Model Generation for Hybrid Systems Verification in HYST

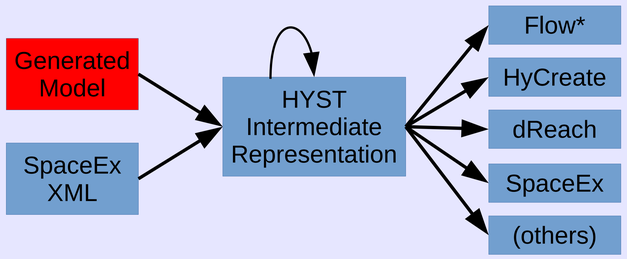
Stanley Bak[1], Sergiy Bogomolov[2], Taylor T. Johnson[3]

[1]Air Force Research Laboratory (AFRL), USA, [2]Institute of Science and Technology (IST) Austria, [3]University of Texas at Arlington (UTA), TX USA

Overview

HYST: a source-to-source translation tool for hybrid automaton models [4]. Three main functions:

- Model translation
- Model transformation
- New: Model Generation



Model transformations ease modeling and improve reachability analysis:

- Model Optimization
- Hierarchy Flattening
- Look-up Table Conversion
- Model-Order Reduction
- Automated Pseudo-Invariants [1]
- Continuization of Real-Time Controllers [5]
- Simulation-Guided Hybridization [3]

References

HYST is open source: https://github.com/verivital/hyst

[1] "High-level Hybrid Systems Analysis with Hypy", S. Bak, S. Bogomolov and C. Schilling, ARCH 2016, **Best Tool Award**

[2] "Chains of Integrators as a Benchmark for Scalability of Hybrid Control Synthesis", S. Livingston and V. Raman, ARCH 2016

[3] "Scalable Static Hybridization Methods for Analysis of Nonlinear Systems", S. Bak, S. Bogomolov, T. Henzinger, T. Johnson, P. Prakash, HSCC 2016, **Best Repeatability Evaluation Award**

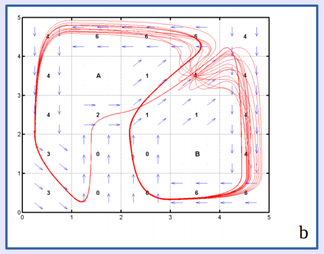
[4] "HYST: A Source Transformation and Translation Tool for Hybrid Automaton Models", S. Bak, S. Bogomolov, T. Johnson, Tools Paper, HSCC 2015

[5] "Periodically-Scheduled Controller Analysis using Hybrid Systems Reachability and Continuization", S. Bak, T. Johnson, RTSS 2015

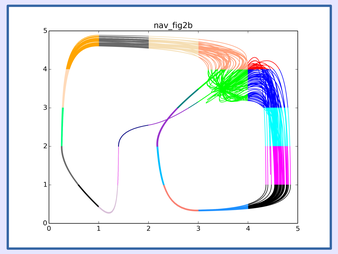
[6] "Benchmarks for Hybrid Systems Verification", Fehnker et. al, (HSCC 2004)

Model Generation

Navigation Benchmark [6] (others: Chains of Integrators Benchmark [2])



From Original Paper



Generated and Simulated

Dynamics: Velocities are steered towards target velocities:

$$\dot{\mathbf{v}} = A(\mathbf{v} - \mathbf{v}_d)$$

$$A = \begin{pmatrix} -1.2 & 0.1 \\ 0.2 & -1.2 \end{pmatrix}$$

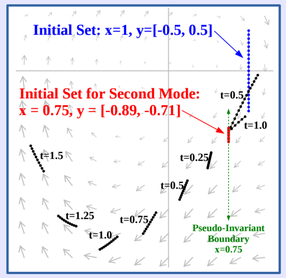
```
NAVIGATION BENCHMARK GENERATOR PARAMETERS:

-i_list i1 i2 ...          : space-separated list of target
                             velocity i value for each mode
                             , each i is 0-8 or 'A' or 'B'
-matrix a11 a12 a21 a22    : space-sepeated values of four-
                             element matrix A, like
                             '-1.2 0.1 0.1 -1.2'
-noise VAL                 : amount of input noise [-val,val]
                             to add to xvel and yel
                             (default: 0.0)
-prefix NAME               : mode name prefix (default: mode_)
-startx REAL               : x start position
-starty REAL               : y start position
-width WIDTH               : width of the grid (# of modes)
```

Model Transformation

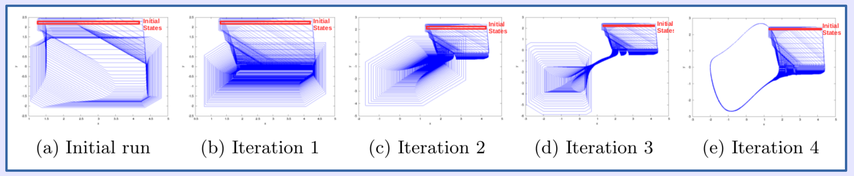
Transformation: Automated Pseduo-Invariants[1]

$$\begin{aligned} x' &= y \\ y' &= (1 - x^2) * y - x \end{aligned}$$

Vanderpol Dynamics



Auxiliary Hyperplane

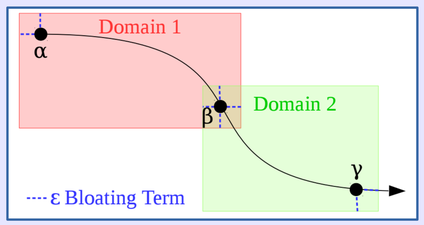


(a) Initial run (b) Iteration 1 (c) Iteration 2 (d) Iteration 3 (e) Iteration 4

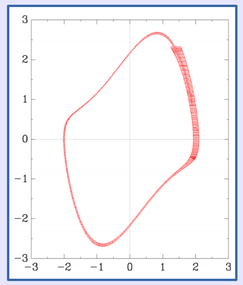
Multiple Iterations may be Necessary

➔ **Simulations are used to determine the placement of auxilary hyperplanes, improving accuracy.**

Transformation: Static Simulation-Guided Hybridization [3]



Simulation-Guided Domains

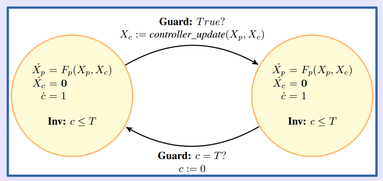


SpaceEx Result

➔ **Time-triggered transitions and limited linearization domains enable scalable abstractions for nonlinear systems.**

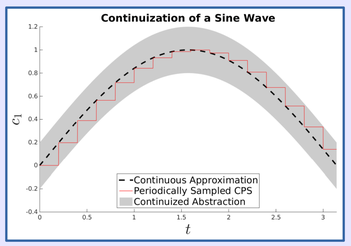
Transformation: Continuization of Real-Time Controllers [5]

➔ **Real-time scheduling guarantees periodic actuation for low-level controllers.**



Model of a Real-Time Low-Level Controller

➔ **Continuization enables analysis of such systems using continuous dynamics approximations with additional bounded noise.**



Enclosing Abstraction