A formal proof in Coq of LaSalle's invariance principle

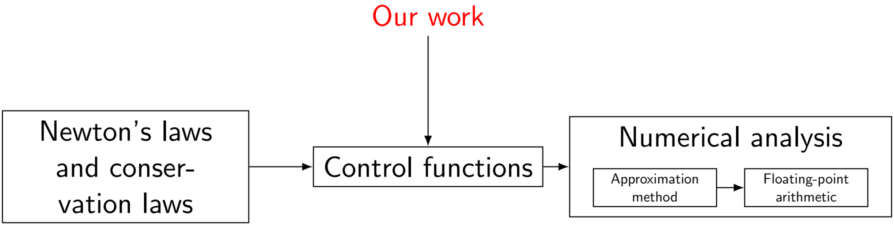
Cyril Cohen & Damien Rouhling

Université Côte d'Azur, Inria, France

September 29, 2017

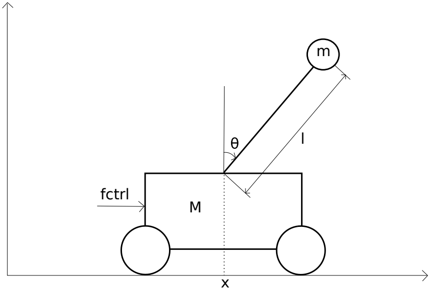
Motivations

- Robotics raises security issues.
- Control theory brings answers, for instance on how to make a robot reach a certain state thanks to a control function.
- We want to certify that such a function actually reaches its goal.



Our goal

- The inverted pendulum is a standard example for testing control functions.



- Goal: stabilize the pendulum on its unstable equilibrium thanks to the control function fctrl.
- Our plan: formalize the proof of stability in [LFB00].

Context

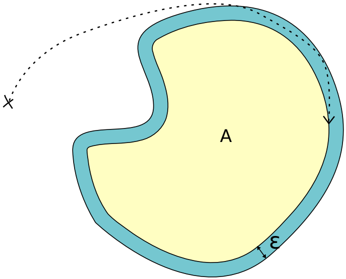
- Our concern is to prove the (asymptotic) stability of a robot.
- Robots are often modeled as dynamical systems defined by systems of differential equations.
- Lyapunov functions and LaSalle's invariance principle [LaS60] are major tools for proving the asymptotic stability of solutions to a system of differential equations in $\mathbb{R}^n$:

$$\dot{y} = F \circ y.$$

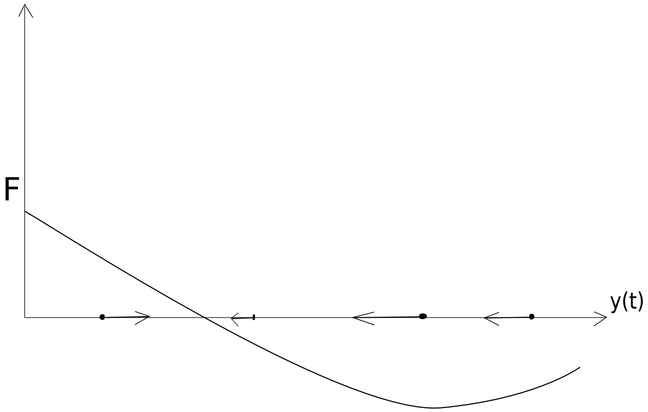
Preliminary definitions

- A set A is said to be invariant if every solution to $\dot{y} = F \circ y$ starting in A (i.e. $y(0) \in A$) remains in A.
- A function of time $y(t)$ approaches a set A as t approaches infinity, denoted by $y(t) \to A$ as $t \to +\infty$, if

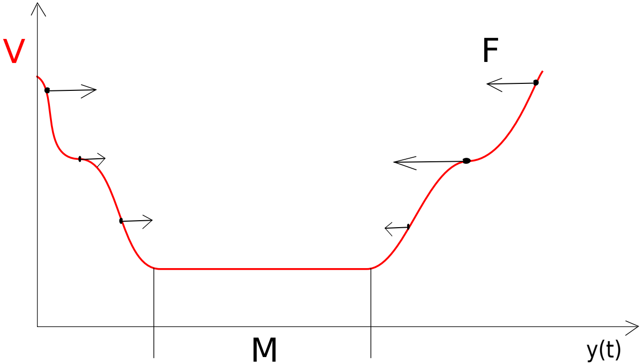
$$\forall \varepsilon > 0, \exists T > 0, \forall t > T, \exists p \in A, \|y(t) - p\| < \varepsilon.$$



LaSalle's invariance principle for real functions



LaSalle's invariance principle for real functions

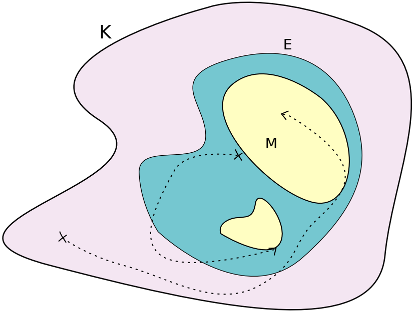


LaSalle's invariance principle [LaS60]

Assume

- $F(0) = 0$
- F has continuous first partial derivatives
- K compact and invariant
- $V : \mathbb{R}^n \to \mathbb{R}$ has continuous first partial derivatives in K
- $\tilde{V}(p) \leqslant 0$ in K where $\tilde{V}(p) := (dV_p \circ F)(p)$
- $E := \left\{ p \in K \mid \tilde{V}(p) = 0 \right\}$
- $M :=$ largest invariant set in E

Then for every solution y starting in K, $y(t) \to M$ as $t \to +\infty$.

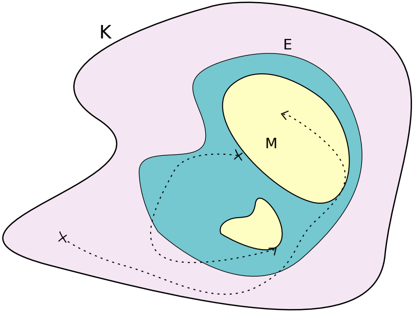


Generalization of LaSalle's invariance principle

Assume

- $\cancel{F(0) = 0}$
- F has continuous first partial derivatives
- K compact and invariant
- $V : \mathbb{R}^n \to \mathbb{R}$ has continuous first partial derivatives in K
- $\tilde{V}(p) \leqslant 0$ in K where $\tilde{V}(p) := (dV_p \circ F)(p)$
- $E := \left\{ p \in K \mid \tilde{V}(p) = 0 \right\}$
- $M :=$ largest invariant set in E

Then for every solution y starting in K, $y(t) \to M$ as $t \to +\infty$.

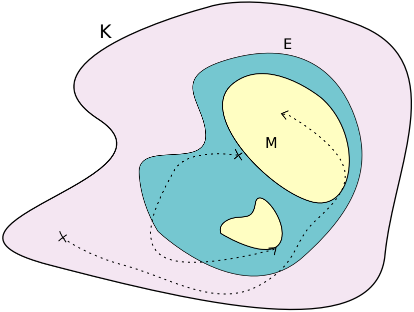


Generalization of LaSalle's invariance principle

Assume

- F has continuous first partial derivatives
- K compact and invariant
- $V : \mathbb{R}^n \to \mathbb{R}$ has continuous first partial derivatives in K
- $\tilde{V}(p) \leqslant 0$ in K where $\tilde{V}(p) := (dV_p \circ F)(p)$
- $E := \left\{ p \in K \mid \tilde{V}(p) = 0 \right\}$
- $M :=$ largest invariant set in E

Then for every solution y starting in K, $y(t) \to M$ as $t \to +\infty$.

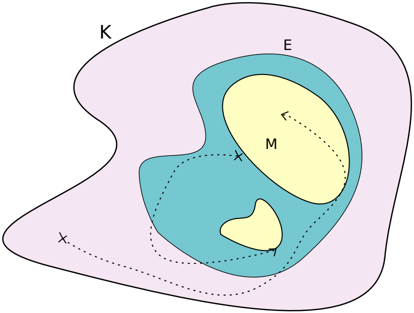


Generalization of LaSalle's invariance principle

Assume

- F is such that we have the existence and uniqueness of solutions to $\dot{y} = F \circ y$ and the continuity of solutions relative to initial conditions in K
- K compact and invariant
- $V : \mathbb{R}^n \to \mathbb{R}$ has continuous first partial derivatives in K
- $\tilde{V}(p) \leqslant 0$ in K where $\tilde{V}(p) := (dV_p \circ F)(p)$
- $E := \left\{p \in K \mid \tilde{V}(p) = 0\right\}$
- $M :=$ largest invariant set in E

Then for every solution y starting in K, $y(t) \to M$ as $t \to +\infty$.

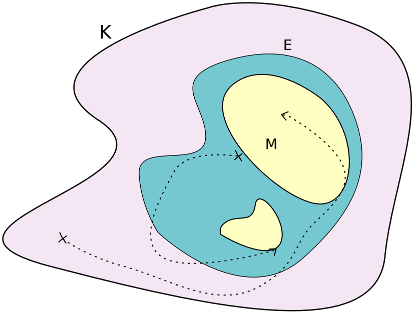


Generalization of LaSalle's invariance principle

Assume

- F is such that we have the existence and uniqueness of solutions to $\dot{y} = F \circ y$ and the continuity of solutions relative to initial conditions in K
- K compact and invariant
- $V : \mathbb{R}^n \to \mathbb{R}$ is differentiable in K
- $\tilde{V}(p) \leqslant 0$ in K where $\tilde{V}(p) := (dV_p \circ F)(p)$
- $E := \left\{ p \in K \mid \tilde{V}(p) = 0 \right\}$
- $M :=$ largest invariant set in E

Then for every solution y starting in K, $y(t) \to M$ as $t \to +\infty$.



The positive limiting set

Definition

Let y be a function of time. The positive limiting set of y, denoted by $\Gamma^+(y)$, is the set of all points p such that

$$\forall \varepsilon > 0, \forall T > 0, \exists t > T, \|y(t) - p\| < \varepsilon.$$

In other terms, $\Gamma^+(y)$ is the set of limit points of y at infinity.

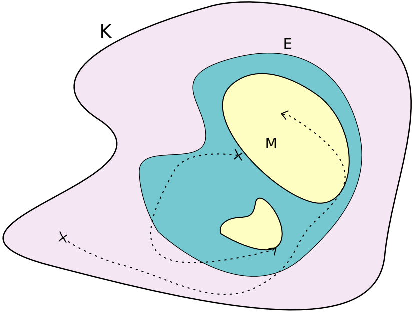
Remark: a function with values (ultimately) in a compact set converges to its positive limiting set as time goes to infinity.

The result we proved

Assume

- F is such that we have the existence and uniqueness of solutions to $\dot{y} = F \circ y$ and the continuity of solutions relative to initial conditions in K
- K compact and invariant
- $V : \mathbb{R}^n \to \mathbb{R}$ is differentiable in K
- $\tilde{V}(p) \leqslant 0$ in K where $\tilde{V}(p) := (dV_p \circ F)(p)$
- $E := \left\{ p \in K \mid \tilde{V}(p) = 0 \right\}$
- $M :=$ largest invariant set in E

Then for every solution y starting in K, $y(t) \to M$ as $t \to +\infty$.

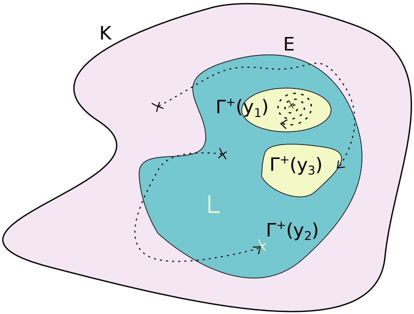


The result we proved

Assume

- F is such that we have the existence and uniqueness of solutions to $\dot{y} = F \circ y$ and the continuity of solutions relative to initial conditions in K
- K compact and invariant
- $V : \mathbb{R}^n \to \mathbb{R}$ is differentiable in K
- $\tilde{V}(p) \leqslant 0$ in K where $\tilde{V}(p) := (dV_p \circ F)(p)$
- $E := \left\{ p \in K \mid \tilde{V}(p) = 0 \right\}$
- $L := \bigcup_{\substack{y \text{ solution} \\ \text{starting in } K}} \Gamma^+(y)$

Then, L is an invariant subset of E and for all solution y starting in K, $y(t) \to L$ as $t \to +\infty$.



Formalization

- Formalization in Coq + SSReflect.
- Libraries: Mathematical Components and Coquelicot.
- Classical reasoning was needed.
- Around 1250 lines of code:
  - Around 1000 lines for notations, topological notions and extensions of Coquelicot.
  - Around 250 lines for properties on positive limiting sets and the actual proof of LaSalle's invariance principle.

Filter-based convergence

- A set of sets F is a filter if
  - $F \neq \emptyset$.
  - $\forall (P, Q) \in F^2, P \cap Q \in F$.
  - $\forall P \in F, \forall Q \supseteq P, Q \in F$.
- We use COQUELICOT's filters [BLM15].
- Examples:
  - Neighbourhood filter of a point p, written `locally` p.
  - Neighbourhood filter of $+\infty$, written `Rbar_locally +oo`.
  - Image of a filter `F` by a function `y`:
    `y @ F` $:= \{A \mid \mathtt{y}^{-1}(A) \in \mathtt{F}\}$.
- Filter inclusion: `F --> G` $:=$ `G` $\subseteq$ `F`.
- Convergence: written `y @ p --> q` thanks to filter inference via canonical structures, instead of
  `filterlim y (locally p) (locally q)` in COQUELICOT.

Filter-based convergence (cont.): generalization to sets

- Generalization of balls: $B_\varepsilon(A) := \bigcup_{p \in A} B_\varepsilon(p)$.
- Generalization of the neighbourhood filter: $\texttt{locally\_set}\ A\ B := \exists \varepsilon > 0, B_\varepsilon(A) \subseteq B$.

```
Lemma locally_set1P p A :
  locally p A <-> locally_set [set p] A.
```

- Convergence: written `y @ +oo --> A` or `y @ p --> A` as for convergence to a point.

Clustering

Clustering generalizes to filters the notion of limit point.

$$\texttt{cluster}\ F := \{p \in U \mid \forall A \in F, \forall B \text{ neighbourhood of } p, A \cap B \neq \emptyset\}$$

Clustering is a central notion in our work.

- Clustering allows us to express compactness in terms of filters.
- Clustering can be used to define positive limiting sets.
- Hausdorff separability can be defined in terms of clustering.

Clustering and limit points

$$\Gamma^+(y) := \{p \mid \forall \varepsilon > 0, \forall T > 0, \exists t > T, \|y(t) - p\| < \varepsilon\}.$$

```
Definition pos_limit_set (y : R -> U) := ...

Lemma plim_set_cluster (y : R -> U) :
  pos_limit_set y = cluster (y @ +oo).
```

Filter-based compactness

A is compact iff every proper filter on A clusters in A.

```
Definition compact (A : set U) := forall (F : set (set U)),
  F A -> ProperFilter F -> A `&` cluster F !=set0.
```

- No subspace topology required.
- Convenient for proofs on convergence and limit points.
- Not adapted for proofs on other notions, such as boundedness.

```
Lemma compactP A : compact A <-> quasi_compact A.
```

Differential equations

- Differential equation $\dot{y} = F \circ y$.

```
Definition is_sol (y : R -> U) :=
  forall t, is_derive y t (F (y t)).
```

- Existence and uniqueness of solutions.

```
Variable sol : U -> R -> U.
Hypothesis sol0 : forall p, sol p 0 = p.
Hypothesis solP :
  forall y, K (y 0) -> is_sol y <-> y = sol (y 0).
```

- Continuity of the solutions relative to initial conditions.

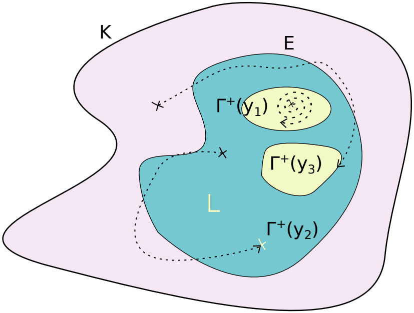
```
Hypothesis sol_cont :
  forall t, continuous_on K (sol^~ t).
```

LaSalle's invariance principle stated

Assume

- F is such that we have the existence and uniqueness of solutions to $\dot{y} = F \circ y$ and the continuity of solutions relative to initial conditions in K
- K compact and invariant
- $V : \mathbb{R}^n \to \mathbb{R}$ is differentiable in K
- $\tilde{V}(p) \leqslant 0$ in K where $\tilde{V}(p) := (dV_p \circ F)(p)$
- $E := \left\{ p \in K \mid \tilde{V}(p) = 0 \right\}$
- $L := \bigcup\limits_{\substack{y \text{ solution} \\ \text{starting in } K}} \Gamma^+(y)$

Then, L is an invariant subset of E and for all solution y starting in K, $y(t) \to L$ as $t \to +\infty$.



LaSalle's invariance principle stated

$$L := \bigcup_{\substack{y \text{ solution} \\ \text{starting in } K}} \Gamma^+(y) = \texttt{limS K}.$$

```
Definition limS (A : set U) :=
  \bigcup_(q in A) cluster (sol q @ +oo).

Lemma invariant_limS A : A `<=` K -> is_invariant (limS A).

Lemma stable_limS (V : U -> R) (dV : U -> U -> R) :
  (forall p : U, K p -> filterdiff V (locally p) (dV p)) ->
  (forall p : U, K p -> (dV p \o F) p <= 0) ->
  limS K `<=` [set p | (dV p \o F) p = 0].

Lemma cvg_to_limS (A : set U) :
  compact A -> is_invariant A ->
  forall p, A p -> sol p @ +oo --> limS A.
```

Conclusion

- A refined version of LaSalle's invariance principle formalized.
- A first step towards a certified control function for the stabilization of the inverted pendulum.
- Filters are convenient, but not for everything.

Further remarks:

- Set theoretic notations and functional/propositional extensionality make proofs closer to textbook mathematics.
- Using a relational description of differentiability instead of a functional one is painful.

Teaser

- Generalization of the notion of solution and of our version of LaSalle's invariance principle.
- Automated derivation/differentiation via type classes.
- The inverted pendulum formalized.

Teaser

- Generalization of the notion of solution and of our version of LaSalle's invariance principle.
- Automated derivation/differentiation via type classes.
- The inverted pendulum formalized.

Thank you!

Bibliography

Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond.
Coquelicot: A User-Friendly Library of Real Analysis for Coq.
Mathematics in Computer Science, 9(1):41–62, 2015.

J. LaSalle.
Some Extensions of Liapunov's Second Method.
IRE Transactions on Circuit Theory, 7(4):520–527, Dec 1960.

R. Lozano, I. Fantoni, and D.J. Block.
Stabilization of the inverted pendulum around its homoclinic orbit.
Systems & Control Letters, 40(3):197–204, 2000.

Hausdorff spaces

```
Definition hausdorff U :=
  forall p q : U, cluster (locally p) q -> p = q.

Lemma hausdorffP U : hausdorff U <-> forall p q : U,
  p <> q -> exists A B, locally p A /\ locally q B /\
    forall r, ~ (A `&` B) r.
```

Classical reasoning

- Closed sets via closures.

```
Lemma closedP (A : set U) :
  closed A <-> closure A `<=` A.
```

- Filter-based compactness.

```
Lemma compactP A : compact A <-> quasi_compact A.
```

- Hausdorff spaces via clusters.

```
Lemma hausdorffP U : hausdorff U <-> forall p q : U,
  p <> q -> exists A B, locally p A /\ locally q B /\
    forall r, ~ (A `&` B) r.
```

- Convergence of a function to its positive limiting set.

```
Lemma cvg_to_pos_limit_set y (A : set U) :
  (y @ +oo) A -> compact A ->
  y @ +oo --> cluster (y @ +oo).
```

- Monotonic bounded real functions converge.

Canonical structures for filter inference

Three structures:

- `canonical_filter_on`: to cast a term to a filter.
- `canonical_filter`: to recognize types whose elements can be casted to filters.
- `canonical_filter_source`: to infer a filter from the source of an arrow type.