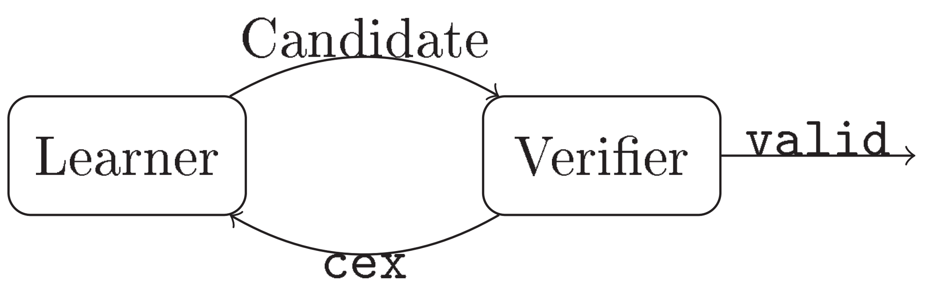
Formal Synthesis of Lyapunov Functions and Barrier Certificates

Alec Edwards
Alessandro Abate, Daniele Ahmed, Mirco Giacobbe, Andrea Peruffo

Objectives

- Safety and stability certification of non-linear continuous-time dynamical systems $\dot{x} = f(x)$.
- Synthesis of Lyapunov functions V for stability and barrier functions B for safety.
- Achieved using a counter-example guided synthesis approach (CEGIS, below). CEGIS is an approach to solving $\exists\forall$ problems, using two opposing compontents. The learner *guesses* candidate solutions using numerical induction, while the verifier checks their validity.



FOSSIL: *A Software Tool*

FOSSIL is a software tool developed for the synthesis of Lyapunov functions and barrier certificates. Relying on flexible, expressive neural network templates and powerful SMT-solvers, FOSSIL is able to certify the stability or safety of a wide range of non-linear systems. FOSSIL is characterised by its component structure, depicted in Figure 1 which serves as an augmented CEGIS loop. The additional components enhance the communication within the loop and improve both the speed and robustness of the procedure.

Learner

- Flexible neural network template characterised by input choice θ.
- Network is trained over a data set S of samples over the domain, using a loss function that penalises violation of the certificate conditions - e.g., for the Lyapunov condition in (1):

$$\mathcal{L}(S) = \sum_{s \in S} \max\{-V(s), 0\} + \sum_{s \in S} \max\{\dot{V}(s), 0\}.$$

Verifier

- An SMT-solver which can check the satisfiability of non-linear formulae over the reals.

$$\exists x \ s.t. \ x \in \mathcal{D} \setminus \{x_e\} \wedge V(x) \leq 0 \vee \dot{V}(x) \geq 0$$

- Seeks a *witness* that satisfies the negation of the conditions in (1) or (2). Any found witness is a point of invalidity, a *counter-example*, and is returned to the learner for further training. If it finds no witness then the certificate is valid.

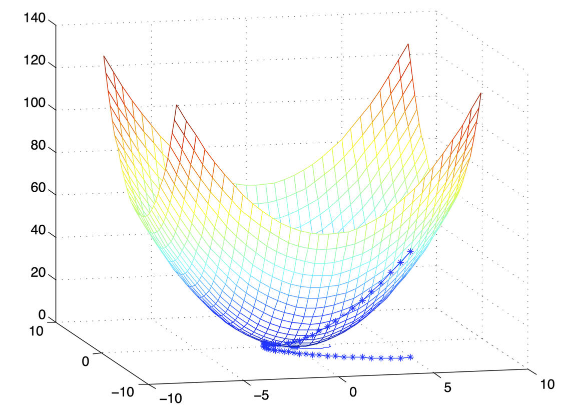
Consolidator

- The verifier returns a single data point *cex* to the learner. The consolidator seeks to enhance this *cex* to improve learning. Two procedures accomplish this:
  - Sample around the original *cex* to find further points that are likely to be invalid.
  - Perform gradient ascent (descent) along certificate function (or time derivative) to find greater or max violation.

Background: Safety and Stability

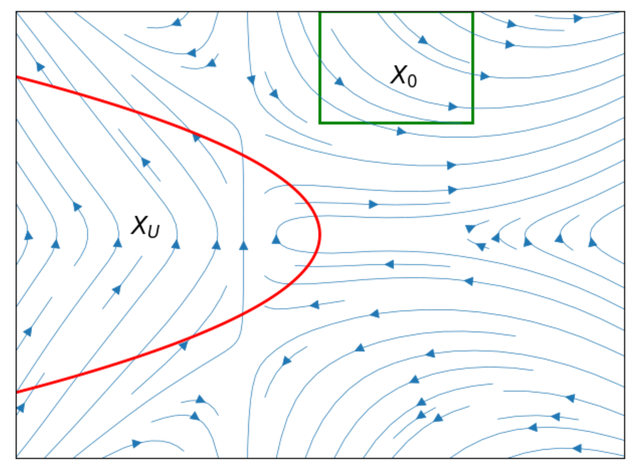
- **Stability**: Trajectories converge towards equilibrium point x_e.
- A *Lyapunov function* $V(x)$ must satisfy:

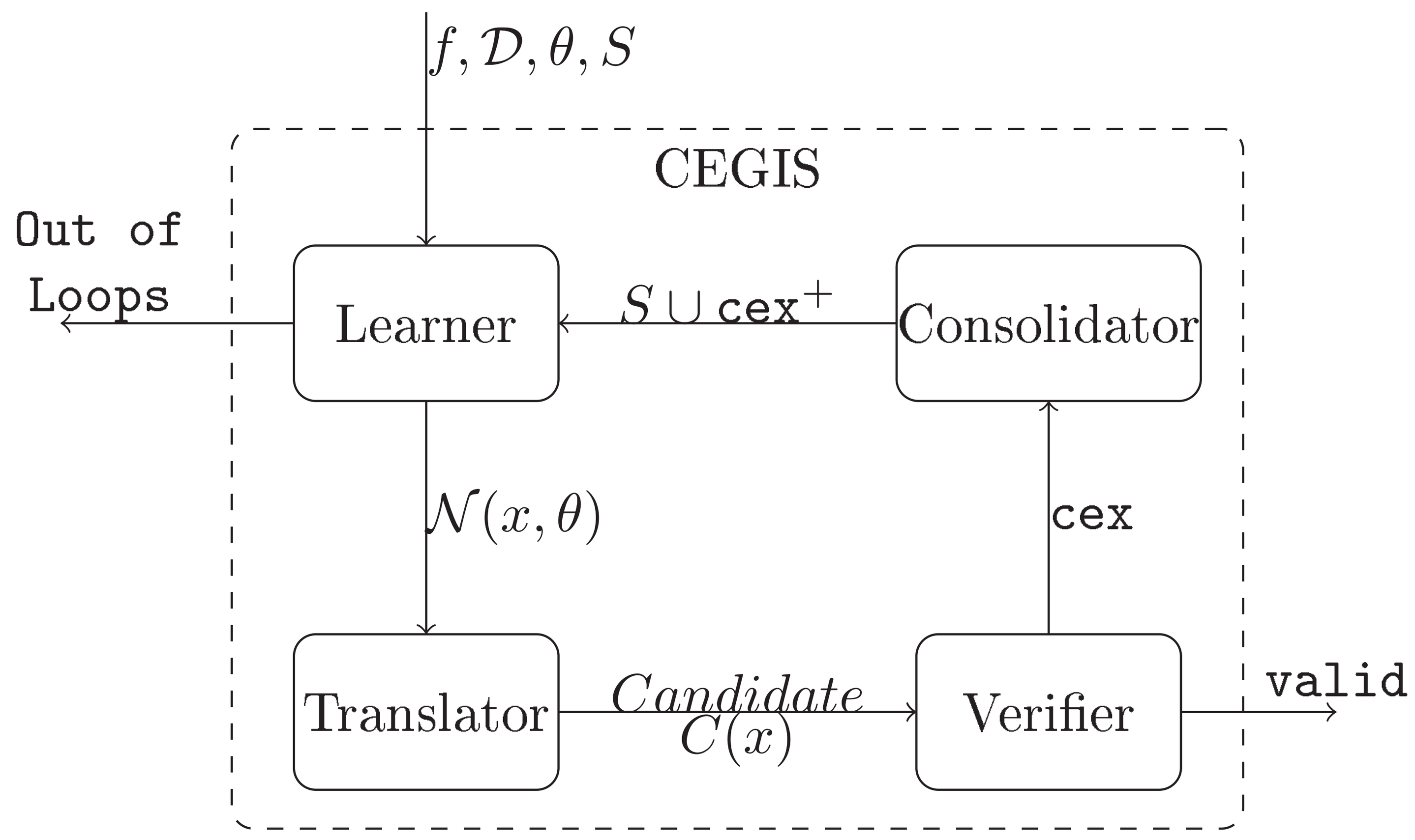
$$V(x_e) = 0,$$
$$\forall x \in \mathcal{D} \setminus \{x_e\} \ V(x) > 0 \ \wedge$$
$$\dot{V}(x) = \nabla V(x) \cdot f(x) < 0. \quad (1)$$



- **Safety**: No trajectory starting in a given initial set X_0 enters an unsafe set X_u over a domain $\mathcal{D}$.
- A *barrier certificate* satisfies:

$$B(x) \leq 0 \ \forall x \in X_0,$$
$$B(x) > 0 \ \forall x \in X_u,$$
$$\dot{B}(x) < 0 \ \forall x \in \mathcal{D} \text{ s.t. } B(x) = 0. \quad (2)$$



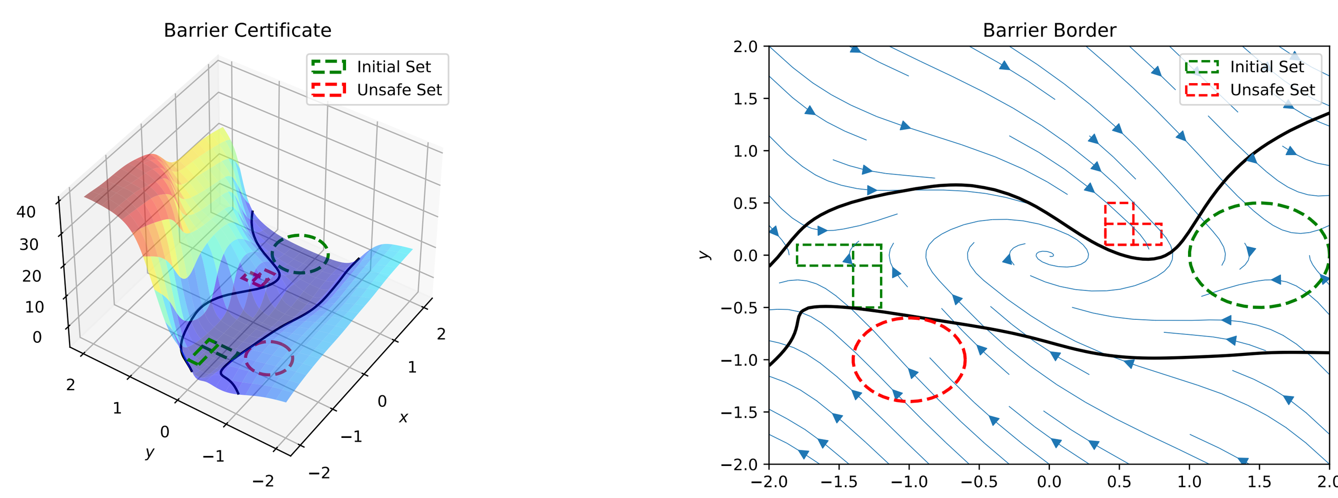


(a) Image A

Figure 1: CEGIS modular architecture within FOSSIL

A Case Study

Here we illustrate an example barrier certificate synthesised by *FOSSIL*. The dynamics shown depict a polynomial system with non-convex initial and unsafe sets. The synthesised barrier certificate consists of a neural network with two hidden layers of 20 neurons each, with sigmoid activation functions. FOSSIL takes 60 s to synthesise and verify the certificate with 2 CEGIS loops.



(a) Surface plot **(b)** Phase portrait

Figure 2: Example barrier certificate synthesised by *FOSSIL*. In both the surface plot (a) and phase portrait (b) the black line illustrates the zero level-set of the barrier function.

UNIVERSITY OF OXFORD

AIMS
EPSRC Centre for Doctoral Training in Autonomous Intelligent Machines & Systems

UKRI
Engineering and Physical Sciences Research Council