Nonlinear Forward Invariant Synthesis: A Cone-Based Abstract Interpretation Approach

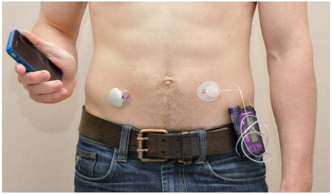
Guillaume Berger*, Masoumeh Ghanbarpour, Sriram Sankaranarayanan

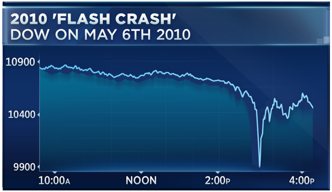
May 15, 2024

University of Colorado Boulder

Table of contents

Safety in Systems and Control





A Formal Definition of System and Safety

Continuous-time system: $\dot{x}(t) = f(x(t))$ for $t \in \mathbb{R}_+$, $x(t) \in \mathbb{R}^n$

Assumption: trajectories are well defined (unique and complete)

Notation: $\phi(t, x)$ trajectory s.t. $\phi(0, x) = x$, at time $t \in \mathbb{R}_+$

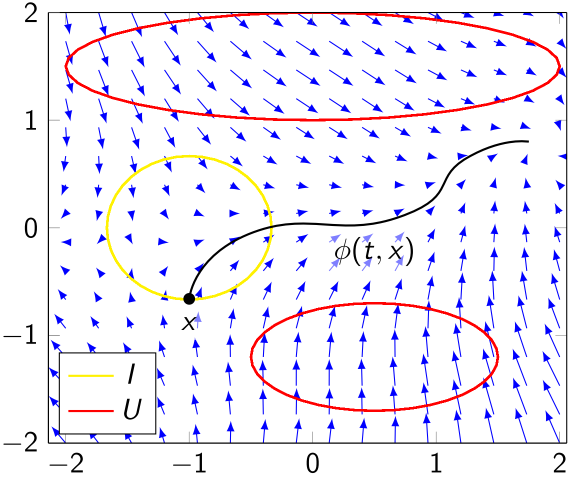
Initial set: $I \subseteq \mathbb{R}^n$

Unsafe set: $U \subseteq \mathbb{R}^n$

Definition

The system with field f, initial set I and unsafe set U is *safe* if for all $x \in I$ and all $t \in \mathbb{R}_+$, $\phi(t, x) \notin U$.

Illustration of System and Safety



Forward Invariant Set

Definition

A set $P \subseteq \mathbb{R}^n$ is *forward invariant* for the field f if $x \in P$ implies that for all $t \in \mathbb{R}_+$, $\phi(t, x) \in P$.

It is a *safe forward invariant set* for the system $\langle f, I, U\rangle$ if moreover $I \subseteq P$ and $P \cap U = \emptyset$.

Theorem (common knowledge)

If P is a safe forward invariant set for $\langle f, I, U\rangle$, then $\langle f, I, U\rangle$ is safe.

Barrier Functions as Forward Invariants

Introduced by S. Prajna [Pra06]

Definition ([Ame+19])

$B : \mathbb{R}^n \to \mathbb{R}$ is a *barrier function* for the system $\langle f, I, U \rangle$ if

a) $B(x) \leq 0$ for all $x \in I$
b) $B(x) > 0$ for all $x \in U$
c) $\nabla B(x) \cdot f(x) \leq -\lambda(x) B(x)$, where λ is continuous

Proposition (see, e.g., [Ame+19])

If B is a barrier function for $\langle f, I, U \rangle$, then $\{x \in \mathbb{R}^n : B(x) \leq 0\}$ is a safe forward invariant set for $\langle f, I, U \rangle$

Table of contents

Barrier Function Synthesis: Vanilla Version

Search B in some class (e.g., polynomial functions) such that

a) $B(x) \leq 0$ for all $x \in I$

b) $B(x) > 0$ for all $x \in U$

c) $\nabla B(x) \cdot f(x) \leq -\lambda(x) B(x)$ for all $x \in \mathbb{R}^n$

Challenges:

- If λ not fixed, the problem is nonconvex :(
- If λ fixed, needs to be carefully crafted :/

For instance, choosing $\lambda(x)$ constant:

- Conservative (implies that $\{x \in \mathbb{R}^n : B(x) \leq 0\}$ is attractive!)
- Which constant to choose (not monotonic!)?

Barrier Function Synthesis: Our Contribution

1. Introduce a new decrease condition (c'): intuitively reads as

$$\nabla B(x) \cdot f(x) \leq -\lambda(x)B(x) \text{ for all } x \in \mathbb{R}^n \text{ with } B(x) \leq 0 \quad (1)$$

2. Justify the validity and advantages of (c')
3. Fixed-point algorithm for synthesis using (c')

New Decrease Condition: Naïve Form

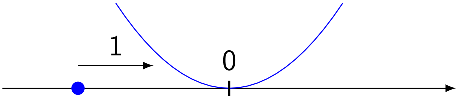
Assume that

$$\nabla B(x) \cdot f(x) \leq -\lambda(x) B(x) \text{ for all } x \in \mathbb{R}^n \text{ with } B(x) \leq 0 \qquad (1)$$

holds. Is $\{x \in \mathbb{R}^n : B(x) \leq 0\}$ forward invariant?

Not always :/

Example: $f(x) = 1$ and $B(x) = x^2$
(1) holds but $\{x \in \mathbb{R}^n : B(x) \leq 0\} = \{0\}$ is not forward invariant



New Decrease Condition: Valid Form

Theorem

Let $p(x) = \nabla B(x) \cdot f(x) + \lambda(x) B(x)$*, and assume that*

$$p(x) = -\sum_{k=0}^{\ell} \sigma_k(x)(-B(x))^k \tag{2}$$

for some $\sigma_k(x) \geq 0$ *continuous. Then,* (1) *holds, and moreover* $\{x \in \mathbb{R}^n : B(x) \leq 0\}$ *is forward invariant.*

New Decrease Condition: Advantages

We can use $\lambda(x)$ constant, i.e., $\lambda(x) = \gamma$:

- Conservativeness decreases monotonically with $\gamma > 0$
- Not conservative for $\gamma > 0$ large enough[1]

[1] Under very mild assumptions. Still conservativeness coming from restricted search space for B and constraints "tractabilization".

Fixed-Point Characterization

Define the map

$$G(B) = \{\ \tilde{B} : \mathbb{R}^n \to \mathbb{R} \ \text{ such that} \\ \tilde{B}(x) \le 0 \text{ and } \nabla \tilde{B}(x) \cdot f(x) + \gamma \tilde{B}(x) \le 0 \\ \text{for all } x \in \mathbb{R}^n \text{ with } B(x) \le 0\ \}$$

Proposition

B satisfies (1) *if and only if $B \in G(B)$*

Proposition

$G(B)$ is a convex cone

Fixed-Point Algorithm

Start with $B_0 : \mathbb{R}^n \to \mathbb{R}$ such that $B_0(x) \leq 0$ for all $x \in I$
$B_1 \in G(B_0)$
$B_2 \in G(B_1)$
etc.
until $G(B_k) = \emptyset$ or $B_k \in G(B_k)$ or $B_k \not> 0$ on U

To avoid large steps:

$$B_{k+1} = \arg\min_{\tilde{B} \in G(B_k)} \|\tilde{B} - B_k\|$$

Fixed-Point Algorithm and Abstract Interpretation

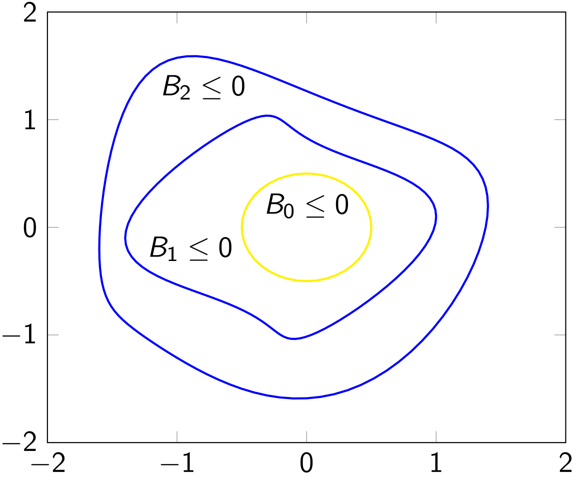


Table of contents

Vector Barrier Functions

Introduced by A. Sogokon, K. Ghorbal, Y. Kiam Tan and A. Platzer [Sog+18]

Definition ([Sog+18])

$B : \mathbb{R}^n \to \mathbb{R}^m$ is a *vector barrier function* for the system with field f, initial set I and unsafe set U if

a) $B(x) \preceq 0$ for all $x \in I$

b) $B(x) \not\preceq 0$ for all $x \in U$

c) $\nabla B(x) \cdot f(x) \preceq AB(x)$ for all $x \in \mathbb{R}^n$,

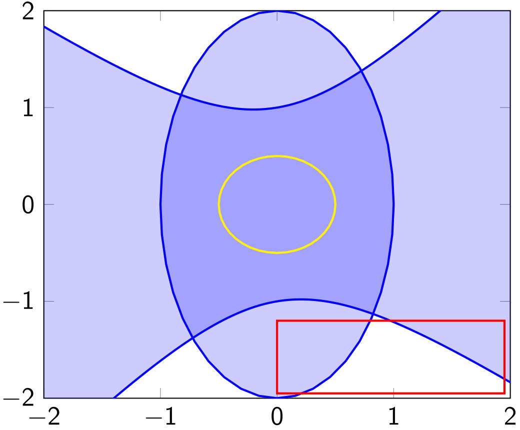
where $A \in \mathbb{R}^{m \times m}$ is Metzler

Proposition ([Sog+18])

If B is a vector barrier function for $\langle f, I, U \rangle$, then $\{x \in \mathbb{R}^n : B(x) \preceq 0\}$ is a safe forward invariant set for $\langle f, I, U \rangle$

Illustration of Vector Barrier Function

$$B(x, y) = \begin{bmatrix} 4x^2 + y^2 - 4 \\ (y - \frac{x}{5})^2 - x^2 - 1 \end{bmatrix}$$



Vector Barrier Function Synthesis: Our Contribution

1. Introduce the condition (c'): intuitively reads as

$$\nabla B(x) \cdot f(x) \preceq -\lambda(x) B(x) \text{ for all } x \in \mathbb{R}^n \text{ with } B(x) \preceq 0 \quad (3)$$

2. Justify the validity and advantages of (c')
3. Fixed-point algorithm for synthesis using (c')

New Decrease Condition: Validity

Theorem

Let $p(x) = \nabla B(x) \cdot f(x) + \lambda(x)B(x)$, *and assume that*

$$p(x) = -\sum_{k_1=0}^{\ell} \cdots \sum_{k_m=0}^{\ell} \sigma_{k_1,\ldots,k_m}(x) \prod_{j=1}^{m} (-[B(x)]_j)^{k_j} \tag{4}$$

for some $\sigma_{k_1,\ldots,k_m}(x) \succeq 0$ *continuous. Then,* (3) *holds, and moreover* $\{x \in \mathbb{R}^n : B(x) \preceq 0\}$ *is forward invariant.*

Fixed-Point Characterization

Define the map

$$G(B) = \{\ \tilde{B} : \mathbb{R}^n \to \mathbb{R}^m \text{ such that} \\ \tilde{B}(x) \preceq 0 \text{ and } \nabla\tilde{B}(x)\cdot f(x) + \gamma\tilde{B}(x) \preceq 0 \\ \text{for all } x \in \mathbb{R}^n \text{ with } B(x) \preceq 0\ \}$$

Proposition

B satisfies (3) *if and only if $B \in G(B)$*

Proposition

$G(B)$ is a convex cone

Fixed-Point Algorithm

Start with $B_0 : \mathbb{R}^n \to \mathbb{R}^m$ such that $B_0(x) \preceq 0$ for all $x \in I$
$B_1 \in G(B_0)$
$B_2 \in G(B_1)$
etc.
until $G(B_k) = \emptyset$ or $B_k \in G(B_k)$ or $B_k(x) \preceq 0$ for some $x \in U$

To avoid large steps:

$$[B_{k+1}]_j = \arg\min_{\tilde{B} \in G(B_k)} \|\tilde{B} - [B_k]_j\|$$

Table of contents

Implementation Details

- Search B as a vector-valued polynomial of bounded degree
- (4) enforced using Sum-of-Squares, i.e.,

$$p(x) = -\sum_{k_1=0}^{\ell} \cdots \sum_{k_m=0}^{\ell} \sigma_{k_1,\dots,k_m}(x) \prod_{j=1}^{m} (-[B(x)]_j)^{k_j}$$

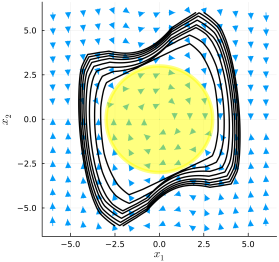
  for SoS polynomials $\sigma_{k_1,\dots,k_m}(x)$
- Implementation in `Julia`, using `SumOfSquares.jl` and `Mosek`

Vanderpol Oscillator I

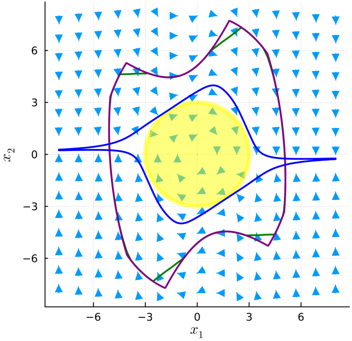
$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} x_2 \\ \frac{1}{2}x_2 - x_1 - \frac{1}{2}x_1^2 x_2 \end{bmatrix}, \qquad I = \left\{ x_1^2 + x_2^2 \leq \frac{1}{4} \right\}$$

Search B as a polynomial of degree 2 with 8 components

Results: Computation time of 50 sec.



Vanderpol Oscillator II



Final output = purple curve, not verified by SMT solver
Trimmed output = green curve, verified by SMT solver
Vanilla SoS output = blue curve, requires degree ≥ 8, not verified by SMT solver

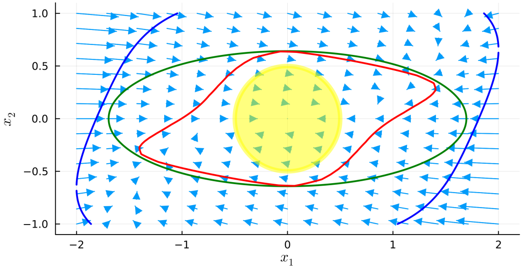
Nonlinear System I

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} -x_1^3 + \frac{1}{2}x_2 \\ -x_1 - 2x_2 \end{bmatrix}, \qquad I = \left\{ x_1^2 + x_2^2 \leq \frac{1}{4} \right\}$$

Search B as a polynomial of degree 2 with 1 (resp. 11) components

Results: Computation time of 1 (resp. 50) sec.

Nonlinear System II



Final output (1 comp.) = green curve
Final output (11 comp.) = red curve
Vanilla SoS output = blue curve, with degree ≥ 4

Summary of Numerical Experiments

Exp. #	Dimension	Time	SMT Solver
1	2	50 sec.	Valid
2 (H_1)	2	1 sec.	Valid
2 (H_2)	2	50 sec.	Valid
3 (H_1)	2	1 sec.	Valid
3 (H_2)	2	12 sec.	Valid
4 (H_1)	2	2.5 sec.	Valid
4 (H_2)	2	152 sec.	Valid
5	3	5.5 sec.	Valid
6	4	372 sec.	T/O
7	2 (hybrid)	110 sec.	Valid
8	2 (hybrid)	115 sec.	Valid

Table of contents

Conclusions

- Introduced a less conservative decrease condition for barrier functions, and provided a fixed-point algorithm for barrier function synthesis using this condition: no more manual search for $\lambda(x)$!
- Extended the approach to vector barrier functions: reduced function complexity!
- Showcased the applicability on numerical examples
- Not discussed: how to choose B_0 (see paper)
- Not discussed: widening to ensure termination (see paper)

Future work:

- Reduce the number of components when possible (merging)
- Increase the convergence speed with momentum/widening techniques
- Apply the projection trick to other fixed-point algorithms

Table of contents

Bibliography I

[Nag42] Mitio Nagumo. "Über die lage der integralkurven gewöhnlicher differentialgleichungen". In: *Proceedings of the Physico-Mathematical Society of Japan. 3rd Series* 24 (1942). DOI: 10.11429/ppmsj1919.24.0_551.

[Par00] Pablo A Parrilo. "Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization". PhD thesis. California Institute of Technology, 2000.

Bibliography II

[PJ04] Stephen Prajna and Ali Jadbabaie. "Safety verification of hybrid systems using barrier certificates". In: *Hybrid Systems: Computation and Control. HSCC 2004.* Ed. by Rajeev Alur and George J Pappas. Vol. 2993. Lecture Notes in Computer Science. Berlin: Springer, 2004, pp. 477–492. DOI: 10.1007/978-3-540-24743-2_32.

[Pra06] Stephen Prajna. "Barrier certificates for nonlinear model validation". In: *Automatica* 42.1 (2006), pp. 117–126. DOI: 10.1016/j.automatica.2005.08.007.

Bibliography III

[SCÁ13] Sriram Sankaranarayanan, Xin Chen, and Erika Ábrahám. "Lyapunov function synthesis using Handelman representations". In: *IFAC Proceedings Volumes* 46.23 (2013), pp. 576–581. DOI: 10.3182/20130904-3-FR-2041.00198.

[Sog+18] Andrew Sogokon et al. "Vector barrier certificates and comparison systems". In: *Formal Methods. FM 2018.* Ed. by Klaus Havelund et al. Vol. 10951. Lecture Notes in Computer Science. Cham: Springer, 2018, pp. 418–437. DOI: 10.1007/978-3-319-95582-7_25.

[Ame+19] Aaron D Ames et al. "Control barrier functions: theory and applications". In: *2019 18th European control conference (ECC)*. IEEE, 2019, pp. 3420–3431. DOI: 10.23919/ECC.2019.8796030.