introduction

1.1 Dynamical systems

A dynamical system with a discrete time is a single self-map $f\colon X \to X$ of a topological space X, together with its iterations $f^n = \underbrace{(f \circ \dots \circ f)}_{n \text{ times}}$. The space X is called the *phase space* of the system. This notion can be generalized to continuous actions of general semigroups on X, see Sec. 1.3.

Here are some basic questions about a dynamical system.

- What are the periodic orbits and fixed points of f?
- What is the limit behaviour of (all, generic) orbits $\{ f^n(x) \mid n \in \mathbb{N} \}$ of f? Do they converge to some of the periodic orbits? If yes, at what rate? Are the orbits dense in the phase space?
- When two maps have "essentially the same" dynamics?

To answer the last question, we need two definitions. We say that maps $f\colon X \to X$ and $g\colon Y \to Y$ are *semiconjugate* by a map $h\colon X \to Y$ if $h \circ f = g \circ h$. If h is a homeomorphism, then we say that it *conjugates* f to g. The main difference between a semiconjugacy and a conjugacy is that in case of a semiconjugacy, the map h can glue together some regions in X and can leave some regions in Y out of its range (hence, out of its "sight"). It is easy to see that a map h (semi)conjugating f to g sends orbits, periodic orbits, and fixed points of f to orbits, periodic orbits, and fixed points of g. One can think about two conjugate maps as the same map written in two different charts. If the conjugating map h is a smooth diffeomorphism, then the conjugacy preserves even more

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

information, including the rate of convergence of orbits. So, it is natural to ask the following question: *when two self-maps are semiconjugate/conjugate/conjugate by a diffeomorphism*? In case of circle self-maps, some partial answers to this question are given in the next subsection.

1.2 Circle self-maps

Circle self-maps $f\colon S^1 \to S^1$, $S^1 = \mathbb{R}/\mathbb{Z}$, constitute an important class of dynamical systems. They appear in applications, e.g., as Poincaré maps of continuous flows on the 2-torus.

The simplest circle self-maps are pure rotations $x \mapsto x + a$. It turns out that any circle homeomorphism f is semiconjugate to a pure rotation $x \mapsto x + \tau(f)$. The number $\tau(f)$ is called the *rotation number* of f.

Here is an explicit construction of $\tau(f)$. Consider a lift $\tilde{f}\colon \mathbb{R} \to \mathbb{R}$ of f to the real line. The *translation number* of $\tilde{f}$ is defined to be the limit

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

The limit exists for all x and does not depend on x. The *rotation number* of f is defined as $\tau(\tilde{f}) \mod \mathbb{Z}$. The motivation behind this definition is that $\frac{f^n(x)-x}{n}$ counts the average number of full turns a point makes per application of f.

Here are a few simple properties of the rotation number.

- The rotation number of the pure rotation $x \mapsto x + a$ equals a.
- $\tau(f \circ g) = \tau(f) + \tau(g)$ whenever f commutes with g; $\tau(f^n) = n\tau(f)$.
- The points of an orbit $\{ f^n(x) \}$ go in the same non-strict circular order as the points of an orbit of $x \mapsto x + \tau(f)$. In particular, $\lfloor f^n(x) - x \rfloor \le n\tau(f) \le \lceil f^n(x) - s \rceil$.
- The rotation number 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. In particular, every circle homeomorphism f is semi-conjugate to the pure rotation $x \mapsto x + \tau(f)$.
- 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.

Let us also formulate a couple of non-trivial theorems about rotation numbers and conjugacy.

Theorem 1 ([Den32]) *Let f be a C^2-smooth circle diffeomorphism with an irrational rotation number. Then f is conjugate to the pure rotation $x \mapsto x + \tau(f)$ by a circle homeomorphism.*

Theorem 2 ([Den32]) *For every rotation number τ there exists a C^1-smooth circle diffeomorphism f with rotation number τ that is not conjugate to the pure rotation $x \mapsto x + \tau$ by a circle homeomorphism.*

Theorem 3 ([Her79; Yoc84]) *Let f be a C^k-smooth diffeomorphism, $k \ge 3$. Suppose that $f'(x) > 0$ for all x, $\tau(f)$ satisfies the Diophantine condition of order δ, and $k > 2\delta + 1$. Then for all $\varepsilon > 0$, f is conjugate to the pure rotation $x \mapsto x + \tau(f)$ by a $C^{k-1-\delta-\varepsilon}$-smooth diffeomorphism.*

The latter theorem implies that two circle diffeomorphisms with the same rotation number that satisfies the Diophantine condition are smoothly conjugate, hence they have essentially the same dynamical properties.

1.3 Group actions on the circle

A *group action* $F\colon G \curvearrowright X$of a group G on a set X is a homomorphism from G to the group of permutations of X. In other words, it is a map $F\colon G \to X \to X$ such that $F(1)$ is the identity map and $F(gh) = F(g) \circ F(h)$. Two actions $F_1\colon G \curvearrowright X$ and $F_2\colon G \curvearrowright Y$ are *(semi)conjugate* by $h\colon X \to Y$ if $F_1(g)$ is semiconjugate to $F_2(g)$ by h for any $g \in G$.

Denote by $\mathrm{Homeo}_+(S^1)$ the group of orientation preserving homeomorphisms of the circle. Then one can think about group actions $F\colon G \curvearrowright S^1$ by orientation preserving homeomorphisms as homomorphisms $F\colon G \xrightarrow{*} \mathrm{Homeo}_+(S^1)$. Here the star above the arrow means that the map is a homomorphism between multiplicative groups. This loosely follows `mathlib` notation $\to^*$.

I formalize two theorems about group actions on the circle by orientation preserving homeomorphisms. It is clear that the relation "there exists a homeomorphism conjugating F_1 to F_2" is an equivalence relation. It turns out that in the case of the circle, the same is true for semiconjugacy.

Theorem 4 ([Ghy87, Proposition 2.1]) *The following relation is an equivalence relation on the space $G \xrightarrow{*} \mathrm{Homeo}_+(S^1)$: $F_1 \sim F_2$ if there exists a monotonically increasing circle self-map h that semiconjugates F_1 to F_2.*

Another theorem gives a necessary and sufficient condition for two group actions to be semiconjugate. The condition is formulated in terms of the *bounded cohomologies* of a group, see next subsection.

1.4 Bounded cohomologies

Bounded cohomologies with integer coefficients $H_b^n(G, \mathbb{Z})$ of a group are defined in the same way as usual cohomologies with the additional requirement that all cochains in the definition have bounded range. Following [Ghy87], consider the 2-cocycle $e \in H_b^2(\mathrm{Homeo}_+(S^1), \mathbb{Z})$ given by $e(f, g) = \lfloor f(g(0)) \rfloor - \lfloor f(0) \rfloor - \lfloor g(0) \rfloor$. This is a cocycle because it is the coboundary of the unbounded cochain $f \mapsto \lfloor f(0) \rfloor$. One can show that this cocycle takes values in $\{ 0, 1 \}$, hence it is indeed a bounded cocycle.

The main theorem of [Ghy87] states that two group actions $F_1, F_2 \colon G \to \mathrm{Homeo}_+(S^1)$ are semiconjugate by a monotone map if and only if $F_1^* e$ equals $F_2^* e$ in $H_b^2(G, \mathbb{Z})$.

Theorem 5 ([Ghy87, Theorem A.1]) *Let F_1, F_2 be two actions of a group G on the circle S^1 by orientation preserving homeomorphisms. Let $e \in H_b^2(\mathrm{Homeo}_+(S^1), \mathbb{Z})$ be the cocycle defined in Sec. 1.4. Then F_1 is semiconjugate to F_2 by an increasing circle self-map if and only if $F_1^* e = F_2^* e$.*

The same theorem can be reformulated without mentioning cohomologies.

Theorem 6 ([Ghy87, Theorem A.1]) *Let F_1, F_2 be two actions of a group G on the circle S^1 by orientation preserving homeomorphisms. Let $e \in H_b^2(\mathrm{Homeo}_+(S^1), \mathbb{Z})$ be the cocycle defined in Sec. 1.4. Then F_1 is semiconjugate to F_2 by an increasing circle self-map if and only if there exists a bounded map $n \colon G \to \mathbb{Z}$ such that for any two $f, g \in G$ we have $e(F_1(f), F_1(g)) - e(F_2(f), F_2(g)) = n(fg) - n(f) - n(g)$.*

1.5 Mathlib and formalization

`Mathlib` [DEL20; TMC20] 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, a bunch of simple properties including those listed in Sec. 1.2, and most statements from [Ghy87]. In particular, I formalized Theorem 4 and Theorem 6.

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 Figure 1. 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.

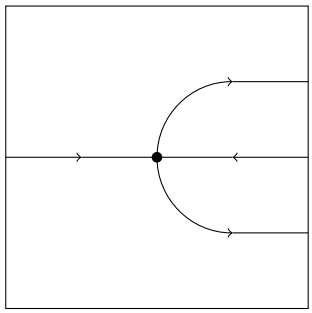

Figure 1: A vector field with a Cherry cell

```
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)
```

Some theorems need to deal with the monoid of monotone circle self-maps, so I define the congruence (i.e., an equivalence relation that respects the multiplication) "$f \sim g \Leftrightarrow \exists n \in \mathbb{Z}, \forall x, f(x) = g(x) + n$" and deal with the quotient space.

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 $|a_n - a_{n+1}| < \frac{1}{2^{n+1}}$, hence this sequence converges and $|f(0) - \tau(f)| \leq 1$. Then I prove that $\tau(f^n) = n\tau(f)$, thus $|f^n(0) - n\tau(f)| \leq 1$, therefore (1) converges to $\tau(f)$ for $x = 0$. Finally, $\tau(f) = \tau(g)$ whenever f is semiconjugate to g; in particular, $\tau(f) = \tau(T_x \circ f \circ T_{-x})$, where $T_a(b) = a + b$, hence (1) converges to $\tau(f)$ for any x.

3 Proof of É. Ghys's theorem

As with many proofs in `mathlib`, Theorem 4 is formalized in more general settings than the original theorem. In this case I formalized it for order isomorphisms of a *conditionally complete lattice*. Recall that a type α with a partial order is called a *lattice* if it has two binary operations join/sup $\sqcup$ and meet/inf $\sqcap$ and they satisfy natural axioms like $a \sqcap b \leq a$ and $a \sqcup b \leq c \iff a \leq c \wedge b \leq c$, see mathlib definition for the complete list of axioms. A lattice is said to be *conditionally complete* if every nonempty bounded above set s has the least upper bound $\operatorname{Sup} s$. Examples of conditionally complete lattices include $\mathbb{R}$, the type of functions $\alpha \to \mathbb{R}$ etc.

Let α be a conditionally complete lattice, let β is a type with a partial order. Let $h\colon \alpha \to \beta$ be a map such that $\{ x \mid h(x) \leq y \}$ is nonempty and bounded above for every y. If h semiconjugates an order automorphism $f\colon \alpha \to \alpha$ to an order embedding $g\colon \beta \to \beta$, then the map $y \mapsto \operatorname{Sup} \{ x \mid h(x) \leq y \}$ semiconjugates g to f.

In case of `h : circle_deg1_lift`, I define the inverse map h^{-1} to be $y \mapsto \operatorname{Sup} \{ x \mid h(x) \leq y \}$, so theorem says that h^{-1} semiconjugates `g : units circle_deg1_lift` to `f : units circle_deg1_lift` whenever h semiconjugates f to g.

As for Theorem 6, the proof closely follows the original paper. The main difference is that at the time I started the project, `mathlib` had no theory of group cohomologies, so I reformulated all statements without the notion of cohomologies. Sometimes this leads to ugly code that definitely should be rewritten once we have a usable theory of group cohomologies in Lean.

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 $f\colon S^1 \to S^1$ *can be lifted* to $\tilde{f}\colon \mathbb{R} \to \mathbb{R}$, 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

[DEL20] F. van Doorn, G. Ebner, and R. Lewis. "Maintaining a Library of Formal Mathematics". In: Intelligent Computer Mathematics, CICM 2020 (2020).

[Den32] A. Denjoy. "Sur les courbes definies par les équations différentielles à la surface du tore". French. In: *Journal de Mathématiques Pures et Appliquées*. 9th ser. 11 (1932), pp. 333–375.

[Ghy87] 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.

[Her79] M. R. Herman. « Sur la Conjugaison Différentiable des Difféomorphismes du Cercle a des Rotations ». Français. In : *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* 49.1 (1979), p. 5-233.

[TMC20] 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).

[Yoc84] J.-C. Yoccoz. « Conjugaison différentiable des difféomorphismes du cercle dont le nombre de rotation vérifie une condition diophantienne ». Français. In : *Annales scientifiques de l'É.N.S.* 4e sér. 17.3 (1984), p. 333-359.