Formal Verification of Station Keeping Maneuvers for a Planar Autonomous Hybrid System

Benjamin Martin[1] Khalil Ghorbal[2] Eric Goubault[1] Sylvie Putot[1]

[1]LIX, École Polytechnique, CNRS, Université Paris - Saclay
[2]INRIA, Rennes

19 September 2017
Formal Verification of Autonomous Vehicles Workshop, Torino

Research partially supported by the DGA MRIS

Outline

Station Keeping

Station keeping maneuver

Move towards a given position in space in finite time, and stays around it for an indefinite amount of time.

Station Keeping

Station keeping maneuver

Move towards a given position in space in finite time, and stays around it for an indefinite amount of time.

Safety property

Station Keeping

Station keeping maneuver

Move towards a given position in space in finite time, and stays around it for an indefinite amount of time.

Safety property and Liveness property.

Station Keeping

Station keeping maneuver

Move towards a given position in space in finite time, and stays around it for an indefinite amount of time.

Safety property and Liveness property.
Case study taken from [Jaulin, 2013]: Maneuver interesting for autonomous sailboats, UAV, etc ... Vehicles that cannot stay idle.

Station Keeping

Station keeping maneuver

Move towards a given position in space in finite time, and stays around it for an indefinite amount of time.

Safety property and Liveness property.
Case study taken from [Jaulin, 2013]: Maneuver interesting for autonomous sailboats, UAV, etc ... Vehicles that cannot stay idle.

Goal

Prove that a given controller performs a station keeping maneuver.

Dubins vehicle

Consider the model of a 2D Dubins car:

$$\begin{cases} \dot{x} &= \cos(\theta) \\ \dot{y} &= \sin(\theta) \\ \dot{\theta} &= u \end{cases},$$

where (x, y) are the position of the vehicle and θ its heading. The angular velocity of the heading is controlled by u.

Dubins vehicle

Consider the model of a 2D Dubins car:

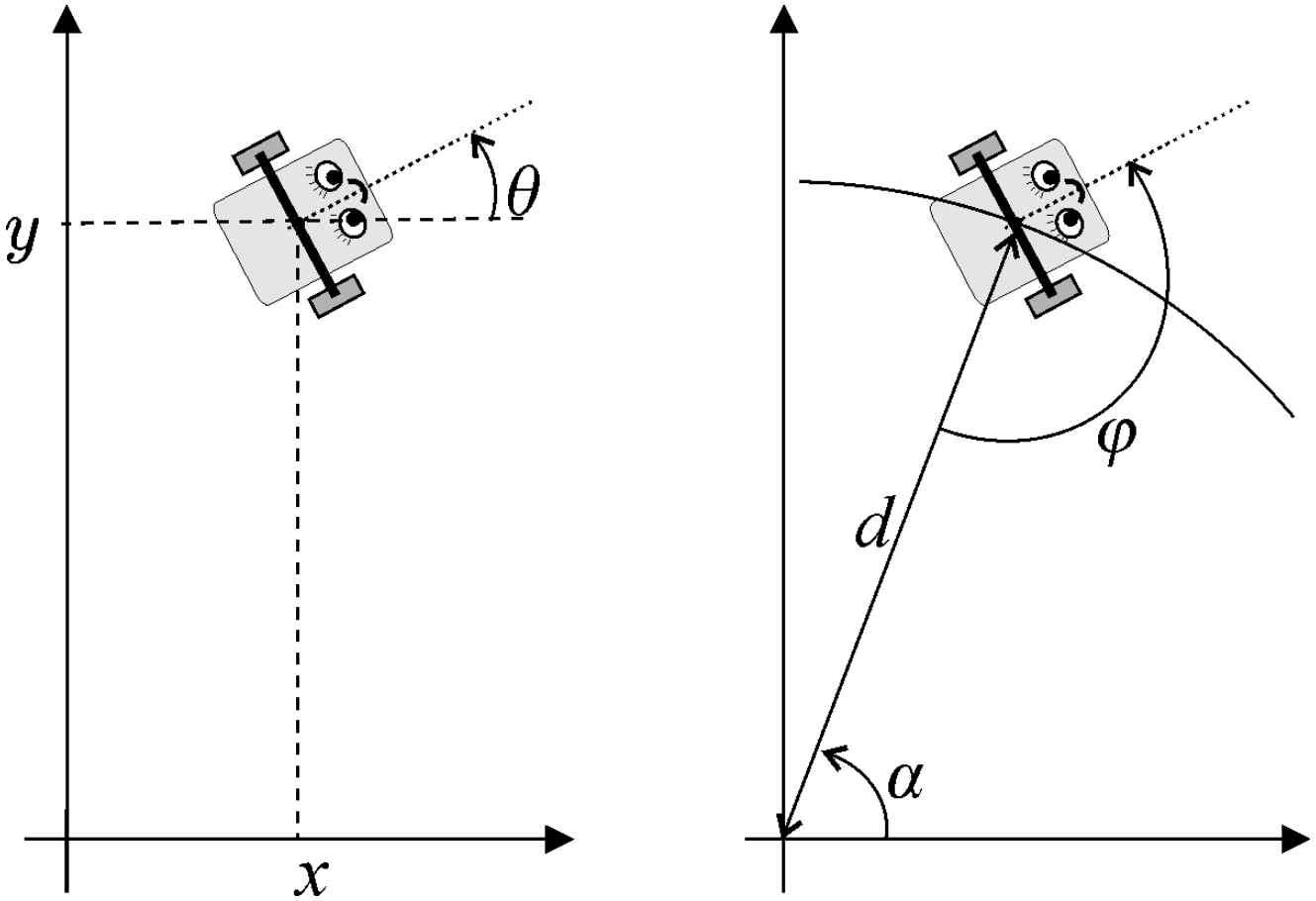
$$\begin{cases} \dot{x} &= \cos(\theta) \\ \dot{y} &= \sin(\theta) \\ \dot{\theta} &= u \end{cases},$$

where (x, y) are the position of the vehicle and θ its heading. The angular velocity of the heading is controlled by u.
Its rewriting in polar coordinates:

$$\begin{cases} \dot{d} &= -\cos(\varphi) \\ \dot{\varphi} &= \frac{\sin(\varphi)}{d} + u \\ \dot{\alpha} &= -\frac{\sin(\varphi)}{d} \end{cases},$$

where (d, α) forms the polar coordinates of the vehicle and φ its bearing w.r.t. the origin. The dynamics of d and φ are independent of α.

Illustration



Courtesy to [Jaulin, 2013]

Controller for a station keeping maneuver

Vehicle moving at constant speed (no possibility to stop)

Controller for a station keeping maneuver

Vehicle moving at constant speed (no possibility to stop)
From [Jaulin, 2013], the following control law has been proposed:

$$u = \begin{cases} 1 & \text{if } \cos(\varphi) \leqslant \frac{\sqrt{2}}{2} \\ -\sin(\varphi) & \text{otherwise} \end{cases},$$

($u = 1 \implies$ Constant control, $u = -\sin(\varphi) \implies$ Proportional control)

Controller for a station keeping maneuver

Vehicle moving at constant speed (no possibility to stop)
From [Jaulin, 2013], the following control law has been proposed:

$$u = \begin{cases} 1 & \text{if } \cos(\varphi) \leqslant \frac{\sqrt{2}}{2} \\ -\sin(\varphi) & \text{otherwise} \end{cases},$$

($u = 1 \implies$ Constant control, $u = -\sin(\varphi) \implies$ Proportional control)

Question

Does this controller perform certainly a station keeping maneuver ?

Related work

In [Jaulin, 2013], a guaranteed numerical approach (based on interval analysis) is proposed:

- Interval quantization of the state space
- subject to limitations of numerical approaches (failure to prove some invariance properties)
- final result not very "accurate"

Related work

In [Jaulin, 2013], a guaranteed numerical approach (based on interval analysis) is proposed:

- Interval quantization of the state space
- subject to limitations of numerical approaches (failure to prove some invariance properties)
- final result not very "accurate"

How about an algebraic approach ?

- recent advances in algebraic methods for constructing invariants [Goubault et al., 2014, Ghorbal and Platzer, 2014]
- hybrid programs and theorem prover `Keymaera X` [Platzer, 2008] and some of its recent successes (e.g. [Loos et al., 2013])

A polynomial model and hybrid program

A polynomial transformation to work with algebraic methods:

$$(Plant)\begin{cases} \dot{g} &= -(he+u)h \\ \dot{h} &= (he+u)g \\ \dot{e} &= ge^2 \\ \dot{d} &= -g \\ \dot{\varphi} &= he+u \end{cases},$$

where $\cos(\varphi) \to g$, $\sin(\varphi) \to h$ and $\frac{1}{d} \to e$. Requires to keep relations between new variables: $h^2 + g^2 = 1$ and $de = 1$. We assume the initial state to satisfy $\Delta = d > 0 \wedge h^2 + g^2 - 1 \wedge de = 1$.

A polynomial model and hybrid program

A polynomial transformation to work with algebraic methods:

$$(Plant)\begin{cases} \dot{g} &= -(he+u)h \\ \dot{h} &= (he+u)g \\ \dot{e} &= ge^2 \\ \dot{d} &= -g \\ \dot{\varphi} &= he+u \end{cases},$$

where $\cos(\varphi) \to g$, $\sin(\varphi) \to h$ and $\frac{1}{d} \to e$. Requires to keep relations between new variables: $h^2 + g^2 = 1$ and $de = 1$. We assume the initial state to satisfy $\Delta = d > 0 \wedge h^2 + g^2 - 1 \wedge de = 1$.

Hybrid Program

$$\alpha := \left\{ \begin{array}{l} \{\text{Plant}_{|u=1} \ \& \ d > 0 \wedge 2g \leqslant \sqrt{2}\} \ \cup \\ \{\text{Plant}_{|u=-h} \ \& \ d > 0 \wedge 2g > \sqrt{2}\} \end{array} \right\}^*$$

Outline

Invariants and Darboux polynomials

Let $\dot{x} = f(x)$ denotes an ODE.

Invariant

A set $S \subseteq \mathbb{R}^n$ is *positive invariant* for f iff $\forall \boldsymbol{x}_0 \in S$, the solution $\phi(\boldsymbol{x}_0, \cdot)$ satisfies $\phi(\boldsymbol{x}_0, t) \in S$, $\forall t \in [0, +\infty) \cap I$.

Invariants and Darboux polynomials

Let $\dot{x} = f(x)$ denotes an ODE.

Invariant

A set $S \subseteq \mathbb{R}^n$ is *positive invariant* for f iff $\forall \boldsymbol{x}_0 \in S$, the solution $\phi(\boldsymbol{x}_0, \cdot)$ satisfies $\phi(\boldsymbol{x}_0, t) \in S$, $\forall t \in [0, +\infty) \cap I$.

Darboux polynomial

A polynomial p is *Darboux* for f iff

$$\dot{p} := \langle \nabla p, f \rangle = cp$$

where $c \in \mathbb{R}[x]$ is a polynomial.

(Well known fact: if p is Darboux for f then $S := \{x : p(x) \sim 0\}$ is invariant for f)

Rational invariants

Control	Darboux Polynomial	Cofactor
$u = 1$	e	ge
	$1 + 2eh$	$2ge$
$u = -h$	e	ge
	h	$(e-1)g$

(Can be obtained algorithmically, up to a (small) fixed degree, see [Matringe et al., 2010, Ghorbal and Platzer, 2014])

Rational invariants

Control	Darboux Polynomial	Cofactor
$u = 1$	e^2	$2ge$
	$1 + 2eh$	$2ge$
$u = -h$	e	ge
	h	$(e-1)g$

(Can be obtained algorithmically, up to a (small) fixed degree, see [Matringe et al., 2010, Ghorbal and Platzer, 2014])

Rational invariants

Control	Darboux Polynomial	Cofactor
$u = 1$	e^2	$2ge$
	$1 + 2eh$	$2ge$
$u = -h$	e	ge
	h	$(e-1)g$

(Can be obtained algorithmically, up to a (small) fixed degree, see [Matringe et al., 2010, Ghorbal and Platzer, 2014])

Where $u = 1$,

$$\frac{1 + 2eh}{e^2},$$

is a rational invariant function for the ODE ($p = 1 + 2eh$ and $q = e^2$, we have $\dot{p}q - p\dot{q} = 0$).

Rational invariants

Control	Darboux Polynomial	Cofactor
$u = 1$	e^2	$2ge$
	$1 + 2eh$	$2ge$
$u = -h$	e	ge
	h	$(e-1)g$

(Can be obtained algorithmically, up to a (small) fixed degree, see [Matringe et al., 2010, Ghorbal and Platzer, 2014])

Where $u = 1$,

$$\frac{1 + 2eh}{e^2},$$

is a rational invariant function for the ODE ($p = 1 + 2eh$ and $q = e^2$, we have $\dot{p}q - p\dot{q} = 0$).

Special case of [Goubault et al., 2014].

Invariant in constant control

Rational invariant function in constant control

$$V_{cst} := \frac{1 + 2eh}{e^2}.$$

Assuming $d > 0$ (hence $de = 1$), then $V_{cst} = d^2 + 2dh$.
In proportional control ($u = -h$), $\dot{V}_{cst} = -2g(h+1)d$, which is negative where it is applied ($g > 0$ and $h \in [-1, 1]$).

Invariant in constant control

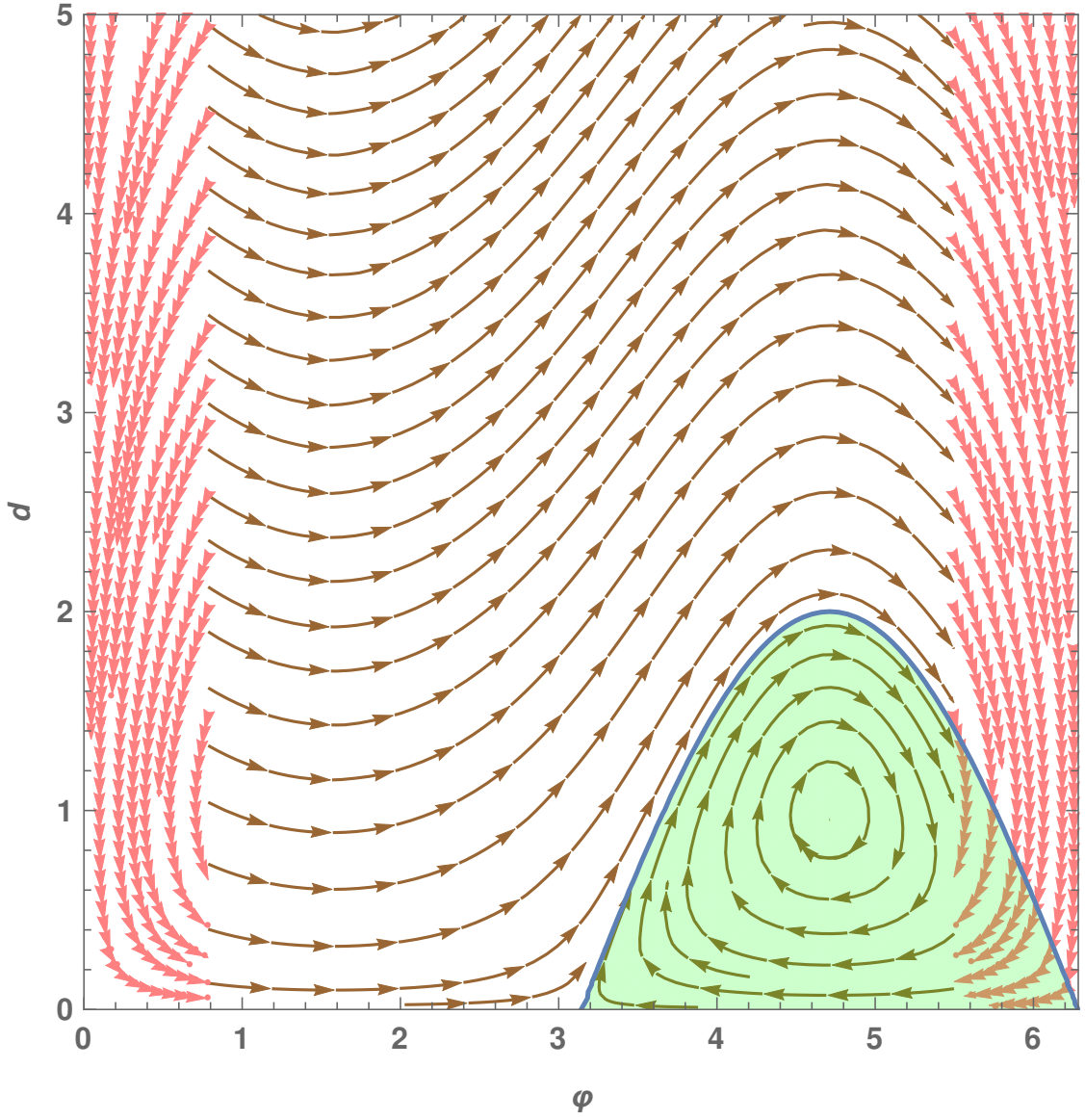
Rational invariant function in constant control

$$V_{cst} := \frac{1 + 2eh}{e^2}.$$

Assuming $d > 0$ (hence $de = 1$), then $V_{cst} = d^2 + 2dh$.
In proportional control ($u = -h$), $\dot{V}_{cst} = -2g(h+1)d$, which is negative where it is applied ($g > 0$ and $h \in [-1, 1]$).

Candidate invariant set for the hybrid system

$$\mathcal{V}_s := \{x : V_{cst}(x) <= s\}, \forall s$$



$\mathcal{V}_0$

Assisting the proof with Keymaera X

Theorem ($V_{cst} \leqslant 0$ is a Positive Invariant)

$$V_{cst} \leqslant 0 \ \wedge \ \Delta \rightarrow \ [\alpha] \ V_{cst} \leqslant 0$$

Assisting the proof with Keymaera X

Proof Result

✔ All goals in your proof agenda have been closed.

Provable

```
NoProofTermProvable(Provable(  ==>  sqrt2^2=2&sqrt2>0&g^2+h^2=1&d*e
=1&d>0&d^2+2*d*h<=0->[{{g'=-(h*e-h)*h,h'=(h*e-h)*g,phi'=h*e-h,e'=g*
e^2,d'=-g&sqrt2*g>=1&d*e=1&d>0}++{g'=-(h*e+1)*h,h'=(h*e+1)*g,phi'=h
*e+1,d'=-g,e'=g*e^2&sqrt2*g<=1&d*e=1&d>0}}*]d^2+2*d*h<=0 proved))
```

Tactic to Reproduce the Proof

```
implyR(1) ; loop({`d^2+2*d*h<=0&h^2+g^2=1`}, 1) ; <(
QE,
QE,
choiceb(1) ; andR(1) ; <(
dC({`h^2+g^2=1`}, 1) ; <(
  dI(1),
    dI(1)
  ),
  dI(1)
)
```

Download tactic | Download lemma | Download archive | Close

Assisting the proof with Keymaera X

Theorem ($V_{cst} \leqslant 0$ is a Positive Invariant)

$$V_{cst} \leqslant 0 \ \wedge \ \Delta \rightarrow \ [\alpha] \ V_{cst} \leqslant 0$$

Proof mostly based on the DI rule:

$$(DI)\frac{\forall x.([x' := f(x)]\dot{p} \leqslant 0)}{p \leqslant 0 \rightarrow [\dot{x} = f(x) \& H]p \leqslant 0}$$

Outline

Reaching the singular case $d = 0$

Starting at $\varphi_0 = 0[2\pi]$ $(u = -h)$ and $d_0 > 0$,

$$\begin{cases} \dot{g} & = & 0 \\ \dot{h} & = & 0 \\ \dot{e} & = & e^2 \\ \dot{d} & = & -1 \\ \dot{\varphi} & = & 0 \end{cases},$$

Reaching the singular case $d = 0$

Starting at $\varphi_0 = 0[2\pi]$ $(u = -h)$ and $d_0 > 0$,

$$\begin{cases} \dot{g} &= 0 \\ \dot{h} &= 0 \\ \dot{e} &= e^2 \\ \dot{d} &= -1 \\ \dot{\varphi} &= 0 \end{cases},$$

$\Longrightarrow$ System that diverges in finite time with respect to e and converge to $d = 0$. Singularity at $d = 0$ and solution not defined for all $t \geqslant 0$.

Reaching the singular case $d = 0$

Starting at $\varphi_0 = 0[2\pi]$ $(u = -h)$ and $d_0 > 0$,

$$\begin{cases} \dot{g} &= 0 \\ \dot{h} &= 0 \\ \dot{e} &= e^2 \\ \dot{d} &= -1 \\ \dot{\varphi} &= 0 \end{cases},$$

$\Longrightarrow$ System that diverges in finite time with respect to e and converge to $d = 0$. Singularity at $d = 0$ and solution not defined for all $t \geqslant 0$.

Polar coordinates issue

The vehicle moves exactly towards the origin $(\varphi = 0)$, reaches the origin and then follows the dynamic at a new states where $\varphi \sim \pi[2\pi]$ and $d > 0$. Jump on the state φ.

Generic case and hybrid program

We assume that $\varphi > 0$, i.e. $h \neq 0 \vee g < 1$, and that the solutions are defined for all $t \in [0, +\infty)$.

Theorem ($V_{cst} \leqslant 0$ is reachable in finite time)

$$\Delta \rightarrow \langle \alpha \rangle \; V_{cst} \leqslant 0$$

Generic case and hybrid program

We assume that $\varphi > 0$, i.e. $h \neq 0 \vee g < 1$, and that the solutions are defined for all $t \in [0, +\infty)$.

Theorem ($V_{cst} \leqslant 0$ is reachable in finite time)

$$\Delta \rightarrow \langle \alpha \rangle \; V_{cst} \leqslant 0$$

Liveness deduction rule from [Sogokon and Jackson, 2015]:

$$(\mathrm{SP})\,\frac{\begin{array}{c} \vdash \exists \epsilon > 0.\ \forall x.\ S \rightarrow (p \geqslant 0 \wedge \dot{p} \leqslant -\epsilon) \\ \vdash S \rightarrow [\dot{x} = f(x)\ \&\ \neg(H \wedge X_T)]S \\ X_0 \wedge \neg X_T \vdash S \qquad\qquad X_0 \vee S \vdash H \end{array}}{\vdash X_0 \rightarrow \langle \dot{x} = f(x)\ \&\ H \rangle X_T}$$

S is a staging set.

Generic case and hybrid program

We assume that $\varphi > 0$, i.e. $h \neq 0 \vee g < 1$, and that the solutions are defined for all $t \in [0, +\infty)$.

Theorem ($V_{cst} \leqslant 0$ is reachable in finite time)

$$\Delta \rightarrow \langle \alpha \rangle \; V_{cst} \leqslant 0$$

Liveness deduction rule from [Sogokon and Jackson, 2015]:

$$(\mathrm{SP})\,\frac{\begin{array}{c} \vdash \exists \epsilon > 0.\ \forall x.\ S \rightarrow (p \geqslant 0 \wedge \dot{p} \leqslant -\epsilon) \\ \vdash S \rightarrow [\dot{x} = f(x)\ \&\ \neg(H \wedge X_T)]S \\ X_0 \wedge \neg X_T \vdash S \qquad\qquad X_0 \vee S \vdash H \end{array}}{\vdash X_0 \rightarrow \langle \dot{x} = f(x)\ \&\ H \rangle X_T}$$

S is a staging set. Rule not yet implemented in `Keymaera X`. Direct application is tedious: need to decompose the proof.

Building a chain of staging sets and progress functions

Decomposition of the (generic) state space into:

$$① := 0 < \varphi < \frac{\pi}{4} \ \wedge \ d > 0$$

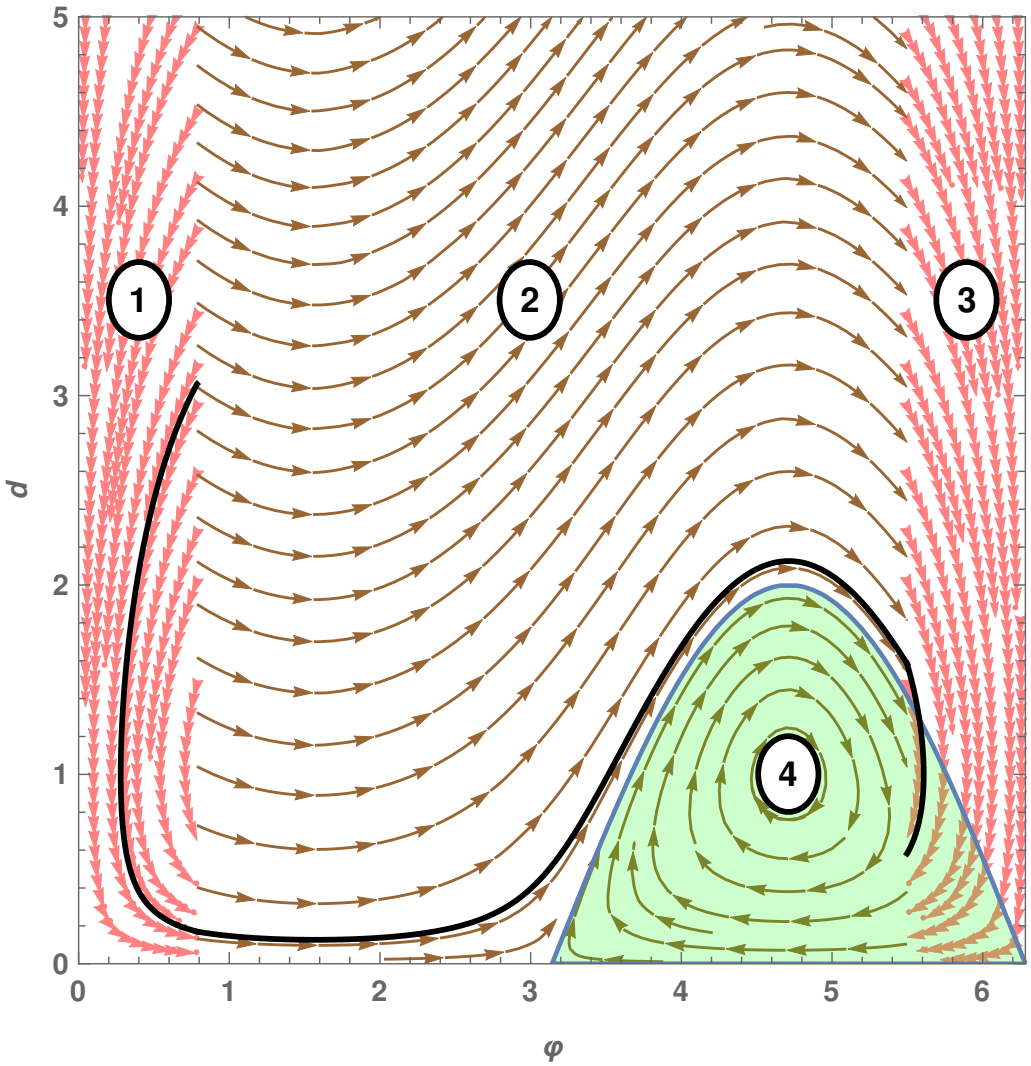
$$② := \frac{\pi}{4} \leqslant \varphi \leqslant \frac{7\pi}{4} \ \wedge \ d > 0 \ \wedge \ V_{cst} > 0$$

$$③ := \frac{7\pi}{4} < \varphi < 2\pi \ \wedge \ d > 0 \ \wedge \ V_{cst} > 0$$

$$④ := V_{cst} \leqslant 0$$

Building a chain of staging sets and progress functions

Decomposition of the (generic) state space into:



Building a chain of staging sets and progress functions

Decomposition of the (generic) state space into:

$$① := 0 < \varphi < \frac{\pi}{4} \ \wedge \ d > 0$$

$$② := \frac{\pi}{4} \leqslant \varphi \leqslant \frac{7\pi}{4} \ \wedge \ d > 0 \ \wedge \ V_{cst} > 0$$

$$③ := \frac{7\pi}{4} < \varphi < 2\pi \ \wedge \ d > 0 \ \wedge \ V_{cst} > 0$$

$$④ := V_{cst} \leqslant 0$$

I. $S = X_0 = ①$, $p = d$, $\epsilon = -\frac{\sqrt{2}}{2}$, $X_T = ②$.
II. $S = X_0 = ②$, $p = -\varphi + \frac{7\pi}{4}$, $\epsilon = -\frac{1}{2}$, $X_T = ③$.
III. $S = X_0 = ③$, $p = d$, $\epsilon = -\frac{\sqrt{2}}{2}$, $X_T = ④$.

Premises $X_0 \wedge \neg X_T \vdash S$ and $X_0 \vee S \vdash H$ are trivially satisfied.

Assisting the proof with Keymaera X ?

Progress functions:

$$\vdash \exists \epsilon > 0.\ \forall x.\ S \rightarrow (p \geqslant 0 \wedge \dot{p} \leqslant -\epsilon)$$

$\Longrightarrow$ We provide ϵ and p. Quantifier elimination over the reals is then enough. The progress function provides an upper bound on the time spent in S.

Assisting the proof with Keymaera X ?

Progress functions:

$$\vdash \exists \epsilon > 0.\ \forall x.\ S \rightarrow (p \geqslant 0 \wedge \dot{p} \leqslant -\epsilon)$$

$\Longrightarrow$ We provide ϵ and p. Quantifier elimination over the reals is then enough. The progress function provides an upper bound on the time spent in S.

Staging set invariance:

$$\vdash S \rightarrow [\dot{x} = f(x)\ \&\ \neg(H \wedge X_T)]S$$

$\Longrightarrow$ requires transformation into a quantifier elimination problem [Liu et al., 2011], procedure not yet implemented in Keymaera X

Assisting the proof with Keymaera X ?

Progress functions:

$$\vdash \exists \epsilon > 0.\ \forall x.\ S \rightarrow (p \geqslant 0 \wedge \dot{p} \leqslant -\epsilon)$$

$\Longrightarrow$ We provide ϵ and p. Quantifier elimination over the reals is then enough. The progress function provides an upper bound on the time spent in S.

Staging set invariance:

$$\vdash S \rightarrow [\dot{x} = f(x)\ \&\ \neg(H \wedge X_T)]S$$

$\Longrightarrow$ requires transformation into a quantifier elimination problem [Liu et al., 2011], procedure not yet implemented in Keymaera X

We have used our own implementation of the latter procedure in Wolfram Mathematica in order to verify the proof.

Result from the chain of invariants

Proposition I.

$$(① \ \wedge \ \Delta) \rightarrow \langle \alpha \rangle \ (②)$$

Proposition II.

$$(② \ \wedge \ \Delta) \rightarrow \langle \alpha \rangle \ (③)$$

Proposition III.

$$(③ \ \wedge \ \Delta) \rightarrow \langle \alpha \rangle \ (④)$$

Result from the chain of invariants

Proposition I.

$$(① \ \wedge \ \Delta) \rightarrow \langle \alpha \rangle \ (②)$$

Proposition II.

$$(② \ \wedge \ \Delta) \rightarrow \langle \alpha \rangle \ (③)$$

Proposition III.

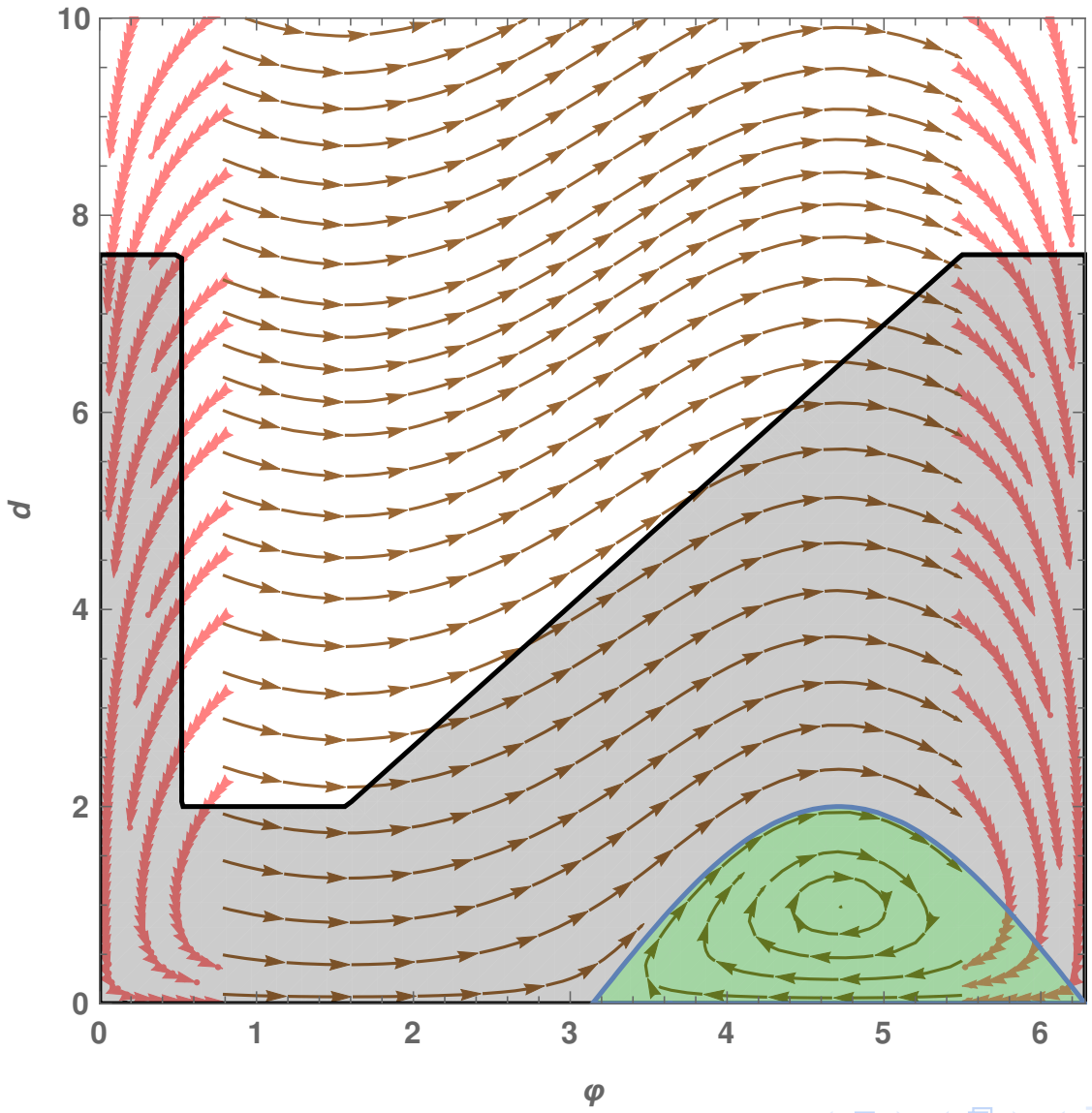
$$(③ \ \wedge \ \Delta) \rightarrow \langle \alpha \rangle \ (④)$$

Theorem (④ is reachable in finite time)

$$\Delta \rightarrow \ \langle \alpha \rangle \ ④$$

Outline

Comparison with [Jaulin, 2013]



Discussion

To conclude:

- A simple case study with an involved formal algebraic proof giving a more accurate analysis than the previous numerical technique
- Recent advances in formal verification are enough for completing the proof
- Possible use of `Keymaera X` as a theorem prover (although currently incomplete)

Discussion

To conclude:

- A simple case study with an involved formal algebraic proof giving a more accurate analysis than the previous numerical technique
- Recent advances in formal verification are enough for completing the proof
- Possible use of `Keymaera X` as a theorem prover (although currently incomplete)

Remaining questions, left for future work:

- How much generic is this proof scheme ? How much is it reusable for the verification of another controller (liveness) ?
- Automatize ?
- What happen when the proof fails ? How to use formal arguments to re-design a new controller ?

References I

[Ghorbal and Platzer, 2014] Ghorbal, K. and Platzer, A. (2014).
Characterizing algebraic invariants by differential radical invariants.
In *TACAS*, pages 279–294. Springer.

[Goubault et al., 2014] Goubault, E., Jourdan, J.-H., Putot, S., and Sankaranarayanan, S. (2014).
Finding non-polynomial positive invariants and Lyapunov functions for polynomial systems through Darboux polynomials.
In *2014 American Control Conference*, pages 3571–3578.

[Jaulin, 2013] Jaulin, L. (2013).
Outer approximation of attractors using an interval quantization.
Reliable Computing, 19:261–273.

References II

[Liu et al., 2011] Liu, J., Zhan, N., and Zhao, H. (2011).
Computing semi-algebraic invariants for polynomial dynamical systems.
In *EMSOFT*, pages 97–106. ACM.

[Loos et al., 2013] Loos, S. M., Renshaw, D., and Platzer, A. (2013).
Formal verification of distributed aircraft controllers.
In *HSCC*, pages 125–130.

[Matringe et al., 2010] Matringe, N., Moura, A. V., and Rebiha, R. (2010).
Generating invariants for non-linear hybrid systems by linear algebraic methods.
In *SAS*, volume 6337 of *LNCS*, pages 373–389. Springer.

References III

[Platzer, 2008] Platzer, A. (2008).
Differential dynamic logic for hybrid systems.
J. Autom. Reasoning, 41(2):143–189.

[Sogokon and Jackson, 2015] Sogokon, A. and Jackson, P. B. (2015).
Direct formal verification of liveness properties in continuous and hybrid dynamical systems.
In *FM*, volume 9109 of *LNCS*, pages 514–531. Springer.

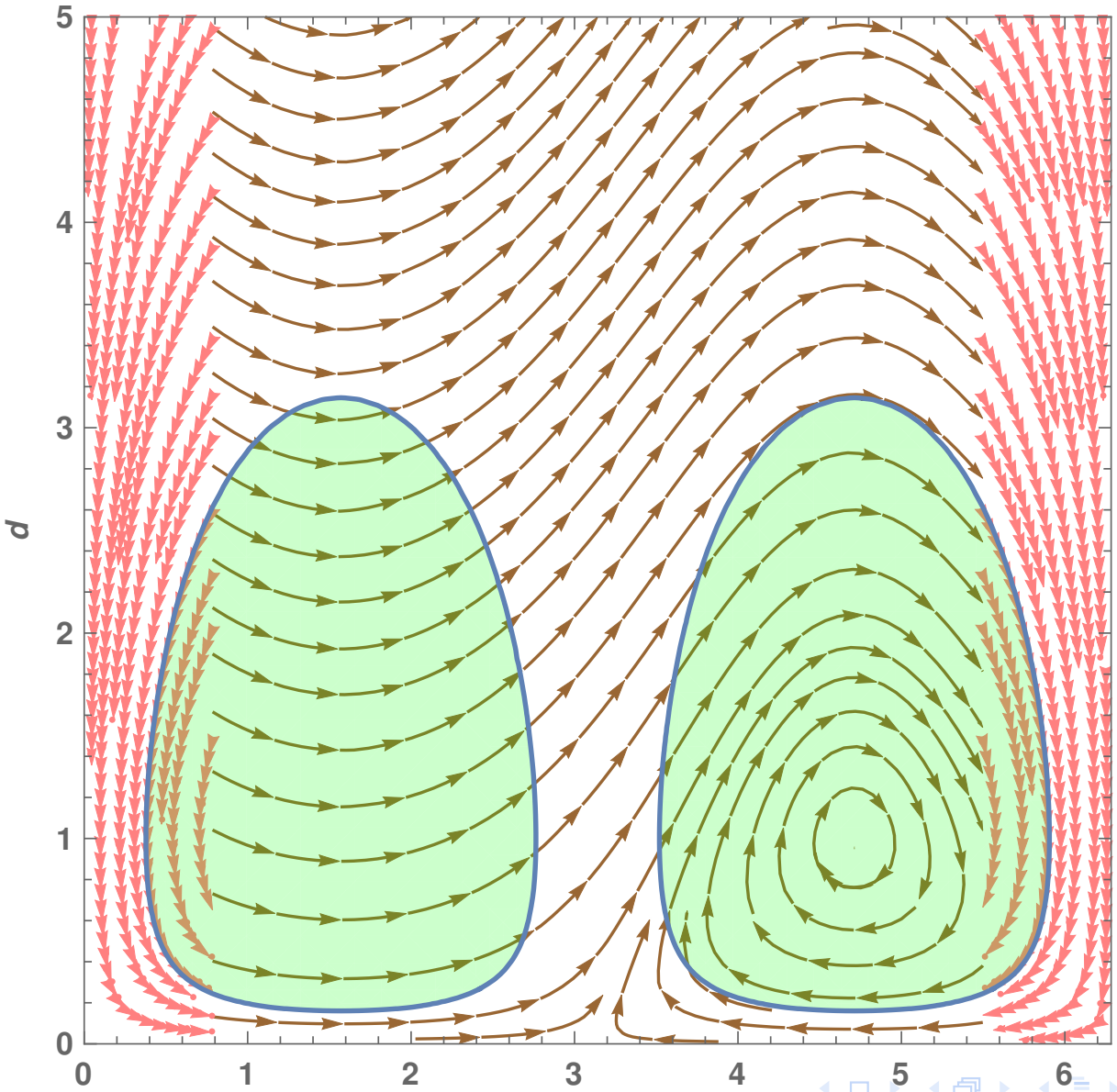
Invariant in Proportional control

From [Goubault et al., 2014], we also have the following logarithmic invariant function in proportional control:

Invariant Logarithmic function ($u = -h$)

$$V_{pro} := \log(d|h|) - d$$

Invariant in Proportional control



Refined Invariant