Combinatorial Abstractions of Dynamical Systems

Rafael Wisniewski[*]
Section of Automation & Control
Aalborg University, Denmark
raf@es.aau.dk

1 Extended Abstract

Formal verification has been successfully developed in computer science for verifying combinatorial classes of models and specifications [2]. In like manner, formal verification methods have been developed for dynamical systems [6]. However, the verification of system properties, such as safety, is based on reachability calculations, which are the sources of insurmountable complexity. This talk addresses indirect verification methods, which are based on abstracting the dynamical systems by models of reduced complexity and preserving central properties of the original systems.

Specifically, in this talk, I consider a dynamical system $\mathscr{C} = (M, \xi)$, where M is the state space - a closed manifold, and ξ is a smooth vector field on M.

We denote a flow line of ξ by $\phi_x(t) \equiv \phi_x^\xi(t)$, that is

$$\frac{d}{dt}\phi_x(t) = \xi\left(\phi_x(t)\right) \text{ with } \phi_x(0) = x.$$

The manifold M is compact; thus, the vector field ξ generates a 1-parameter group $\phi_t : M \to M,\ t \in \mathbb{R}$, of diffeomorphisms. The smooth flow map $\phi : \mathbb{R} \times M \to M$ is related to ϕ_t in the following way

$$\phi(t,x) \equiv \phi_t(x) \equiv \phi_x(t).$$

We will examine examples of candidates for the combinatorial system $\mathscr{D}$ that mirrors the behaviour of C. For now, the combinatorial system $\mathscr{D}$ is a pair (Z, Φ) consisting of a finite set Z, and a function $\Phi : \mathbb{R} \times Z \to 2^Z$, where 2^Z denotes the power set of Z. We think about Z as a discrete state space and about Φ as a discrete flow map. Subsequently, we will discuss methods of converting the dynamical system $\mathscr{C}$ to a combinatorial object $\mathscr{D}$.

For $z \in Z$, the cell $[z] = \mathscr{A}^{-1}(z) \subset M$. If the cells are disjoint, the collection $K = \{[z] |\ z \in Z\}$ is called a partition of the state space M; whereas, if a pair $[z] \cap [z'] \neq \emptyset$, the collection is called a cover.

An abstraction is an over-approximation if for any $(t,x) \in \mathbb{R}_{\geq 0} \times M$

$$\mathscr{A} \circ \phi(t,x) \subseteq \Phi(t, \mathscr{A}(x));$$

$\mathscr{A}$ is an under-approximation if

$$\Phi(t, \mathscr{A}(x)) \subseteq \mathscr{A} \circ \phi(t,x).$$

If $\mathscr{A}$ is a both under- and an over-approximation, then it is called a complete abstraction. For the questions related to safety, one might choose an over-approximation; whereas, for the questions corresponding to reachability, one might work with an under-approximation. Conservativeness of the abstraction,

[*] This work was supported by MT-LAB, a VKR Centre of Excellence for the Modeling of Information Technology.

Bortolussi, Bujorianu, Pola (Eds.): HAS 2013
EPTCS 124, 2013, pp. 5–8, doi:10.4204/EPTCS.124.2

say over-approximation, is measured by the volume,

$$\sup_{t\in\mathbb{R}_{\geq 0}} \max_{z\in Z} \mathrm{vol}(\Phi(t,z)\setminus \mathscr{A}\circ\phi(t,[z])).$$

Below, we sketch a number of examples discussed during the talk.

Example 1. *Suppose $\{U_z|z\in Z\}$ is a finite family of subsets covering M. Let $\mathscr{D}$ be given by Z and $\Phi(t,z)=\mathscr{A}\circ\phi(t,[z])$. Pick an order on Z. We define the abstraction $\mathscr{A}$ by*

$$\mathscr{A}: x\mapsto \min\{z\in Z|\ x\in U_z\}. \tag{1}$$

As a consequence of the definition of Φ, the abstraction $\mathscr{A}$ is an over-approximation. In this example, the computation of Φ might be tedious if not impossible. Therefore, an approximation is in place.

To this end, we define

$$\mathrm{pol}\{v_1,...v_l\}=\left\{\sum_{i=1}^{l}\alpha_i v_i(x)\ \middle|\ \alpha_i\geq 0 \textit{ and } \sum_{i=1}^{l}\alpha_i^2=1\right\}.$$

Let $L=\{L_i|\ i=1,\dots,l\}$ be a family of linear vector fields, and define multivalued map $F(x)=\mathrm{pol}L(x)$. Suppose that $\xi\in F(x)$, and define

$$\Phi(t,z)=\mathscr{A}\circ\mathrm{pol}\{\phi^{L_1}(t,[z]),\dots,\phi^{L_l}(t,[z])\}.$$

The over-approximation might be relatively conservative, but the computation is simplified as the flow maps are linear in the second argument. The algorithm can be additionally simplified if the sets U_k are polyhedral (in local patches).

Example 2. *Suppose that there exists a Finsler-Lyapunov (smooth) function [3] $V: TM\to\mathbb{R}$ (where $\pi: TM\to M$ is the tangent bundle) such that*

1. *$V(v)>0$ for all $v\in TM\setminus 0_M$.*
2. *There is $p\in\mathbb{N}$ such that $V(\lambda v)=\lambda^p V(v)$ for all $v\in TM$ and $\lambda>0$.*
3. *There is $p\in\mathbb{N}$ such that $V(v+w)^{\frac{1}{p}}<V(v)^{\frac{1}{p}}+V(w)^{\frac{1}{p}}$ for all $v,w\in TM$ with $\pi(v)=\pi(w)$.*

The function V defines metric ρ on M [7]

$$\rho(x_1,x_2)=\inf_{\gamma\in\Gamma(x_1,x_2)}\int_I V(\dot\gamma)^{\frac{1}{p}}ds,$$

where $I=[0,1]$, $\dot\gamma=\gamma_*(d/dt)$, $\Gamma(x_1,x_2)$ is the set of curves $I\to M$ with $\gamma(0)=x_1$ and $\gamma(1)=x_2$. Following Theorem 1 in [Forni and Sepulchre], if $dV: TM\to T^*(TM)$ satisfies the following inequality written in local coordinates

$$DV(x,w)(\xi(x),D\xi(x)w)\leq -\alpha(V(x,w)),\ \textit{ for all } (x,v)\in TM.$$

where α is a non-decreasing continuous function. Then $\rho(\phi(t,x_1),\phi(t,x_2))\leq\alpha(\rho(x_1,x_2))$. Hence, the system incrementally stable [1].

Since the state space M is compact, it is possible to cover M by the finite family $\{D(x_z,r_z)|\ z\in Z\}$ of disks $D(x,r)=\{y\in M|\ \rho(x,y)<r\}$ [4]. We define the abstraction $\mathscr{A}$ as in (1), and the combinatorial system $\mathscr{D}$ by Z and $\Phi(t,z)=\mathscr{A}\phi(t,x_z)$. The abstraction $\mathscr{A}$ is an over-approximation. We note that computation of Φ amounts to simulating the dynamical system $\mathscr{C}$ for a finite number of initial conditions x_z.

Example 3. *Let ξ be a Morse-Smale vector field on M [Palis and de Melo]. Recall, a vector field $\xi \in \mathfrak{X}^r(M)$ will be called Morse-Smale provided it satisfies the following five conditions:*

1. *ξ has a finite number of singular points, say $\beta_1, ..., \beta_k$, each hyperbolic,*
2. *ξ has a finite number of closed orbits (periodic solutions), say $\beta_{k+1}, ..., \beta_N$, each hyperbolic;*
3. *For any $x \in M,\ \alpha(x) = \beta_i$ and $\omega(x) = \beta_j$ for some i and j;*
4. *$\Omega(\xi) = \{\beta_1, ..., \beta_N\}$;*
5. *The stable and unstable manifolds associated with the β_i have transversal intersection.*

The sets $\beta_1, ..., \beta_N$ will be called the singular elements of the vector field ξ. The set of the singular elements of ξ will be denoted by $\mathscr{C}r(\xi)$. The stable (unstable) manifold of ξ at a singular element β is denoted by $W^s(\beta_i)$ ($W^u(\beta_i)$).

We define a partial order relation on the singular elements of a Morse-Smale vector field: $\beta_i \succ \beta_j$ will mean that $W(\beta_i, \beta_j) \equiv W^u(\beta_i) \cap W^s(\beta_j) \neq \emptyset$.

Consequently, each $W(\beta_i, \beta_j)$ is a cell, with the property that if $x \in W(\beta_i, \beta_j)$ then $\phi(t,x) \in W(\beta_i, \beta_j)$ for all $t \in \mathbb{R}$. Since the number of singular elements is finite, we can define $\mathscr{D}$ by

$$Z = \{W(\beta_i, \beta_j) |\ \beta_i \succ \beta_j\} \text{ and } \Phi(t,z) = z.$$

Example 4. *On the state space M, we define a family of functions $\{V_i : M \to \mathbb{R} |\ i = 1, \ldots, l\}$ that satisfy*

1. *$dV_i(\xi)(x) \leq 0$.*
2. *Let $\mathrm{Reg}(V_i)$ be the set of regular values of V_i. For any singular element β of ξ,*
   - *if $V_i^{-1}(\mathrm{Reg}(V_i)) \cap W^s(\beta) \neq \emptyset$ then $W^u(\beta) \subset V_i^{-1}(V_i(\beta))$;*
   - *if $V_i^{-1}(\mathrm{Reg}(V_i)) \cap W^u(\beta) \neq \emptyset$ then $W^s(\beta) \subset V_i^{-1}(V_i(\beta))$.*

For each function V_i, we associate a family of regular values $A^i \equiv \{a_0^i, \ldots, a_k^i |\ a_{k-1}^i < a_k^i\} \subset \mathbb{R} \cup \{-\infty, +\infty\}$. For $a_j^i \in A^i$, we define a shift operator $\sigma \equiv \sigma^i : a_j^i \mapsto a_{j-1}^i$ We use the notation $z = (z_1, \ldots, z_l)$ and define a cells $[z]$ with $z_i \in A^i$ by

$$[z] = \bigcap V_i^{-1}([\sigma z_i, z_i])$$

Let $\mathbb{R}_\infty \equiv \mathbb{R} \cup \{-\infty, +\infty\}$. For each $z \in Z \equiv A^1 \times \ldots \times A^l$, we define a cube $\Box_z \equiv [\underline{b}_{z_1} \overline{b}_{z_1}] \times \ldots \times [\underline{b}_{z_l} \overline{b}_{z_l}] \subset \mathbb{R}_\infty^l$ with $\underline{b}_{z_i}$ ($\overline{b}_{z_i}$) being the minimal (maximal) time over the trajectories staring at $V_i^{-1}(\sigma z_i)$ and leaving $V_i^{-1}(z_i)$ (If $V_i^{-1}([\sigma z_i, z_i])$ is a positive invariant set, this time is set to $+\infty$). We denote the set of cubes in $\mathbb{R}^l$ by Box. *As a consequence, the combinatorial system is characterised by a map $\Box : Z \to \mathrm{Box}$ defined by $z \mapsto \Box_z$.*

The following operator L will be instrumental: $L = (L_1, \ldots, L_l) \to \mathbb{R}_\infty^l$, where $L_i = \partial \circ \pi_i$, π_i is the projection on the ith component, and $\partial[\underline{b}, \overline{b}] = \overline{b} - \underline{b}$.

We define, a combinatorial system $\mathscr{D}$ by Z and Φ as

$$\begin{aligned} \Phi(t,z) \quad = \quad & \max\{z' \in A^1 \times \ldots \times A^l |\ \Box_z \equiv \Box_{z^0} < \Box_{z^1} \ldots < \Box_{z^m} \equiv \Box_{z'}, \\ & L(\Box_{z^0} + \ldots + \Box_{z^m}) \leq (t, \ldots, t), \text{ and } z^{i-1} = \sigma z^i \text{ for } i = 1, \ldots, m\}. \end{aligned}$$

By [5], this abstraction is complete.

References

[1] D. Angeli (2002): *A Lyapunov approach to incremental stability properties*. *Automatic Control, IEEE Transactions on* 47(3), pp. 410 –421, doi:10.1109/9.989067.

[2] E. M. Clarke, E. A. Emerson & A. P. Sistla (1986): *Automatic verification of finite-state concurrent systems using temporal logic specifications*. *ACM Trans. Program. Lang. Syst.* 8(2), pp. 244–263, doi:10.1145/5397.5399.

[3] F. Forni & R. Sepulchre (2012): *A differential Lyapunov Framework for Contraction Analysis*. *arXiv:1208.2943v1*.

[4] Goran Frehse, Sumit Jha & Bruce Krogh (2008): *A Counterexample-Guided Approach to Parameter Synthesis for Linear Hybrid Automata*. In Magnus Egerstedt & Bud Mishra, editors: *Hybrid Systems: Computation and Control*, *Lecture Notes in Computer Science* 4981, Springer Berlin / Heidelberg, pp. 187–200, doi:10.1007/978-3-540-78929-1_14.

[5] Christoffer Sloth & Rafael Wisniewski (2013): *Complete abstractions of dynamical systems by timed automata*. *Nonlinear Analysis: Hybrid Systems* 7(1), pp. 80 – 100, doi:10.1016/j.nahs.2012.05.003. Available at `http://www.sciencedirect.com/science/article/pii/S1751570X12000180`. IFAC World Congress 2011.

[6] P. Tabuada (2009): *Verification and control of hybrid systems: a symbolic approach*. Springer, doi:10.1007/978-1-4419-0224-5.

[7] L. Tammasy (2008): *Relation between metric spaces and Finsler spaces*. *Differential Geometry and its Applications* 26(5), pp. 483 – 494, doi:10.1016/j.difgeo.2008.04.007. Available at `http://www.sciencedirect.com/science/article/pii/S0926224508000284`.