Robust Control Abstractions for Verification of Uncertain Systems

Ulf T. Jönsson

1 Introduction

Control design is almost exclusively done based on simplified models. Therefore there is need for control abstraction for complex systems. As is discussed in Section **??**, High frequency dynamics, time delays, and hard nonlinearities such as friction and deadzones are often ignored in the higher level control design in order to use tractable design procedures. The resulting system must be verified with respect to stability and performance and then it is essential to take model approximations into account. This is particularly important for the complex mobile system designs studied in Recsys. Simulation can give much insight but for a rigorous proof of safe and reliable operation of the control system it is necessary to use methods from systems analysis.

Stationary solutions such as relative equilibria are routinely verified using Lyapunov theory, dissipation theory, or integral quadratic constraints. The verification of hybrid systems will generally require additional analytical tools in order to take into account mode switching. Reachability analysis is an important tool for this purpose. It refers to the problem of computing bounds on the set of states that can be reached by a dynamical system. This gives a tool for verifying that the state of a switched hybrid automaton stays in a "safe region" of the state space in each mode of the automaton.

The available methods for reachability analysis generally assume some uncertain system model. The uncertainty descriptions used are, for example, differential inclusions [3, 15, 11, 2], set disturbances [16, 13], and ellipsoidal approximations [12, 1]. These uncertainty models can be rather coarse or even unsuitable when taking into account unmodeled dynamics or unmodeled nonlinearities. We consider reachability analysis of systems where the disturbances and the model uncertainties are characterized by integral quadratic constraints (IQC) defined in the time domain. The IQCs give excellent modeling of many types of structured uncertainty.

Two problems of reachability analysis can be identified

1. Reach set computation, which is the problem of computing bounds on the reach set for trajectories of finite time extent. This gives a tool for verifying that the state of a switched hybrid automaton stays in a "safe region" of the state space in each mode of the automaton.

2. Transition analysis, which is the problem of estimating the mapping from one switching surface to another. This can be used to estimate the switching dynamics of an uncertain hybrid system.

We have considered both these problems in [5, 4, 6]. We survey the obtained results below.

2 Model Abstractions in Reachability Analysis

The models used in reach set computation can be generally be considered to be an *abstraction* of the real system where the dynamics is divided into two parts, a nominal dynamics and an uncertainty structure. The nominal dynamics must be tractable for computation and it can be anything from pure integrators [4, 6] to general nonlinear differential equations. The uncertainty is often constrained to belong to some convex set such as ellipsoids or polyhedra. In our work, we consider the model abstractions consisting of a nominal linear dynamics with uncertainty characterized by integral quadratic constraints. The model abstraction is defined as

$$\Sigma(x_0) : \begin{cases} \dot{x}(t) = A(t)x(t) + B(t)w(t) + u(t), \ x(0) = x_0 \\ \int_0^t \sigma_k(x(s), w(s), s)ds \geq 0, \ k = 1, \ldots, K. \end{cases} \tag{1}$$

where σ_k are general quadratic functions and $A(\cdot)$, $B(\cdot)$, and $u(\cdot)$ are given possibly time-varying matrices. A typical integral quadratic constraint is

$$\int_0^t \alpha(\tau)(|Cx(\tau)|^2 - |w(\tau)|^2)d\tau \geq 0$$

which is a weighted energy bound on the input-output relation.

3 Reach Set Computation

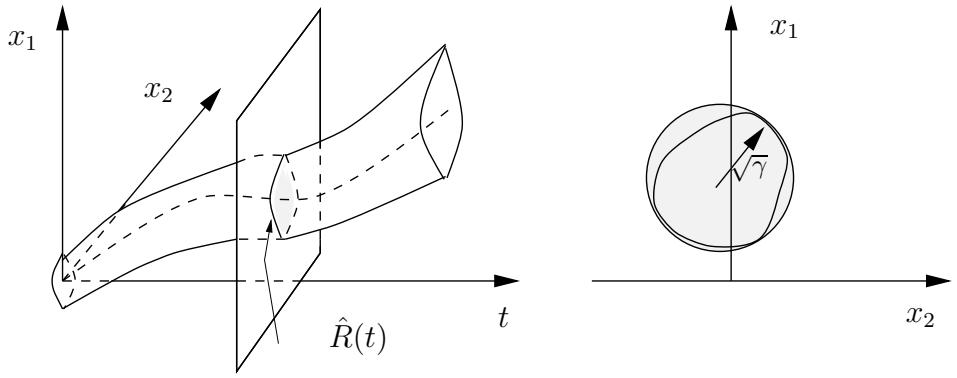
For a given a set of initial conditions X_0 and a system dynamics Σ, we want to compute a bound on the reach set

$$R = \cup_{t=0}^{T} \{x(t) : x \in \Sigma(x_0); x_0 \in X_0\} \subset \cup_{t=0}^{T} \hat{R}(t).$$

Each time slice in the bound is an ellipsoid

$$\hat{R}(t) = \{x : \psi(t, x) \leq \gamma(t)\},$$

where $\psi(t, x) = x^T Y(t)x + 2a(t)^T x + b(t)$ and $Y(t) \geq 0$. Here Y, a and b are given and our task is to minimize the radius $\sqrt{\gamma(t)}$. Typically, the ellipsoid is centered around the nominal trajectory indicated in dashed line in the figure below. The nominal solution is obtained when the disturbance w is set to zero in (1).



Minimization of the radius can be done according to the next proposition.

Proposition 3.1. *We have*

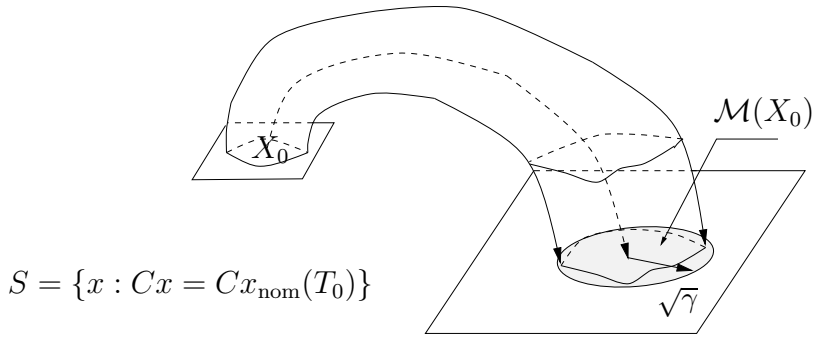
$$\gamma(t) = \sup \psi(t, x(t)) \quad \textit{subject to} \quad \begin{cases} \dot{x} = Ax + Bw + u, \quad x(0) \in X_0 \\ \int_0^t \sigma_k(x, w, s) ds \geq 0, \ k = 1, \ldots, K \\ \int_0^t [|x|^2 + |w|^2] ds < \infty \end{cases} \tag{2}$$

4 Transition Analysis

For a given a set of initial conditions X_0 and system dynamics Σ, we want to compute a bound on the intersection with a switching hyperplane S. We thus have to estimate the set

$$\mathcal{M}(X_0) = \{x(T) \in S : x \text{ is a solution to } \Sigma(x_0);\ x_0 \in X_0;\ T \in \mathbf{T}_{\text{tran}}\}.$$

where $\mathbf{T}_{\text{tran}}$ is a set that contains all the possible transition times, i.e., times for which the trajectory first intersects S_1. We will use as an estimate the smallest spherical ball that contains $\mathcal{M}(X_0)$. Ellipsoidal bounds can be obtained in the same way.



We assume that $S = \{Cx :\in \mathbf{R}^n\}$ and let $C_\perp$ be the orthogonal complement of C, i.e.,

$$CC_\perp = 0 \quad \text{and} \quad C_\perp^T C_\perp = I_p$$

where p is the rank of C. Furthermore, let Y be the projection matrix $Y = C_\perp C_\perp^T$. We have the following proposition

Proposition 4.1. *Let* $\alpha = Cx_{\text{nom}}(T_0)$ *and*

$$\psi(T, x) = (x - x_{\text{nom}}(T_0))^T Y (x - x_{\text{nom}}(T_0)),$$

and finally

$$\gamma = \sup \psi(T, x(T)) \quad \textit{subj. to} \quad \begin{cases} \dot{x} = Ax + Bw + u, \quad x(0) \in X_0, \\ Cx(T) = \alpha, \ Cx(t) < \alpha, \ t \in [0, T] \\ \int_0^T \sigma_k(t, x, w) dt \geq 0, \quad k = 1, \ldots, K_\sigma \\ \int_0^T [|x|^2 + |w|^2] dt < \infty, \ T \in \mathbf{T}_{\text{tran}} \end{cases} \tag{3}$$

Then γ *is the smallest positive number such that*

$$\mathcal{M}(X_0) \subset \{x \in S_1 : |x - x_{\text{nom}}(T_0)| \leq \sqrt{\gamma}\}.$$

5 The Optimization Problem

The optimization problems in (2) and (3) are generally nonconvex and infinite dimensional. There is a systematic procedure for computing useful upper bounds using Lagrangian relaxation. We here discuss the simplest case, namely the optimization problem in Proposition 3.1 with $X_0 = \{x_0\}$. The solution strategy for the optimization problem is based on the following ideas

- At any $t \in [0, T]$
  - Make a Lagrangian relaxation of the integral quadratic constraints. This is done along the lines of the general framework discussed in [14].
  - The dual function can now be computed using LQ optimal control techniques.
  - The dual optimization is done using cutting hyperplanes along the lines of [9, 10, 8].
  - The above procedure leads to an upper bound $\hat{\gamma}(t)$. It is of general interest to if $\hat{\gamma}(t) = \gamma(t)$, i.e. if there is no duality gap? The answer is generally negative and no a priori information on the duality gap can be given. However, it is sometimes simple to verify a posteriori whether the duality gap is zero or not. We discuss this for our special case below.
- The time-interval $[0, T]$ can be gridded rigorously such that a maximally sparse grid can be used to give a suboptimal solution of given accuracy.

Lagrangian Relaxation

We first introduce some new notation

$$\begin{aligned}
\mathcal{H}(x_0) &= \{z = (x, u) \in \mathbf{L_2}[0, T] : \dot{x} = Ax + Bw;\ x(0) = x_0\} \\
\Phi_0(z) &= \psi(x(T)) \\
\Phi_k(z) &= \int_0^T \sigma_k(x, w, t)dt, \quad k = 1, \ldots, K
\end{aligned}$$

The optimization problem in (2) can now be relaxed as follows

$$\begin{aligned}
\gamma(T) &= \sup_{z \in \mathcal{H}(x_0)} \Phi_0(z) \quad \text{subj. to} \quad \Phi_k(z) \geq 0, \quad k = 1, \ldots, K \\
&\leq \inf_{\tau \geq 0} \sup_{z \in \mathcal{H}(x_0)} \underbrace{\Phi_0(z) + \sum_{k=1}^{K} \tau_k \Phi_k(z)}_{\Phi(\tau, z)} \leq \inf_{\tau \in \mathcal{D}_0} \max_{z \in \mathcal{H}(x_0)} \Phi(\tau, z)
\end{aligned}$$

where $\mathcal{D}_0 = \{\tau \geq 0 : \sup_{z \in \mathcal{H}(x_0)} \Phi(\tau, z) \text{ is strictly concave}\}$.

Computing the Dual Function

Given that $\tau \in \mathcal{D}_0$, then it is easy to compute the dual function using LQ optimal control theory. Dynamic programming gives

$$\begin{aligned}\hat{\gamma}(\tau, T) &:= \max_{z \in \mathcal{H}(x_0)} \Phi(\tau, z) \\ &= \max_{\dot{x}=Ax+Bu} \hat{x}(T)^T \hat{Y} \hat{x}(T) + \int_0^T (\hat{x}^T \hat{Q}_\tau \hat{x} + 2\hat{x}^T \hat{S}_\tau w + w^T R_\tau w) dt \\ &= \hat{x}_0^T \hat{P}_\tau(0) \hat{x}_0\end{aligned}$$

where

$$\dot{\hat{P}} + \hat{A}^T \hat{P} + \hat{P}\hat{A} + \hat{Q}_\tau = (\hat{P}\hat{B} + \hat{S}_\tau) R_\tau^{-1} (\hat{P}\hat{B} + \hat{S}_\tau)^T, \quad \hat{P}(T) = \hat{Y}$$

$$\hat{x} = \begin{bmatrix} x \\ 1 \end{bmatrix}, \ \hat{Y} = \begin{bmatrix} Y & a \\ a^T & b \end{bmatrix}, \ \hat{Q}_\tau = \begin{bmatrix} Q_\tau & q_\tau \\ q_\tau^T & \rho_\tau \end{bmatrix}, \ \hat{A} = \begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix}, \text{ e.t.c.}$$

Here $\hat{Q}_\tau = \sum_{k=1}^K \hat{\tau}_k Q_k$, $\hat{S}_\tau = \sum_{k=1}^K \hat{\tau}_k \hat{S}_k$, $\hat{R}_\tau = \sum_{k=1}^K \hat{\tau}_k \hat{R}_k$ where the $\hat{Q}_k$, $\hat{S}_k$ and $\hat{R}_k$ contains the coefficients for the cost term corresponding to the k^{th} IQC, i.e. $\Phi_k(z)$.

Dual Optimization

The dual optimization problem

$$\hat{\gamma}(T) = \inf_{\tau \in \mathcal{D}_0} \hat{\gamma}(\tau, T)$$

is convex and can be solved using cutting plane techniques as in [9, 10, 8]. The oracles for testing feasibility and for generating new cuts are obtained using results from LQ theory. The details are given in [6, 5].

Exactness of the Lagrange Relaxation

In contrast to many optimization problems with nonconvex constraints that appear in IQC analysis, the problems we consider here will generally have a nonzero duality gap. However, it is sometimes possible to determine a posteriori whether an exact solution was obtained or not. For the special case discussed in this section it is possible to obtain the following result

Proposition 5.1. *Suppose there exists $\tau^* \in \mathcal{D}_0$ such that $\hat{\gamma}(\tau^*, T) = \inf_{\tau \in \mathcal{D}_0} \hat{\gamma}(\tau, T)$. Then*

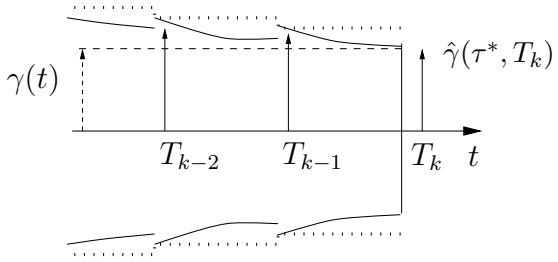
(i) There is no duality gap, i.e.

$$\begin{aligned}\gamma(T) &= \sup_{z \in \mathcal{H}(x_0)} \Phi_0(z) \quad \textit{subj. to} \quad \Phi_k(z) \geq 0, \ \forall k \\ &= \inf_{\tau \in \mathcal{D}_0} \hat{\gamma}(\tau, T)\end{aligned}$$

- $z(\tau^*) = \text{argmax}_{z \in \mathcal{H}(x_0)} \Phi(\tau^*, z)$ *solves the primal.*

Rigorous Gridding

We have now seen how a bound $\hat{\gamma}(t)$ on $\gamma(t)$ in (2) can be computed. The remaining problem is to develop a procedure to obtain a sparse finite grid of the time interval such that a rigorous upper bound is obtained for all $t \in [0, T]$. We start to use the above procedure to obtain an upper bound $\hat{\gamma}(\tau*, T)$. The idea is then to use the value function of the relaxed optimization problem to verify that $\gamma(t) \leq \hat{\gamma}(T) + \epsilon$ on a nontrivial interval. This procedure is continued backwards in time as is illustrated in the figure below.



The algorithm for generating the grid points is

1. Let $\hat{\gamma}(T_k) = \hat{\gamma}(\tau^*, T_k) + \epsilon$
2. Use the value function to verify $\gamma(t) \leq \hat{\gamma}(T_k)$ on $t \in [T_{k-1}, T_k]$

$$\hat{Y} - \lambda \hat{P}(t) \leq \begin{bmatrix} 0 & 0 \\ 0 & \epsilon + (1-\lambda)\hat{\gamma}(\tau^*, T_k) \end{bmatrix}, \qquad t \in [T_{k-1}, T_k]$$

   where $\lambda > 1$.
3. Go to 1.

6 Examples

We consider two examples. In the first we consider exclusively reach set computation and in the second we consider mainly transition analysis.

Example 1. *We consider the problem of steering a mobile robot from rest at* $(-5, 1)$ *to rest at* $(-1, 5)$ *in such a way that the robot we stays inside the corridor, see left hand side figure below. The equations of a particular nonholonomic robot, the unicycle, are*

$$\begin{aligned} \dot{x} &= v\cos(\theta) \\ \dot{y} &= v\sin(\theta) \\ \dot{\theta} &= \omega \\ \dot{v} &= -\delta_1 v + F/m \\ \dot{\omega} &= -\delta_2 \omega + \tau/J \end{aligned}$$

where δ_1, δ_2 *are uncertain and possible time-varying but bounded. They represent damping and the effect of viscous friction. The following choice of coordinates*

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \end{bmatrix} = \begin{bmatrix} x_1 + L\cos(\theta) \\ x_2 + L\sin(\theta) \\ v\cos(\theta) - L\omega\sin(\theta) \\ v\sin(\theta) - L\omega\cos(\theta) \\ \theta \end{bmatrix}$$

make the system holonomic and the resulting feedback linearized dynamics becomes

$$\begin{bmatrix} \dot{y}_1 \\ \dot{y}_2 \\ \dot{y}_3 \\ \dot{y}_4 \\ \dot{y}_5 \end{bmatrix} = \begin{bmatrix} y_3 \\ y_4 \\ \nu_1 + \Delta_{11}(t)y_3 + \Delta_{12}(t)y_4 \\ \nu_2 + \Delta_{21}(t)y_3 + \Delta_{22}(t)y_4 \\ -\frac{1}{2L}y_3 \sin(y_5) + \frac{1}{2L}y_4 \cos(y_5) \end{bmatrix}$$

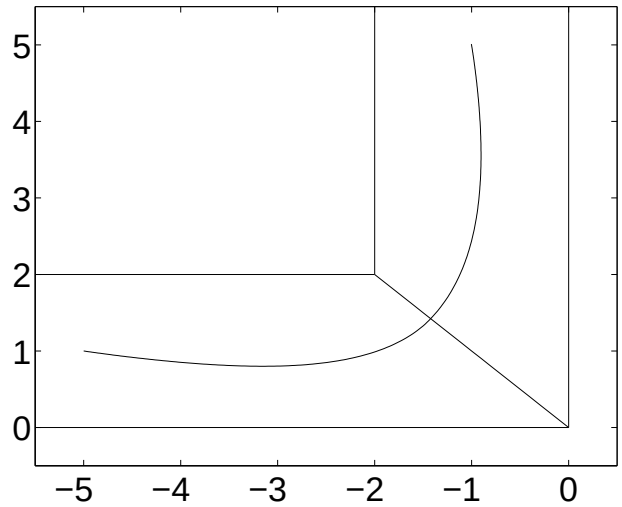
where

$$\begin{aligned} \Delta(t) &= \begin{bmatrix} \cos(\theta) & -L\sin(\theta) \\ \sin(\theta) & L\cos(\theta) \end{bmatrix} \begin{bmatrix} \frac{\delta_1}{2}\cos(\theta) & \frac{\delta_1}{2}\sin(\theta) \\ -\frac{\delta_2}{2L}\sin(\theta) & \frac{\delta_2}{2L}\cos(\theta) \end{bmatrix} \\ &= \begin{bmatrix} \frac{\delta_1}{2}\cos(\theta)^2 + \frac{\delta_2}{2}\sin(\theta)^2 & \frac{\delta_1-\delta_2}{2}\sin(\theta)\cos(\theta) \\ \frac{\delta_1-\delta_2}{2}\sin(\theta)\cos(\theta) & \frac{\delta_1}{2}\sin(\theta)^2 + \frac{\delta_2}{2}\cos(\theta)^2 \end{bmatrix} \end{aligned}$$

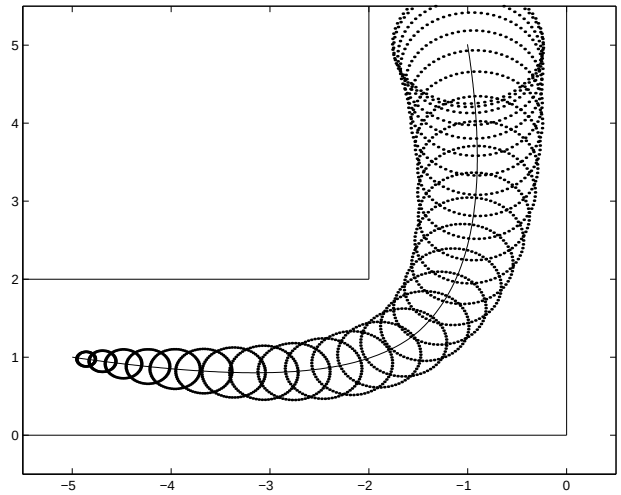
This is a bounded time-varying matrix. We assume that uncertain (possibly time-varying) parameters δ_k are bounded such that dynamics is contained in the behavior of the abstract model

$$\ddot{y} = u + w, \quad \text{where} \quad \int_0^t (|\dot{y}|^2 - 3^2|w|^2)ds \geq 0.$$

The nominal trajectory is designed based on the linear dynamics $\ddot{y} = u$. We want to verify that the robot stays inside the following corridor when friction and unmodeled dynamics is present via the uncertain model. The nominal design is done using dynamic programming in a similar way as described in [7].



Reachability analysis proves that the robot indeed stays inside the corridor, as we can see in the figure below. Each ellipsoid represents the reach set at the time instant when the trajectory is at the center point of the ellipsoid.



The second example is taken from [4, 6].

Example 2. *In this example we consider the relay oscillator*

$$\begin{aligned} \dot{x} &= Ax + B\varphi(y_2) + Fu \\ y_1 &= Cx, \qquad y_2 = C_2 x \\ u &= -\begin{cases} 1 & y_1(t) \geq 0.1 \text{ or } y_1(t) > -0.1 \text{ and } u(t^-) = 1 \\ -1 & y_1(t) \leq -0.1 \text{ or } y_1(t) < 0.1 \text{ and } u(t^-) = -1 \end{cases} \end{aligned} \tag{4}$$

where

$$\begin{aligned} A &= \begin{bmatrix} 0 & 1 \\ -1 & -1.4\zeta\omega \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad F = \begin{bmatrix} 0 \\ 5 \end{bmatrix} \\ C &= \begin{bmatrix} 1 & 0 \end{bmatrix}, \quad C_2 = \begin{bmatrix} 0 & 1 \end{bmatrix} \end{aligned}$$

and where φ is Lipschitz continuous and satisfies the sector bound $|\varphi(y_2)| \leq 0.4|y_2|$.

For the case when $\varphi \equiv 0$ then the system (4) has a stable limit cycle. The objective of the example is to use transition analysis to prove that there is a periodic solution for every possible Lipschitz continuous nonlinearity satisfying the above sector condition. In this case we have two switching hyperplanes

$$S_k = \left\{ x \in \boldsymbol{R}^2 : Cx = d_k \right\}, k = 1, 2.$$

where $d_1 = 0.1$ and $d_2 = -0.1$. Using the nominal trajectory this can equally well be stated $S_k = \{x \in \boldsymbol{R}^2 : C(x - x_{\text{nom}}(T_{0_k})) = 0\}$, where T_{0_k}, $k = 1, 2$ are the nominal switching times.

We can view the relay oscillator as a hybrid automaton with two modes. We model the dynamics in each mode as the uncertain system

$$\Sigma_k(x_0) = \begin{cases} \dot{x} = Ax + Bw \pm F, \quad x(0) = x_0 \\ \int_0^t (0.16 x^T C_2^T C_2 x - |w|^2) dt \geq 0 \end{cases}$$

where $k = 1, 2$. The nonlinear dynamics in (4) is covered by this uncertain system since the IQC covers the effect of the nonlinearity. Let $X_k = \{x \in S_k : (x - x_{\text{nom}}(T_{0_k}))^T Y (x - x_{\text{nom}}(T_{0_k})) \leq 1\}$, $k = 1, 2$, where $Y = 16 C_2^T C_2$. By showing that

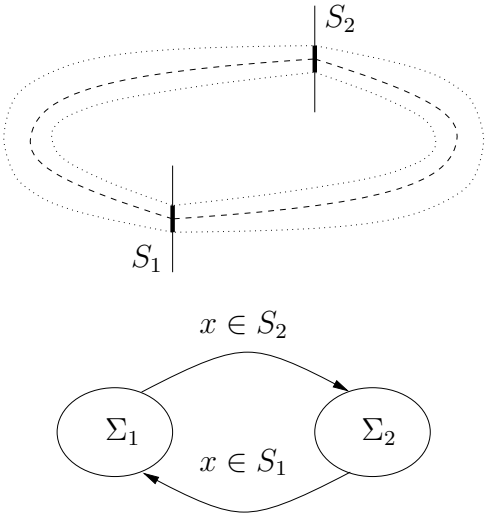


Figure 1: The relay oscillator is a hybrid automaton with two modes. Our analysis shows that the nonlinear system in (4) has a limit cycle that intersects the switching surfaces within the dark thick intervals X_k, $k = 1, 2$. The nominal limit cycle is drawn with dashed line and the perturbed system has a limit cycle that belongs to some tube around it. The analysis does not give any estimate of this tube, only its intersection with the switching surface.

(*i*) *the switchings are transversal.*

(*ii*) *the switching takes place in the correct order* $\Sigma_1 \to \Sigma_2 \to \Sigma_1 \to \dots$

(*iii*) $\mathcal{M}_1(X_1) \subset X_2$ *and hence by symmetry* $\mathcal{M}_2(X_2) \subset X_1$

it follows from [4, 6] that there exists a limit cycle for (4) that intersect the switching surfaces within a distance $1/\sqrt{16} = 0.25$ *from the nominal solution, see Figure 1 for an illustration. The main condition to verify is condition* (*iii*)*. This is done by computing an upper bound on* γ *in Proposition 4.1.*

References

[1] O. Botchkarev and S. Tripakis. Verification of hybrid systems with linear differential inclusions using ellipsoidal approximations. In N. Lynch and B. Krogh, editors, *Hybrid Systems: Computation and Control*, LNCS 1790, pages 73–88. Springer-Verlag, 2000.

[2] A. Chutinan and B.H. Krogh. Verification of polyhedral-invariant hybrid automata using polygonal flow pipe approximations. In *In Hybrid systems: Computation and Control*, Lecture Notes in Computer Science. Springer-Verlag, 1999.

[3] T. A. Henzinger, P.-H. Ho, and H. Wong-Toi. Hytech: a model checker for hybrid systems. *Software Tools for Technology Transfer*, 1:110–122, 1997.

[4] U. Jönsson. On reachability analysis of uncertain hybrid systems. In *Proceedings of the IEEE Conference on Decision and Control 2002*, pages 2373–2378, Las Vegas, Nevada, USA, 2002.

[5] U. Jönsson. Robustness of trajectories with finite time extent. *Automatica*, 38(9):1485–1497, September 2002.

[6] U. Jönsson. Robustness of transitions in switched linear systems. *International Journal of Robust and Nonlinear Control*, 15:293–314, 2005.

[7] U. Jönsson, C. F. Martin, and Y. Zhou. Trajectory planning under a stochastic uncertainty. In *Fifteenth International Symposium on Mathematical Theory of Networks and Systems*, 2002.

[8] C. Kao, A. Megretski, and U. Jönsson. A cutting plane algorithm for robustness analysis of periodic systems. *IEEE Transactions on Automatic Control*, 46(4):579–592, April 2001.

[9] C-Y Kao. *Efficient Compuational Methods for Robustness Analysis*. PhD thesis, Massachusetts Institute of Technology, Cambridge, Massachusetts, 2002.

[10] C.-Y. Kao, A. Megretski, and U. Jönsson. Specialized fast algorithms for iqc feasibility and optimization problems. *Automatica*, 40(2):239–252, 2004.

[11] B.H. Krogh and A. Chutinan. *In Paul M. Frank (Ed): Advances in Control (Highlighys of ECC'99)*, chapter Hybrid Systems: Modeling and Supervisory Control, pages 227–246. Springer, 1999.

[12] A. B. Kurzhanski and Pravin Varaiya. Ellipsoidal techniques for reachability analysis. In N. Lynch and B. Krogh, editors, *Hybrid Systems: Computation and Control*, LNCS 1790, pages 202–214. Springer-Verlag, Heidelberg, 2000.

[13] J. Lygeros, C. Tomlin, and S. Sastry. Controllers for reachability specifications of hybrid systems. *Automatica*, pages 349–370, March 1999.

[14] A. Matveev and V. A. Yakubovich. Nonconvex problems of global optimization: linear-quadratic control problems with quadratic constraints. *Dynamics and Control*, 7(2):99–134, 1997.

[15] A. Puri and P. Varaiya. Verification of hybrid systems using abstractions. In *Also Hybrid Systems II*, LNCS 999, pages 359–369. Springer-Verlag, 1995.

[16] P. Varaiya. Reach set computation using optimal control. In *Proc. of KIT Workshop on Verification of Hybrid Systems*, Grenoble, France, 1998.