Reachability in Hybrid Systems: 25 Years of Optimism

Eugene Asarin Thao Dang

IRIF, Université de Paris, CNRS

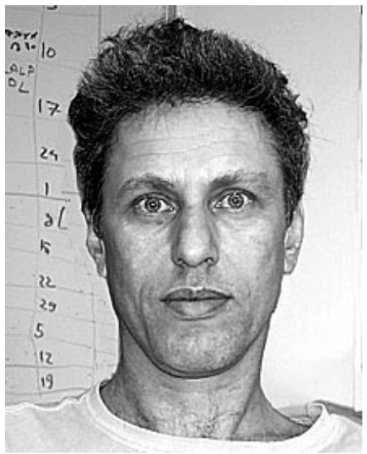
VERIMAG, CNRS, Université Grenoble Alpes

HSCC, April 2019

Oded Maler — Barbaric Science from a Captive Poet

Barbaric research...

Bringing light of computer science, poetry, and philosophy everywhere, including control; and fighting windmills. HSCC is a result, no?



"*The rest of the paper concerns the philosophy of continuous mathematics and control. Given that these philosophical remarks deserve to be exposed in a* **French cafe** *at best but not in a world class journal*", IEEE anonymous referee (2000)

Disclaimers & acknowledgments

This talk

- a patchwork based on Oded's and our material
- no new results
- some formulas, some pictures, some French café discussion
- an Oded-centric, biased, incomplete survey
- sorry if we forgot to mention your contribution
- sorry if we wrongly mention an impact of Oded on your work

Part I

First attempt: reachability and PCD

Hybrid Systems, first days

Early 90s hopes

- Cyberphysical/hybrid systems everywhere
- Control Science has perfect tools for continuous systems
- Computer Science has perfect tools for discrete systems, verification etc.
- Together we are inventing beautiful models of cyberphysical systems
- Together we will analyze, synthesize, verify them
- Research and industial impact will be huge.

The Project (Maler, Pnueli, many of you, 90s)

Verify hybrid systems (starting from simple models and simple properties, ending at planes and cars)

What is verification: OM slide

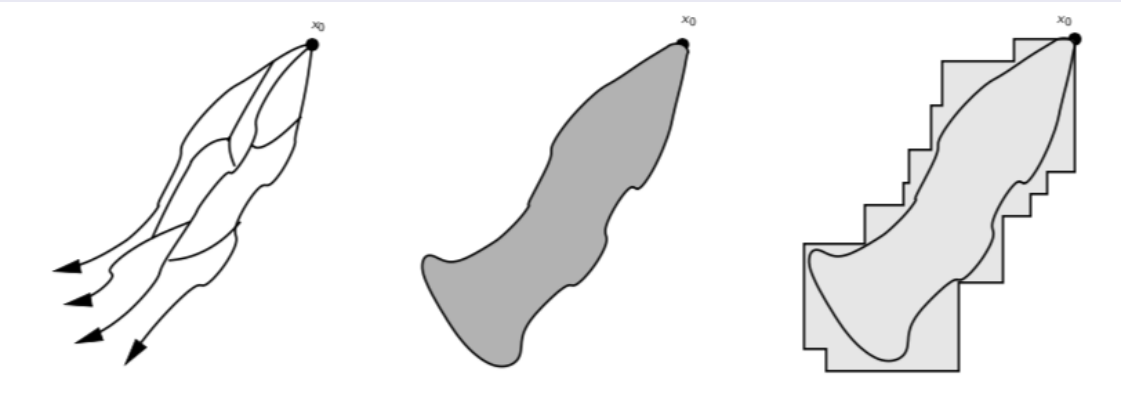
What is Verification ?

- The generic question:
- Given a complex discrete dynamical system with some **uncontrolled inputs** or unknown parameters
- Check whether **all** its **behaviors** satisfy some properties
- Properties:
  - Never reach some part of the state space
  - Always come eventually to some (equilibrium) state
  - Never exhibit some pattern of behavior
  - Quantitative versions of such properties..
- Existing verification tools can do this type of analysis for huge systems by sophisticated graph algorithms

Verification boils down to reachability

Definition (Reachability, given a system)

- $Reach(x, y) \Leftrightarrow$ exists a trajectory from x to y
- $ReachSet(x)$: set of all y s.t. exists a trajectory from x to y
- same notions for sets: $Reach(A, B)$ etc.



Verifying safety $\Leftrightarrow$ deciding reachability

An HS never enters a bad state? $\Leftrightarrow$ $\neg Reach(Init, Bad)$

The challenge

For various classes of hybrid systems

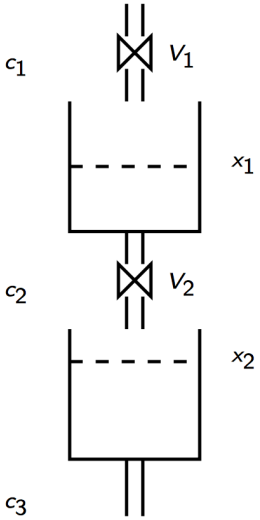
- *(central before 95)* Decide relation $Reach(A, B)$ (find an algorithm answering yes/no)
- compute (exactly or approximately) $ReachSet(A)$

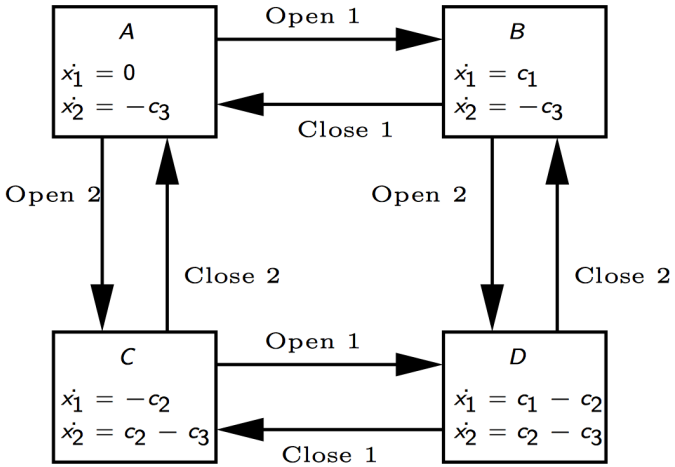
This question is...

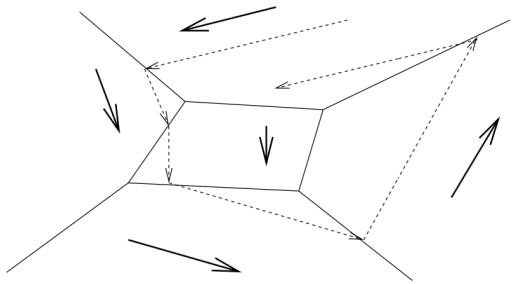
- a key to verification
- in the DNA of HSCC
- main topic of RP etc..
- focus of my talk

Reasons to be optimistic

- Encouraged by verification of **timed automata**
- Starting with very simple **Piecewise-Constant Derivative systems (PCD)**
  - very simple continuous dynamics
  - no input, no disturbance, no jumps
  - complexity comes from discrete dynamics switching



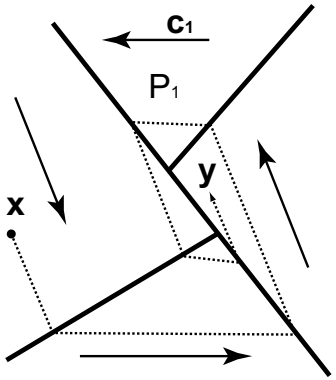




Special classes of Hybrid Automata 2

My favorite class

PCD = Piecewise Constant Derivatives

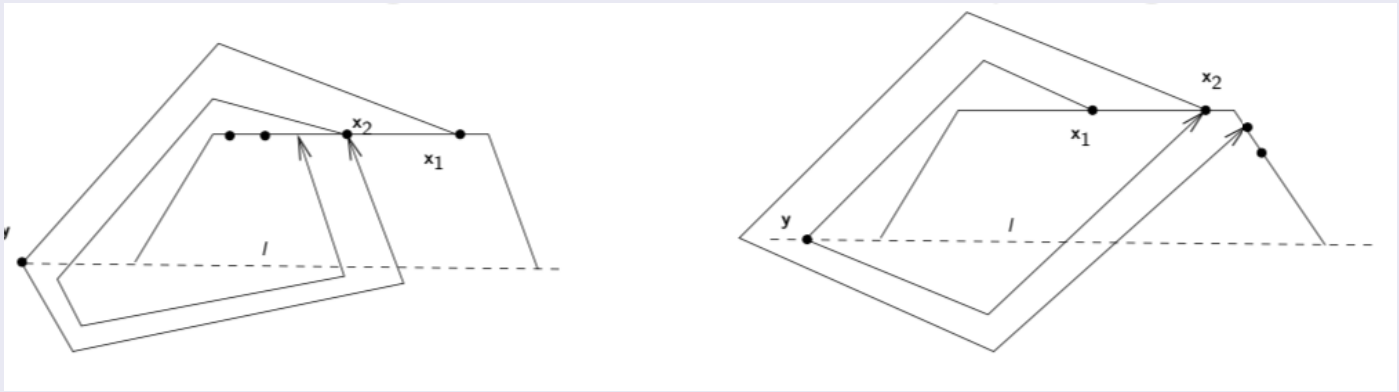


$\dot{\mathbf{x}} = \mathbf{c}_i$ for $\mathbf{x} \in P_i$

Enchantment: Planar PCD

A beautiful theory of Maler and Pnueli for 2dim PCD

- based on plane topology and many bright ideas
- reinvention of Poincaré-Bendixson theory
- a trajectory cannot intersect itself $\Rightarrow$ it can only spiral in or out
- the limit of such a spiral easy to compute
- reachability decidable by a wonderful algorithm.



Bad news arrive (Oded starts working with EA)

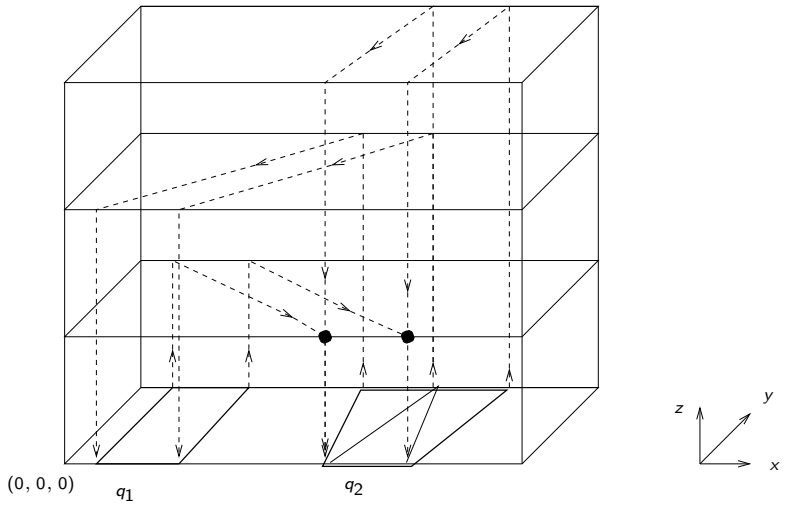
- Oded: let us extend decidability to 3D, nD.
- Eugene: no, no, no
- We learn how to program a stack by a 3D PCD, a Turing machine in 4D, then 3D PCD (very funny)
- By usual CS black magic $\Rightarrow$ reachability undecidable in 3D PCD
- all the hopes are broken!

An illustration : 3DPCD

Simulation of PDAs by PCDs

- Put the appropriate element for each state and connect via "bands" that "carry" the stack value
- A PCD for the PDA defined by:

$q_1 : S :=\text{PUSH}(1, S)$; GOTO q_2;
$q_2 : (v, S) :=\text{POP}(S)$; If $v = 1$ THEN GOTO q_2 ELSE GOTO q_1



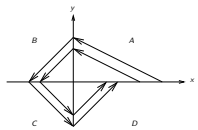
- Every PDA can be simulated by a 3-dimensional PCD system

Mathematical fantasy: theoreticians go wild

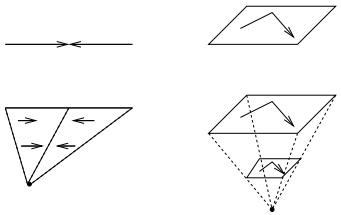
- If we allow Zeno behaviors, PCD are stronger than Turing machines
- We learned how to program Zeno PCD with transfinite broken trajectories
- Zeno PCD can decide any arithmetic predicat
- Very strange body of work, especially for Oded
- Gave birth to one brilliant researcher (O. Bournez)!

Gadgets used in the Construction

- Division by 2:



- Projectivisation:



- Corollary: PCDs can realize the whole arithmetical hierarchy

Summary of results on PCD

- Algorithm for deciding reachability problems (between two points, between two regions)

  [O. Maler and A. Pnueli, Reachability Analysis of Planar Multi-Linear Systems, 1993]

- Proof of undecidability for 3 dimensions by showing that PCDs can simulate any Turing Machine (2PDA)

  [E. Asarin and O. Maler, On some Relations between Dynamical Systems and Transition Systems, 1994]

- Proof (using Zeno paradox) of how all the arithmetical hierarchy can be realized by PCDs

  [E. Asarin and O. Maler, Achilles and the Tortoise Climbing Up the Arithmetical Hierarchy, 1995]

Technical Follow-ups and Impacts

- A generalization to planar differential inclusions (Asarin, Pace, Schneider and Yovine)
- Decidability boundaries for linear hybrid automata (Henzinger et al., partly earlier, partly later)
- Stability of Polyhedral Switched Systems (M. Viswanathan, P. Prabhakar et al.)
- A new paradigm of analog computation (O. Bournez et al.)
- Approximation of continuous systems by tractable piecewise simpler derivative systems (by various researchers from both CS and control sciences)

Intellectual Impacts

These theoretical results came with

- some **disappointment** (we cannot answer anything, even about systems with such simple continuous dynamics!)
- **new motivation** for researchers in verification
  - How to handle continuous dynamics? $\Rightarrow$ Change of point of view
  - In the continuous world, seeking exact answers is not wise
  - More meaningful to seek approximate answers on more complex systems with non-trivial continuous dynamics

Intellectual Impacts

Not only theoretical results, but also **effort to look from the perspective of the others**

"*Hopefully, this will provide control theorists and engineers with an additional perspective of their discipline as seen by a sympathetic outsider, uncommitted to the customs and traditions of the domain*" (Control from Computer Science, IFAC Annual Reviews in Control, Oded Maler, 2003)

- **attention** and **enthusiasm** in the **control theory** community who began to embrace **formal methods**
- creation of **conferences**, in particular HSCC (Hybrid Systems: Control and Computation) conference series, started in 1998
- **joint projects** (such as European projects VHS (Verification of Hybrid Systems) 2001, CC (Control and Computation) 2005, PROSYD (Property-based System Design) 2007)

Part II

Towards d/dt

Hybrid Systems II: Challenge Updated

New challenge

Compute approximately the ReachSet of continuous and hybrid systems. If possible take care of inputs, disturbances etc.

Remarks

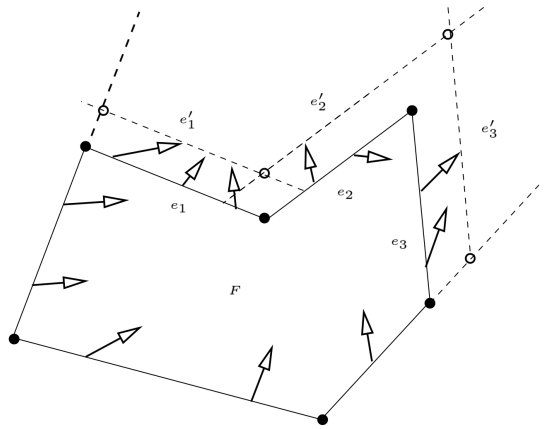
- A key to practical approximated verification of HS
- Requires synergy of Verification, Control and Numerics
- First step: choose a representation for sets in $\mathbb{R}^n$
- Second: compute their evolution

First attempts (too much CS)

- Approximating continuous dynamics by timed automata (UPPAAL, KRONOS) and linear hybrid automata (HYTECH) [Stursberg, Henzinger, et al.]
- The resulting approximate models are too large

(Ambitious) Reachable Set Computation

$$\dot{x} = f(x), \text{any } f$$

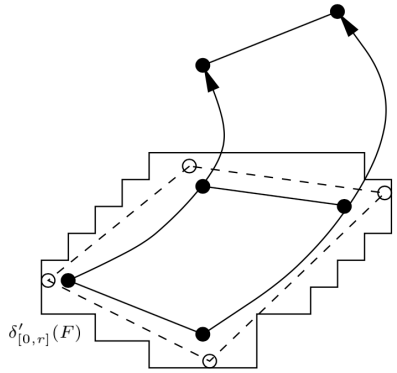


- Via face lifting due to continuity of trajectories
- Set-based Euler integration scheme

[Dang and Maler 1998]

(Less ambitious and more thoughtful) Reachable Set Computation

$$\dot{x} = Ax$$



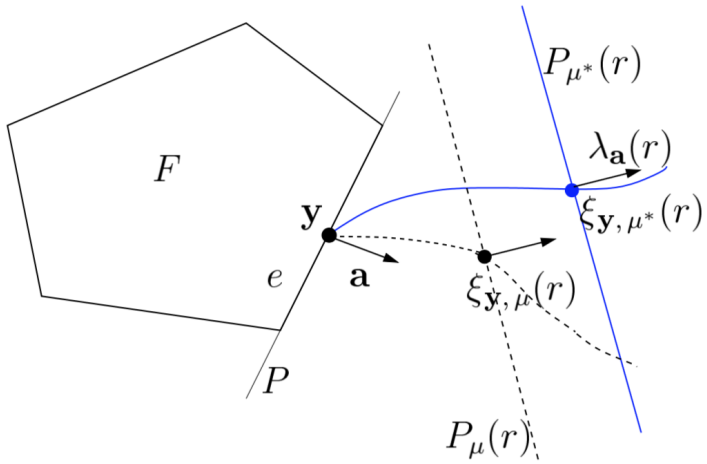
- Using convex and orthogonal polyhedra, exploiting structural properties, tool **d/dt** [Asarin, Bournez, Dang, Maler 2000]

Related work

- **CheckMate** [Chutinan, Krogh 1999] (convex-polyhedron based reachability, for abstraction purposes)
- **Ellipsoidal calculus** [Kurzhanski, Varaiya 97], **Level sets**[Mitchell,Tomlin 00], **MPT tool** [Morari et al]

Systems with Uncertain Input - Optimal Control

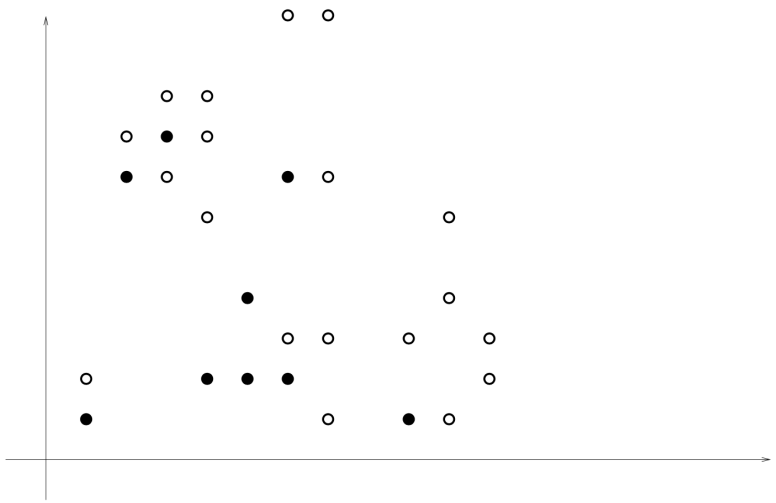
$$\dot{x} = Ax + u$$

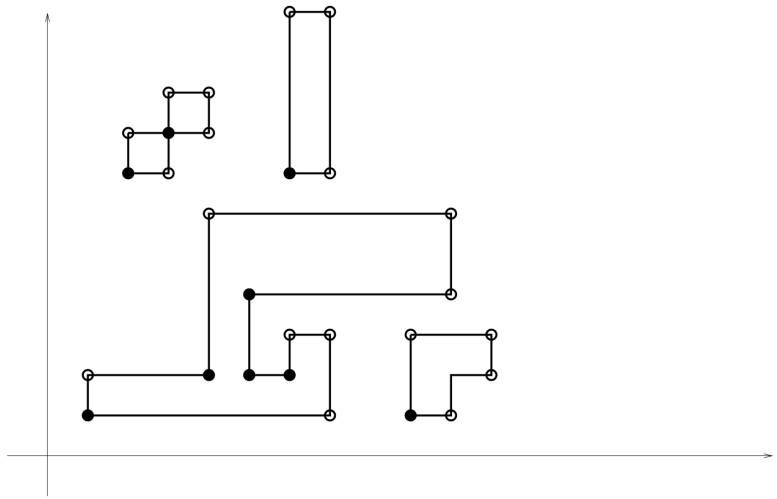


- Adjoint system: $\dot{\lambda}_{\mathbf{a}} = -A^T\mathbf{a}$
- $\mu^*(t)$ optimal input that drives the system furthest in the direction of $\lambda_{\mathbf{a}}(t)$

Orthogonal Polyhedra

- **Non-convex** set representation, crucial ingredient
- Orthogonal polyhedra, represented by **colored vertices**
- Collaboration with Olivier Bournez
- Used for modelling constraints of timed PV programs [Dang and Genet 2006]





Reachable Set Computation - Impacts

- Opened a direction for exporting algorithmic verification to continuous and hybrid systems
- Not limited to verification, useful for **control synthesis**
- Well-accepted by both model-checking and control communities, and recently attracted researchers from program verification/abstract interpretation
- Reachable set computation has become a **central problem** in hybrid systems research

Part III

Boosting reachability analysis

21st century challenges for HS reachability

- do not desperate
- do something with dimensionality curse
  - better data structures
  - better algorithms
- do something with nonlinearity
- make usable tools
- extend applicability niche

New progress around Oded

- new collaborators: A.Girard, C.Le Guernic
- new data structures for sets:
  - a normal one: zonotopes
  - a crazy CS one: lazily computed support functions
- new algorithmics

Another Oded's slide

Linear Reachability: State of the Art

- New algorithmics by C. Le Guernic and A. Girard
- Efficient computations: linear transformation applied to fixed number of points in each iteration
- No accumulation of over-approximation errors
- Initially used **zonotopes**, a class of sets closed under both linear operations and Minkowski sum; Can be applied to any "lazy" representation of the sequence of the computed sets
- Based on the observation that two consecutive sets

$$\begin{aligned} P_k &= A^k P_0 \oplus A^{k-1} V \oplus A^{k-2} V \oplus \ldots \oplus V \\ P_{k+1} &= A^{k+1} P_0 \oplus A^k V \oplus A^{k-1} V \oplus \ldots \oplus V \end{aligned}$$

  share a lot of terms
- Can compute within few minutes the reachable set after 1000 steps for linear systems with 200 (!) state variables

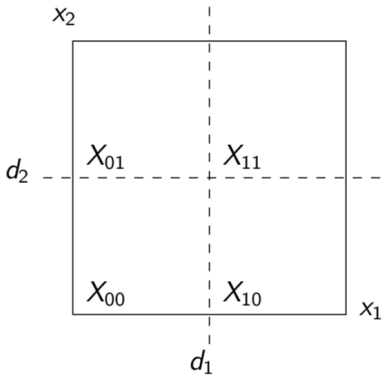
Nonlinearity challenge

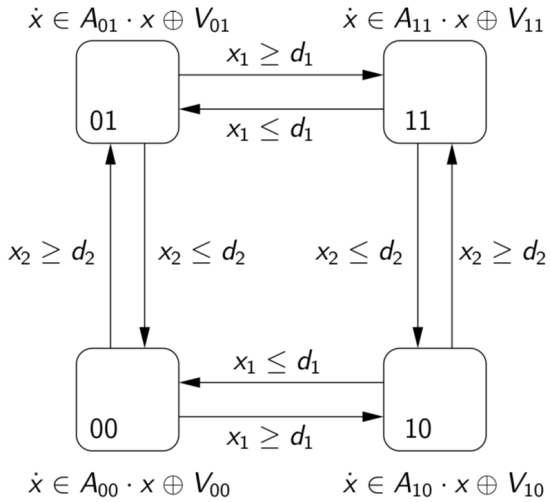
There are good tools for reachability in linear systems, how to do nonlinear ones? By reduction!

Hybridization: reducing nonlinear systems to piecewise linear ones

Hybridization (Asarin, Dang, Girard, Maler, around 2003)

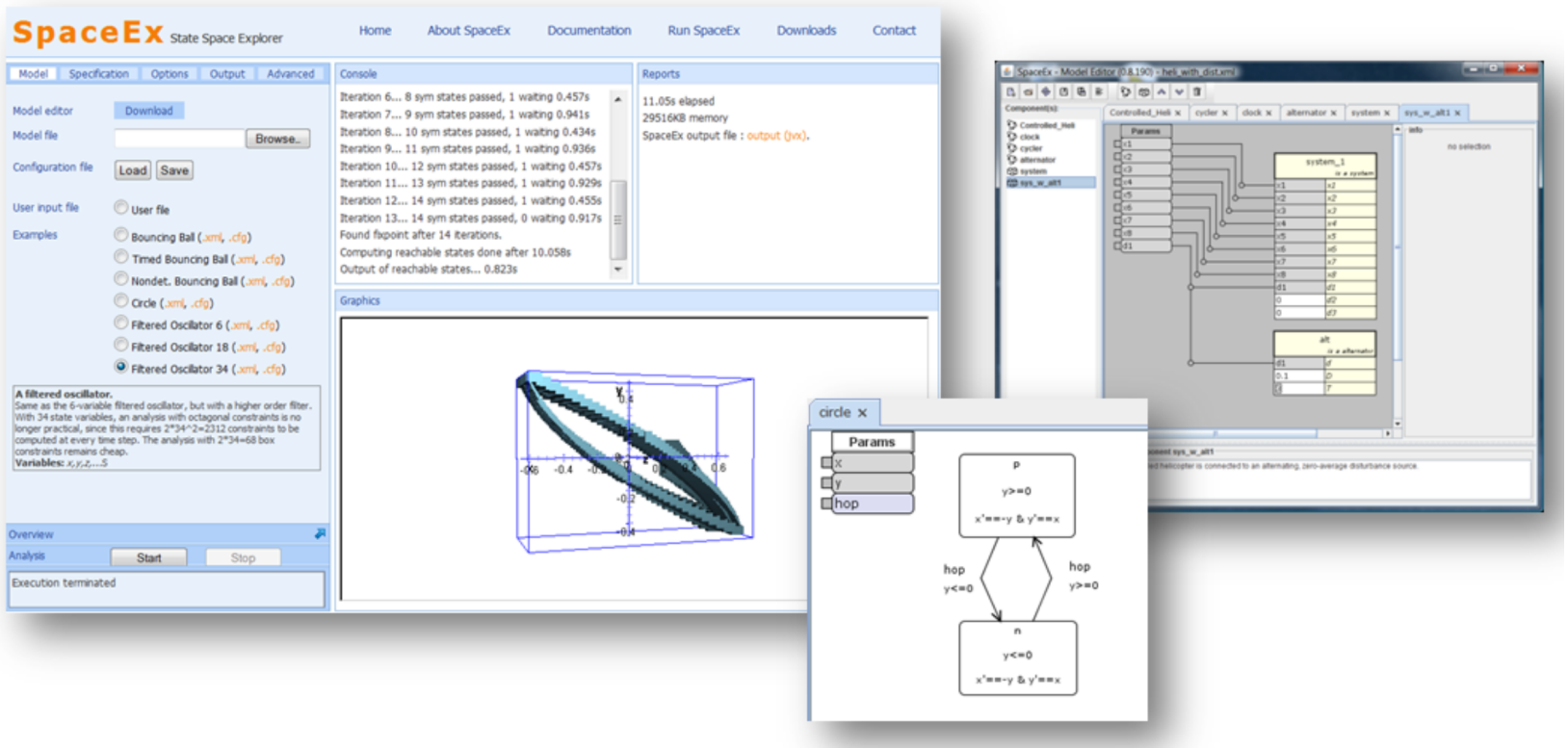
- $\dot{x} = f(x)$ and partition the state space into domains
- In each domain X_q, $f(x) \in A_q x \oplus V_q$ for every $x \in X_q$
- A_q is a local linearization of f with error bounded by V_q
- A piecewise linear (with uncertain input) systemsı





SpaceEx - leading hybrid systems verification tool

"A small step in Space, a giant leap for Mankind!" usually quoted by Oded



[Goran Frehse, Colas Le Guernic, et al.]

Part IV

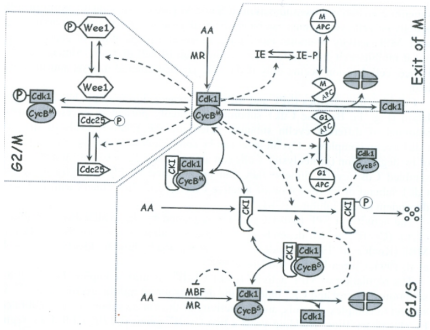
Is it usable?

Is it usable

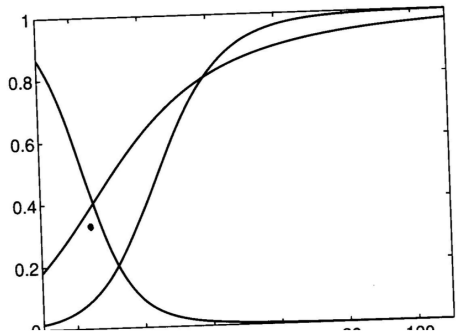
- Sometimes. . . You know better than me
- Important to find application domains
- Some are old, some are new: especially System biology

New exploration: Systems Biology

- Seek (conceptual and mathematical) models of dynamical systems at various levels of abstraction for **understanding** and **learning** about **underlying mechanisms**
- Relation between a dynamical system model which "explains" the mechanism AND experimentally observed behavior



and



- Need of dynamical models with which we can validate/falsify **hypotheses** and **predict**
- Some successful case studies

Maybe circumvent reachability

- reachability feasible and useful
- however full verification of HS based on reachability still difficult
- could do something else and lighter: e.g. monitoring/runtime verification bunch of work on STL, monitoring and parameter synthesis
- this follows the trend of CS verification
- not in this talk

Conclusion

25 years of optimism for an impossible challenge of HS reachability led to fantastic results, including this conference/week.