# A formal proof in Coq of LaSalle's invariance principle

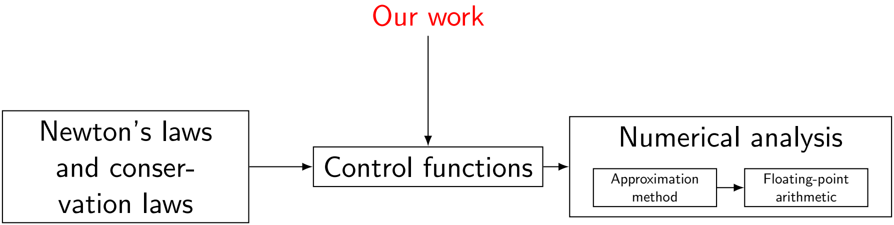
Cyril Cohen & Damien Rouhling

Université Côte d'Azur, Inria, France

May 29, 2017

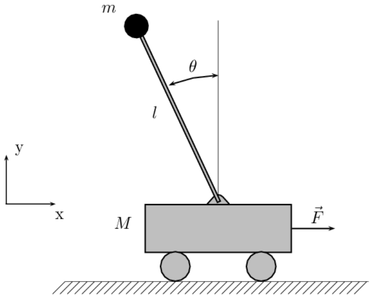
# Motivations

- 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 F.
- Our plan: formalize the proof of stability in [LFB00].

# Context

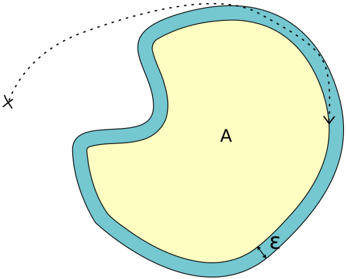
- Our concern is to prove the (asymptotic) stability of a robot.
- Robots are often modeled as dynamical systems defined by systems of differential equations.
- LaSalle's invariance principle [LaS60] is a major tool for proving the asymptotic stability of solutions to a system of differential equations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

$$\dot{x} = X \circ x.$$

# Preliminary definitions

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

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



# LaSalle's invariance principle [LaS60]

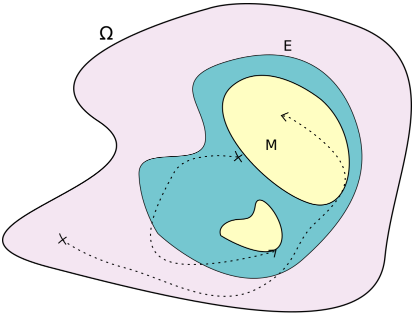
**Theorem (LaSalle's invariance principle)**

Assume $X$ has continuous first partials and $X(0) = 0$. Let $\Omega$ be an invariant compact set. Suppose there is a scalar function $V$ which has continuous first partials in $\Omega$ and is such that $\tilde{V}(p) \leqslant 0$ in $\Omega$. Let $E$ be the set of all points $p \in \Omega$ such that $\tilde{V}(p) = 0$. Let $M$ be the largest invariant set in $E$.
Then for every solution $x$ starting in $\Omega$, $x(t) \to M$ as $t \to +\infty$.

$$\tilde{V}(p) = \langle (\text{grad } V)(p), X(p) \rangle = (dV_p \circ X)(p)$$

# LaSalle's invariance principle [LaS60]

- $\Omega$ compact and invariant
- $V : \mathbb{R}^n \to \mathbb{R}$
- $\tilde{V}(p) = (dV_p \circ X)(p)$
- $\tilde{V}(p) \leqslant 0$ in $\Omega$
- $E = \left\{ p \in \Omega \mid \tilde{V}(p) = 0 \right\}$
- $M =$ largest invariant set in $E$



# The positive limiting set

**Definition**

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

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

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

# The result we proved

**Theorem**

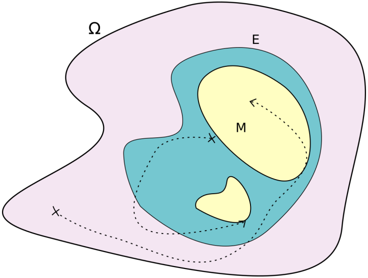
Assume $X$ is such that we have the existence and uniqueness of solutions to $\dot{x} = X \circ x$ and the continuity of solutions relative to initial conditions. Let $\Omega$ be an invariant compact set. Suppose there is a scalar function $V$, differentiable in $\Omega$. Suppose $\tilde{V}(p) \leqslant 0$ in $\Omega$. Let $E$ be the set of all points $p \in \Omega$ such that $\tilde{V}(p) = 0$. Let $L$ be the union of all $\Gamma^+(x)$ for $x$ solution starting in $\Omega$.

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

$$\tilde{V}(p) = (dV_p \circ X)(p)$$

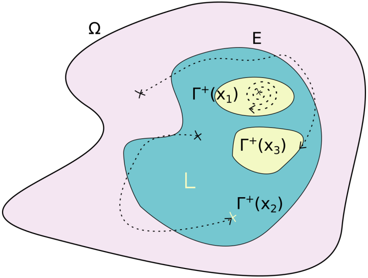
# The result we proved

LaSalle's version:




$M =$ largest invariant set in $E$

Our version:




$$L = \bigcup_{\substack{x \text{ solution} \\ \text{starting in } \Omega}} \Gamma^+(x)$$

$L$ is invariant

- $\Omega$ compact and invariant
- $\tilde{V}(p) = (dV_p \circ X)(p)$
- $\tilde{V}(p) \leqslant 0$ in $\Omega$
- $E = \left\{ p \in \Omega \mid \tilde{V}(p) = 0 \right\}$

# Formalization

- Formalization in Coq + SSReflect.
- Libraries: Mathematical Components and Coquelicot.
- Classical reasoning was needed.
- Around 1300 lines of code:
  - Around 1100 lines for notations, topological notions and extensions of Coquelicot.
  - Around 200 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 $p$:
    `locally` $p = \{N \mid \exists \varepsilon > 0, B_\varepsilon(p) \subseteq N\}$.
  - Neighbourhood filter of $+\infty$:
    `Rbar_locally +oo` $= \{N \mid \exists M, [M, +\infty) \subseteq N\}$.
  - Image of a filter `F` by a function `x`:
    `x @ F` $= \{A \mid \{p \mid$ `x` $p \in A\} \in$ `F`$\}$.
- Filter inclusion: `F --> G` $=$ `G` $\subseteq$ `F`.
- Convergence: written `x @ p --> q` thanks to filter inference via canonical structures.

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

- Generalization of balls: $B_\varepsilon(A) = \bigcup_{p \in A} B_\varepsilon(p)$.

```
Definition ball_set (A : set U) (eps : posreal) :=
  \bigcup_(p in A) ball p eps.
```

- Generalization of the neighbourhood filter:
  `locally_set` $A\ B = \exists \varepsilon > 0, B_\varepsilon(A) \subseteq B$.

```
Definition locally_set (A : set U) :=
  [set B | exists eps : posreal,
           ball_set A eps `<=` B].
Lemma locally_set1P p A :
  locally p A <-> locally_set [set p] A.
```

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

```
Lemma cvg_to_set1P x p :
  x @ +oo --> [set p] <-> x @ +oo --> p.
```

# Clustering

Clustering generalizes to filters the notion of limit point.

```
Definition cluster (F : set (set U)) (p : U) :=
  forall A B, F A -> locally p B -> A :&: B !=set0
```

Clustering is a central notion in our work.

- Clustering can be used to define positive limiting sets.
- Clustering allows us to express compactness in terms of filters (for $\Omega$).
- Hausdorff separability can be defined in terms of clustering.

# Clustering and limit points

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

```
Definition pos_limit_set (x : R -> U) :=
  \bigcap_(eps : posreal) \bigcap_(T : posreal)
    [set p | Rlt T `&` (x @^-1` ball p eps) !=set0].

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

# Filter-based compactness

```
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 $\dot{x} = X \circ x$.

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

- Existence and uniqueness of solutions.

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

- Continuity of the solutions relative to initial conditions.

```
Hypothesis sol_cont :
  forall t, forall p, continuous (sol^~ t) p.
```

# LaSalle's invariance principle stated

**Theorem**

Assume $X$ is such that we have the existence and uniqueness of solutions to $\dot{x} = X \circ x$ and the continuity of solutions relative to initial conditions. Let $\Omega$ be an invariant compact set. Suppose there is a scalar function $V$, differentiable in $\Omega$, such that $\tilde{V}(p) \leqslant 0$ in $\Omega$. Let $E$ be the set of all points $p \in \Omega$ such that $\tilde{V}(p) = 0$ and $L$ be the union of all $\Gamma^+(x)$ for $x$ solution starting in $\Omega$.
Then, $L$ is an invariant subset of $E$ and for all solution $x$ starting in $\Omega$, $x(t) \to L$ as $t \to +\infty$.

$$\tilde{V}(p) = (dV_p \circ X)(p)$$

# LaSalle's invariance principle stated

$\Omega =$ `S` and $L =$ `limS S`.

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

Lemma invariant_limS S : is_invariant (limS S).

Lemma stable_limS (S : set U) (V : U -> R)
  (V' : U -> U -> R) : compact S -> is_invariant S ->
  (forall p : U, S p -> filterdiff V (locally p) (V' p)) ->
  (forall p : U, S p -> (V' p \o X) p <= 0) ->
  limS S `<=` [set p | (V' p \o X) p = 0].

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

# 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.
- The absence of a function similar to `Derive` for differentials is painful.
- The axiomatization of real numbers is not powerful enough for proofs on least upper bounds.

# 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.
- The absence of a function similar to `Derive` for differentials is painful.
- The axiomatization of real numbers is not powerful enough for proofs on least upper bounds.

**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 x (A : set U) :
  (x @ +oo) A -> compact A ->
  x @ +oo --> cluster (x @ +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.