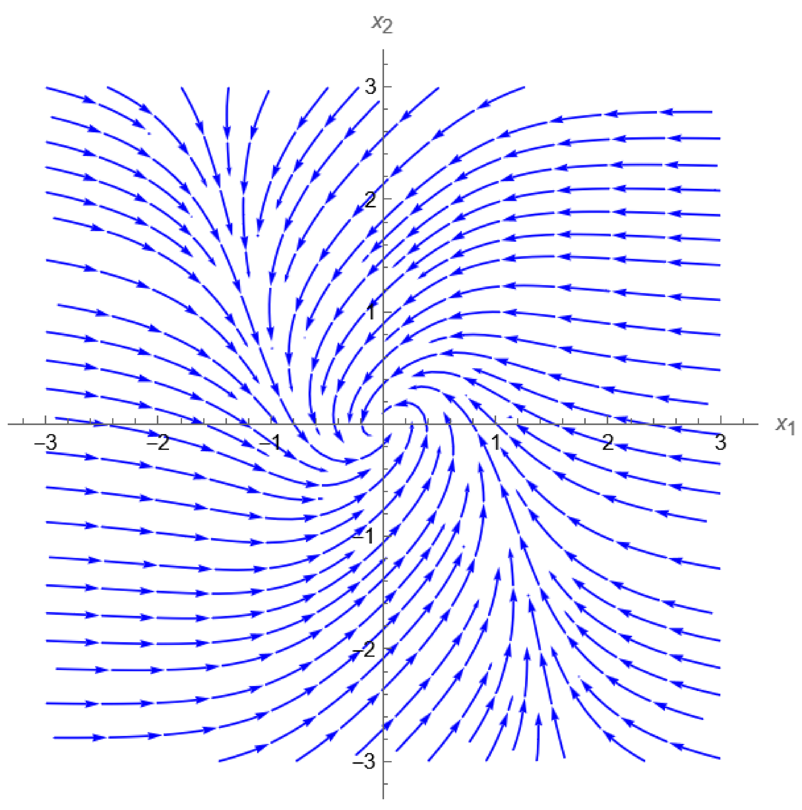
Methods for Verifying Safety and Stability in Cyber-Physical Systems

Lancaster University
School of Computing and Communications

Dr. Andrew Sogokon (a.sogokon@lancaster.ac.uk)
Prof. Neeraj Suri (neeraj.suri@lancaster.ac.uk)

Lyapunov Functions



- **Stability** in nonlinear ordinary differential equations is often proved by exhibiting a Lyapunov function.
- A Lyapunov function V is a scalar function modelling abstract "energy" in the system.
- Intuitively, the function V is required to decrease along the trajectories of the system (i.e. "energy" dissipates).

Vector Comparison Systems

- Typically, one deals with a single **scalar** function V (which is required to be positive definite and non-increasing.)
- The classic criterion for stability was generalized by R. E. Bellman in 1962 using a **vector comparison principle**.
- Bellman's idea of ***Vector Lyapunov functions*** is to use multiple functions (in a vector **V**) that individually need to satisfy less rigid criteria.
- The biggest practical bottleneck in using Lyapunov functions to prove stability lies in **finding** the function that satisfies the criteria (which involves a differential inequality).
- The motivation for using vector Lyapunov functions is that (intuitively) less rigid criteria can make these functions easier to find.

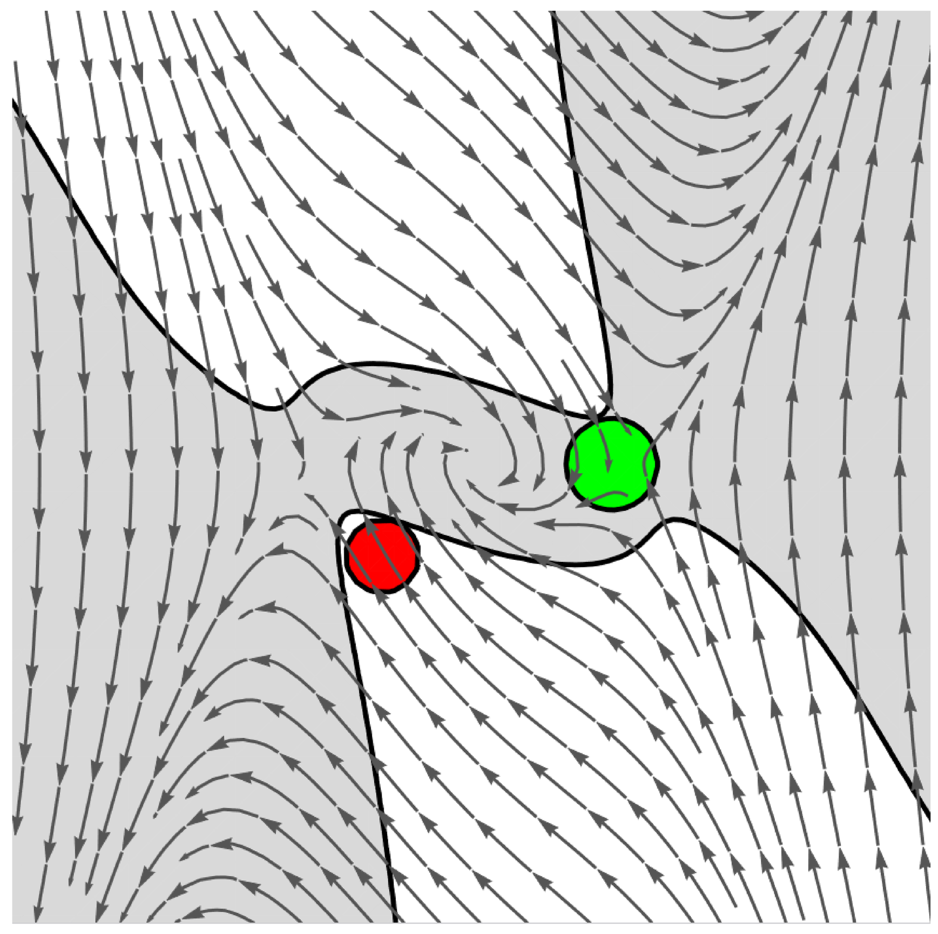
Learning Vector Certificate Functions

Lyapunov functions can be represented as NNs

- Recent work in control theory literature explored using artificial neural networks to represent Lyapunov functions.
- Scalar functions V can be **learned** and verified using tools such as SMT solvers.
- We are investigating whether vector Lyapunov functions **V** have any advantages over scalar functions in being "easier to learn".

Barrier Certificates

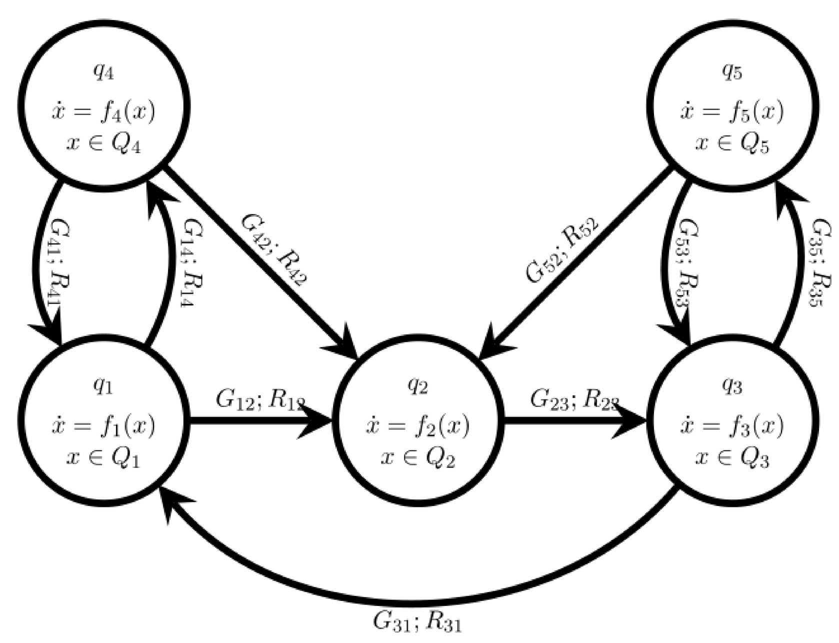
- **Barrier certificates** are Lyapunov-like functions B that are used for *safety verification* of nonlinear systems.
- Given a set of *initial states*, a set of *unsafe states* and a system of ordinary differential equations, a barrier certificate B acts as a certificate that no trajectory starting from the initial set can evolve into any of the unsafe states.



- The sub-level set $B \leq 0$ defines a *positively invariant set* of the system.
- Our earlier work developed *vector barrier certificates* **B** (albeit only of polynomial form).
- Barrier certificates can likewise be represented using artificial neural networks and *learned*.

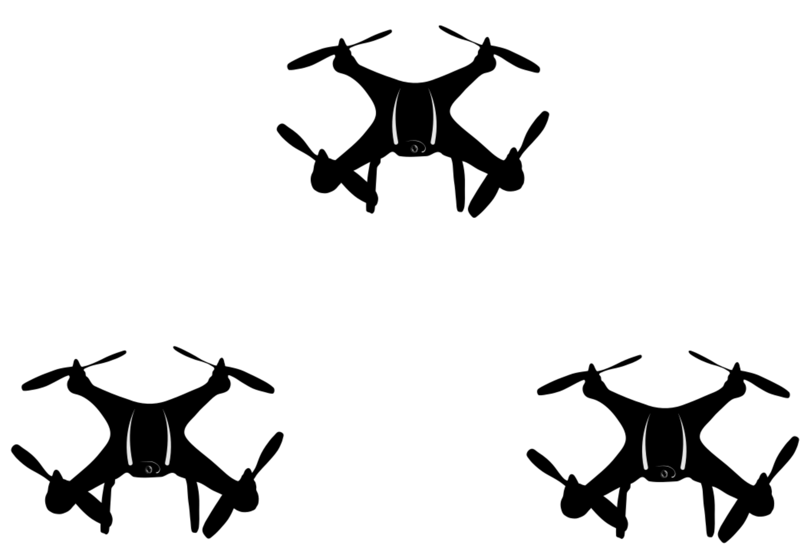
Invariant Generation for Hybrid Automata

- Barrier certificates provide a method for searching for positively invariant sets.
- This method can be applied to verify safety of hybrid automata (HA), which combine discrete and continuous behaviour.
- Many other methods for generating invariants exist.
- We are developing an invariant generation toolbox for HA.



Safety Verification for CPS

- Cyber-physical systems (CPS) can be modelled using hybrid automata (or *networks* of hybrid automata).
- Rigorous methods for proving safety in formal models such as HA can translate into more robust CPS designs with greater assurances of safe operation.



This work is supported by the Engineering and Physical Sciences Research Council [grant number: EP/V026763/1]