StocHy: a new tool for the verification and control of stochastic processes

Nathalie Cauchi, Alessandro Abate

nathalie.cauchi@cs.ox.ac.uk, alessandro.abate@cs.ox.ac.uk

1. Introduction

StocHy supports the modelling and analysis of stochastic (hybrid) systems. It is an integrated yet modular framework centered around the discrete-time stochastic hybrid system formalism [1].

The tool allows for easy definition of stochastic processes and provides three main analysis tools (i) **simulation engine**; (ii) **formal verification** via abstractions; and (iii) **optimal policy synthesis**.

StocHy aims to:

- simplify the modelling process
- provide an integrated approach for formal verification and synthesis
- ease the adoption of stochastic models by non-expert users
- push forward research within the domain of stochastic

2. Models

We consider discrete time stochastic processes with discrete modes evolving according to:

$$x[k+1] = F(q[k], x[k], u[k]) + G(q[k])w[k]$$
$$q \in Q, x \in X \subset \mathbb{R}^m, u \in U \subset \mathbb{R}^n, w \in W \subset \mathbb{R}^r$$

where x, u are vectors if the system states and inputs respectively, Q is a finite set of discrete modes, $F : Q \times X \times U \to X$ is a (non)-linear function, $G : Q \times W \to W$ is the disturbance vector and w is a sequence of i.i.d Gaussian random variable with zero mean and variance σ^2.

The transitions between discrete modes may also depend on the system state and exogenous inputs,

$$q[k+1] = \delta_{ij}(q[k], x[k], u[k]).$$

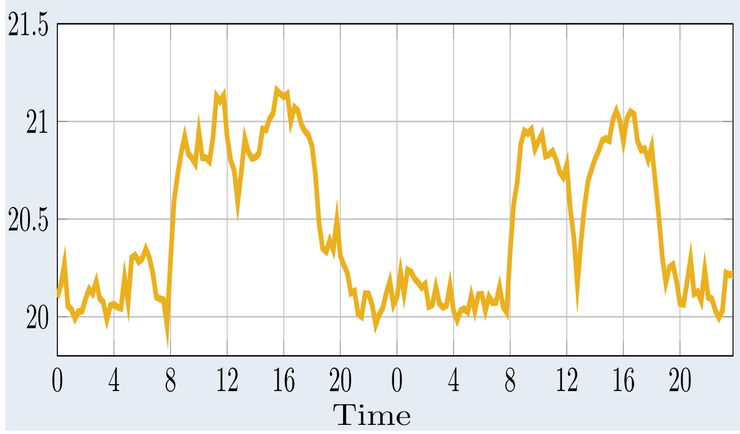
Here, $\delta_i j$ defines the condition for transitioning to new mode and act as *guards*.

Model dynamics

Simulation

1. Monte Carlo simulations
2. one plot per discrete mode

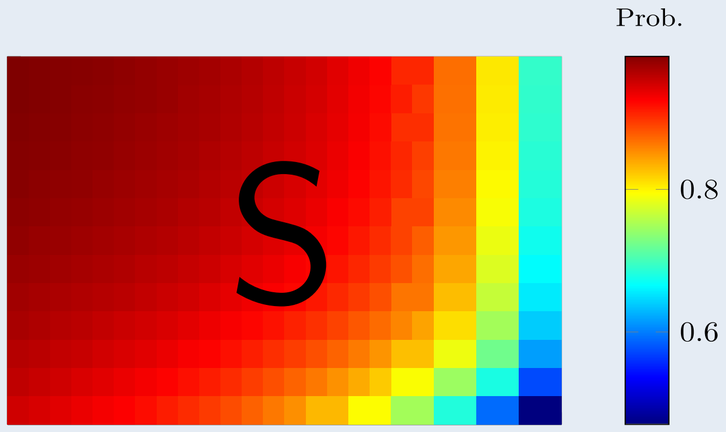
plot of continuous variable with time



Verification

1. formal abstractions of dynamics
2. probabilistic reachability analysis [2]

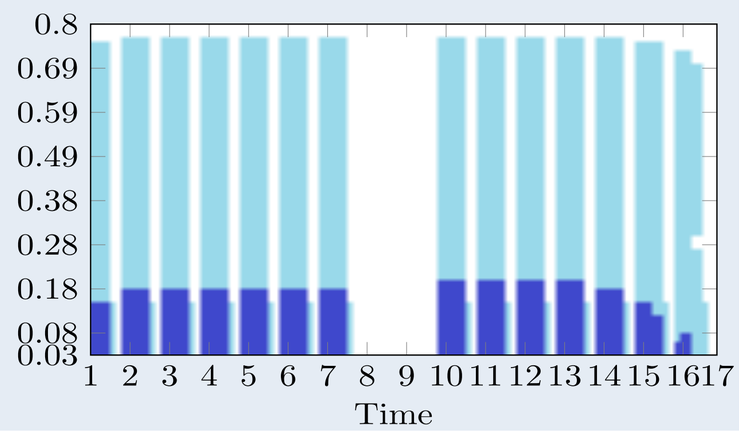
$$\Psi := \mathrm{P}_{=p}\left[\Box^{\leq N}\ \mathsf{S}\ \right]$$



Policy Synthesis

1. stochastic dynamic programming
2. control policy refinements via (ε, δ) - simulation relations [3]

look-up table: optimal control actions



StocHy: stochastic systems made easy!

3. Future work goals

- GUI interface for input model
- general formal modelling language for stochastic processes
- formal abstractions into interval Markov decision processes
- policy synthesis via reinforcement learning
- interfacing with other model checking tools in community

The toolbox will be issued soon!

References

[1] A. Abate, M. Prandini, J. Lygeros, and S. Sastry, "Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems," *Automatica*, vol. 44, no. 11, pp. 2724–2734, 2008.

[2] S. E. Z. Soudjani, C. Gevaerts, and A. Abate, "Faust^2: Formal abstractions of uncountable-state stochastic processes," in *Tools and Algorithms for the Construction and Analysis of Systems*, pp. 272–286, Springer, 2015.

[3] S. Haesaert, N. Cauchi, and A. Abate, "Certified policy synthesis for general markov decision processes: An application in building automation systems," *Performance Evaluation*, vol. 117, pp. 75–103, 2017.

[4] N. Cauchi and A. Abate, "Benchmarks for cyber-physical systems: A modular model library for buildings automation," in *IFAC Conference on Analysis and Design of Hybrid Systems*, 2018.

DEPARTMENT OF COMPUTER SCIENCE

UNIVERSITY OF OXFORD

OXFORD CONTROL AND VERIFICATION