Optimization Based Search for Error Trajectories of Hybrid Dynamical Systems

Jan Kuřátko and Stefan Ratschan
Institute of Computer Science Academy of Sciences of the Czech Republic
Faculty of Mathematics and Physics, Charles University in Prague

Motivation

Hybrid dynamical systems feature both continuous and discrete state and evolution. A current problem in the field of **verification** is to test a hybrid dynamical system whether its trajectories attain certain states. For a given set of **initial** and **unsafe** states of a system we need to check whether a system is unsafe. A system is said to be unsafe if there exist trajectories reaching unsafe states. Finding these trajectories is the process of **falsification**.

Problem Formulation

Given: Hybrid dynamical system H, set of initial states I and set of unsafe states U.
Falsify: Find **any** trajectory $x(t)$, $t \in [t_0, t_f]$, of H such that $x(t_0) \in I$ and $x(t_f) \in U$.

Basic Method

- We **minimize** a distance function $J(x)$ to sets I and U.
- A minimum of $J(x)$ is a **candidate** for an **error** trajectory.
- To improve the speed of convergence we perform **sensitivity** analysis according to [1].
- There is a problem in finding a **good** starting point $x(t_0)$ and t_f, hence, the problem with **convergence** and uninteresting **local** minima.

Distance Function

Assuming I and U are **ellipsoids**, then

$$J(x) \equiv \|x(t_0) - c_I\|^2_{E_I} + \|x(t_f) - c_u\|^2_{E_U} \ .$$

The points c_I and c_U are centres of I, U respectively. Matrices E_I and E_U are symmetric positive definite and characterize I and U.

Illustration on a Sample Problem

We have the following hybrid dynamical system with **two** locations. It features **discontinuous** right hand side and a trajectory of a system.

$$\dot{x}(t) = \begin{cases} F(x) = \begin{bmatrix}0\\1\end{bmatrix} & \text{if} \quad x_2(t) \le -0.1 \\ \\ F(x) = \begin{bmatrix}0\\2\end{bmatrix} & \text{if} \quad x_2(t) \ge 1.4 \end{cases}$$

The line $x_2(t) + 0.1 = 0$ gives a switching hyper-surface and when a trajectory $x(t)$ reaches a point $\begin{bmatrix}x_1(t)\\-0.1\end{bmatrix}$ we jump to a point $\begin{bmatrix}x_1(t) - 7.5\\1.4\end{bmatrix}$ and continue with the evolution. Both initial and unsafe set are **disks** of radius equal to **four**. Set I is centred at $\begin{bmatrix}0\\-5\end{bmatrix}$, U at $\begin{bmatrix}0\\5\end{bmatrix}$ respectively.

When we use **HSOLVER** [2], we get that the initial point $x(t_0)$ must be in $[3.5, 4] \times [-6.94, -0.5]$ and the end point $x(t_f)$ must be in $[-4, -3.5] \times [1, 6.94]$. Therefore, we can start our optimization **near** a local minimum and obtain the result

$$x(t_0) = \begin{bmatrix}3.75\\-5\end{bmatrix} \quad \text{and} \quad t_f = 6.7 \ ,$$

which yields the following **error** trajectory. It is also optimal according to the **Hybrid Maximum Principle**.

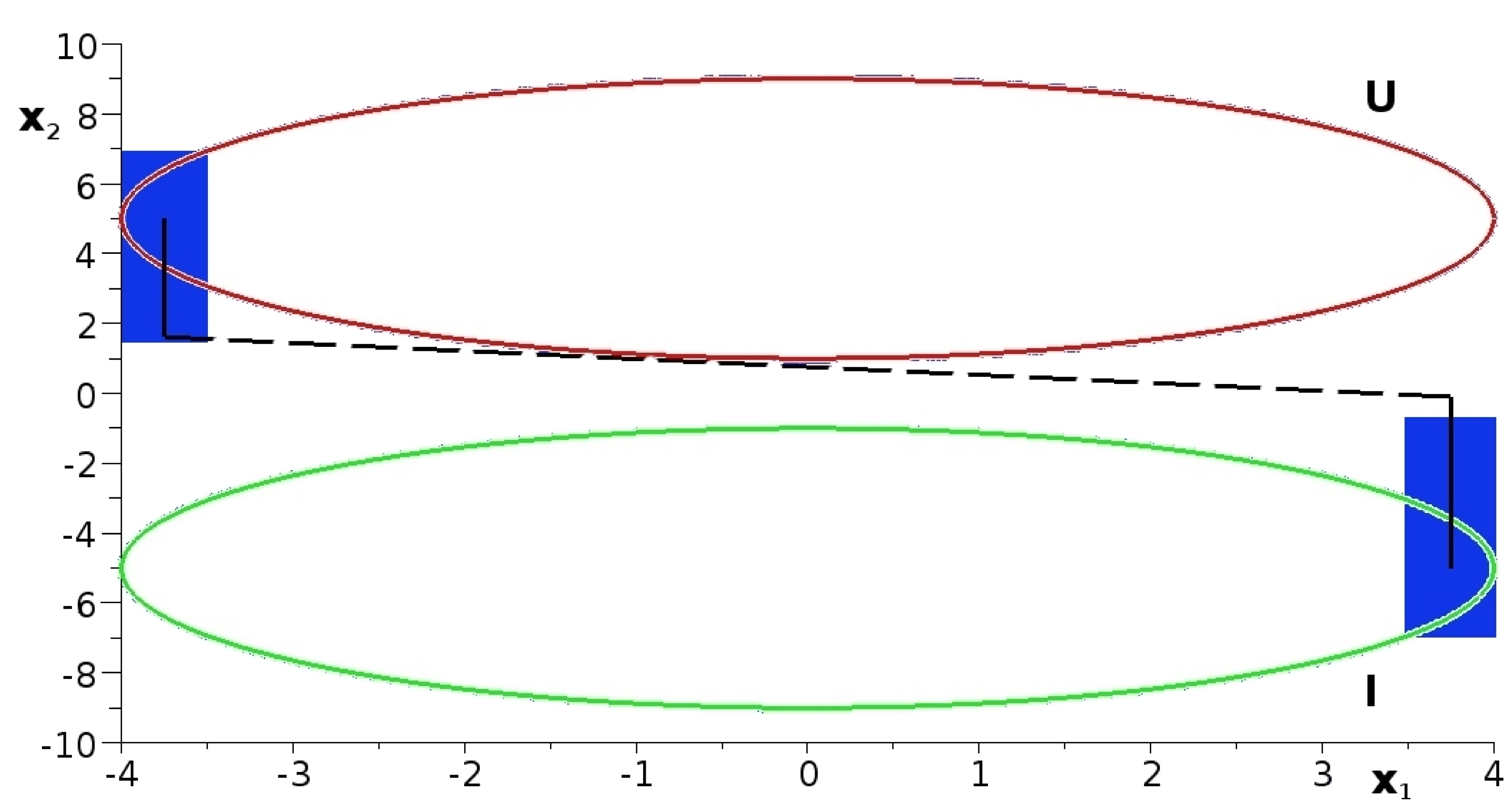

Figure 1: One error trajectory of the system.

Convergence

We use **verification** tools such as *HSOLVER* [2], to get a **good** guess on a starting point $x(t_0)$ and t_f, which is **near** a local minimum corresponding to an **error** trajectory.

Conclusion

Our method for the falsification of hybrid dynamical systems is

- **easy** to implement
- **simple** to understand
- applicable on **non-linear** dynamics
- a **complement** to verification tools

References

[1] I. A. Hiskens and M. A. Pai. Trajectory sensitivity analysis of hybrid systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 47(2), February 2000.

[2] http://hsolver.sourceforge.net.

Acknowledgements

This work was supported by the Czech Science Foundation (GACR) grant number P202/12/J060 with institutional support RVO:67985807.

Contact Information

- Web: http://www.cs.cas.cz/~kuratko
- Email: kuratko@cs.cas.cz
- Web: http://www.cs.cas.cz/~ratschan
- Email: stefan.ratschan@cs.cas.cz