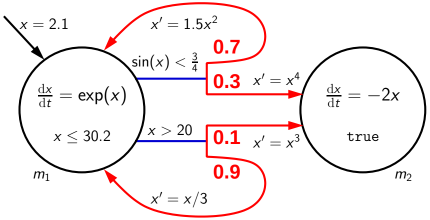
Analysis of Probabilistic Hybrid Automata



Probability of $\Diamond(m_2 \wedge x \leq -9.8)$*?*

Stochastic SMT−based Model Checking

$\exists trans \in \{1,2\} : \text{Я}_{[1\to 0.7, 2\to 0.3]} prob_1 \in \{1,2\} : \text{Я}_{[1\to 0.1, 2\to 0.9]} prob_1 \in \{1,2\} : \cdots$

$\wedge \Big(\big(m_1 \wedge trans = 1 \wedge \sin(x) < \frac{3}{4} \wedge prob_1 = 1\big) \Longrightarrow \big(x' = 1.5x^2 \wedge m'_1\big)\Big)$

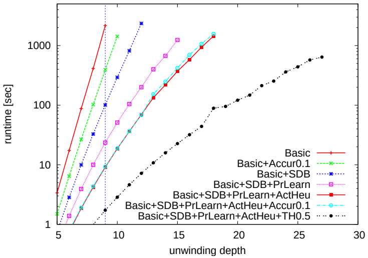
$\wedge \Big(\big(m_1 \wedge trans = 1 \wedge \sin(x) < \frac{3}{4} \wedge prob_1 = 2\big) \Longrightarrow \big(x' = x^4 \wedge m'_2\big)\Big)$

$\wedge \ \ldots$

State of affairs	*Future work*
Discrete−time / Scheduled event	Continuous−time
Bounded MC	Full MC (stochastic interpolation)
Reachability	Expressive logics Probabilistic stability
Probability results	Counter−examples

SSMT Algorithm

− Traversing quantifier tree
− SMT solver for quantifier−free subproblems
− Aggressive pruning rules for efficiency



Quantitative Program Semantics and Analysis

- Probabilistic Programming Languages
  - pccp [AGP97,ICCL98,MFCS98]
  - pKLAIM [Coordination04,SecCo04]
  - pCHAM [FMCO05]
  - pLambda [JLC05]
  - pWhile [APLAS07,ICICS08]
- Denotational and Operational Semantics
- Quantitative Static Program Analysis
- Quantitative Aspects in Computer Security
- Implementation Based on Linear Algebra

Quantitative Program Semantics and Analysis

- Probabilistic Programming Languages
- Denotational and Operational Semantics
  - Probabilities and Non-Determinism
  - Discrete Time vs Continuous Time
  - Operator Algebras [MFCS98,MFCSIT04]
  - Compositional Semantics [APLAS07]
- Quantitative Static Program Analysis
- Quantitative Aspects in Computer Security
- Implementation Based on Linear Algebra

Quantitative Program Semantics and Analysis

- Probabilistic Programming Languages
- Denotational and Operational Semantics
- Quantitative Static Program Analysis
  - Probabilistic Abstract Interpretation
  - Moore-Penrose Pseudo Inverse [PPDP00,LNCS4444]
  - Syntax Directed Semantics [JFP05,APLAS08]
- Quantitative Aspects in Computer Security
- Implementation Based on Linear Algebra

Quantitative Program Semantics and Analysis

- Probabilistic Programming Languages
- Denotational and Operational Semantics
- Quantitative Static Program Analysis
- Quantitative Aspects in Computer Security
  - Approximate Confinement [AGP00,CSFW02,CONCUR03]
  - Hypothesis Testing [CSFW02,TCS05,JCS04]
  - Most Effective Attacker [CSFW02,SAS02]
  - Timing Attacks and (Counter)Measures [SAS02,ICICS08]
  - Probabilistic Program Transformation [JLAP07,ICICS08]
- Implementation Based on Linear Algebra

Quantitative Program Semantics and Analysis

- Probabilistic Programming Languages
- Denotational and Operational Semantics
- Quantitative Static Program Analysis
- Quantitative Aspects in Computer Security
- Implementation Based on Linear Algebra
  - Sparse Matrices
  - Tensor Product
  - Octave and OCaml

Research interests

- process algebra for hybrid systems: HYPE
  - discrete and continuous behaviour
  - permits modelling of individual flows
  - compositionality as an important feature
  - Galpin, Hillston & Bortolussi, MFPS 2008, ENTCS 218, 2008
- spatial stochastic process algebra
  - addition of spatial aspects to PEPA
  - physically distributed systems, computer and biological
  - Galpin, AINA 2009, to appear
- semantic equivalences in discretised systems
  - behavioural equivalence between two discrete models of the same system

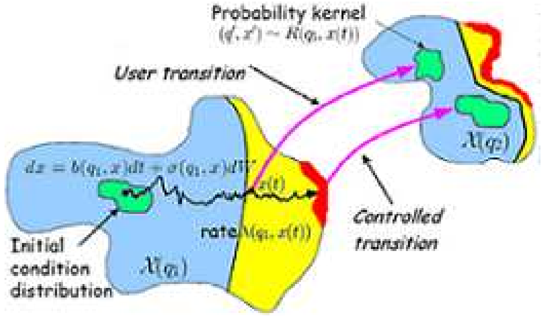
Application of logic to control problems using Multi-dimensional System co-Engineering

Manuela L. Bujorianu and Marius C. Bujorianu

Centre for Interdisciplinary Computational and Dynamical Analysis, University of Manchester

Multi-dimensional system co-engineering [1], abbreviated **MscE** [2], is a modeling framework that combines formal, mathematical and control engineering. It contains

- a reference model, called *colored stochastic hybrid systems* (cSHS),
- specification logics like SafAL (the Safety analysis logic), Hil (the Hilbertean logic), CSL (extended for continuous processes), united in the paradigm of *Hilbertian Formal Methods* [5]) for specification of safety and reachability properties, and
- a toolset for formal and dependable verification.



The cSHS combines a very general model of *stochastic hybrid systems* (SHS) [3] with runtime analysis information, modeled as colors. A SHS describes the evolution of a *hybrid system* (HS) under the influence of stochastic perturbations. A HS consists of a digital controller and a plant that can evolve in different modes, modeled as (deterministic or stochastic) continuous dynamical system. Moreover, the cSHS model is extended to communicating autonomous multi-agent systems [6]. Instances of this framework have been used to model and analyze systems forms air traffic control [4], [7]. Currently we explore the issues of modeling, control, coordination and verification for aerospace systems, such as (formations of autonomous) satellites.

[1] Multi-dimensional System Co-Engineering http://personalpages.manchester.ac.uk/staff/Manuela.Bujorianu/MScE.htm

[2] M.C. Bujorianu, M.L. Bujorianu and H. Barringer "A Formal framework for user centric control of multi-agent cyber-physical systems" in Michael Fisher, Fariba Sadri, Michael Thielscher Proceedings of the 9th International Workshop on Computational Logic in Multi-Agent Systems (CLIMA), Springer Verlag LNCS, 2009

[3] M.L. Bujorianu. "Extended Stochastic Hybrid Systems and their Reachability Problem" In: Proceedings Hybrid Systems: Computation and Control, HSCC 2004, pp. 234-249, Springer LNCS vol. 2993, 2004,

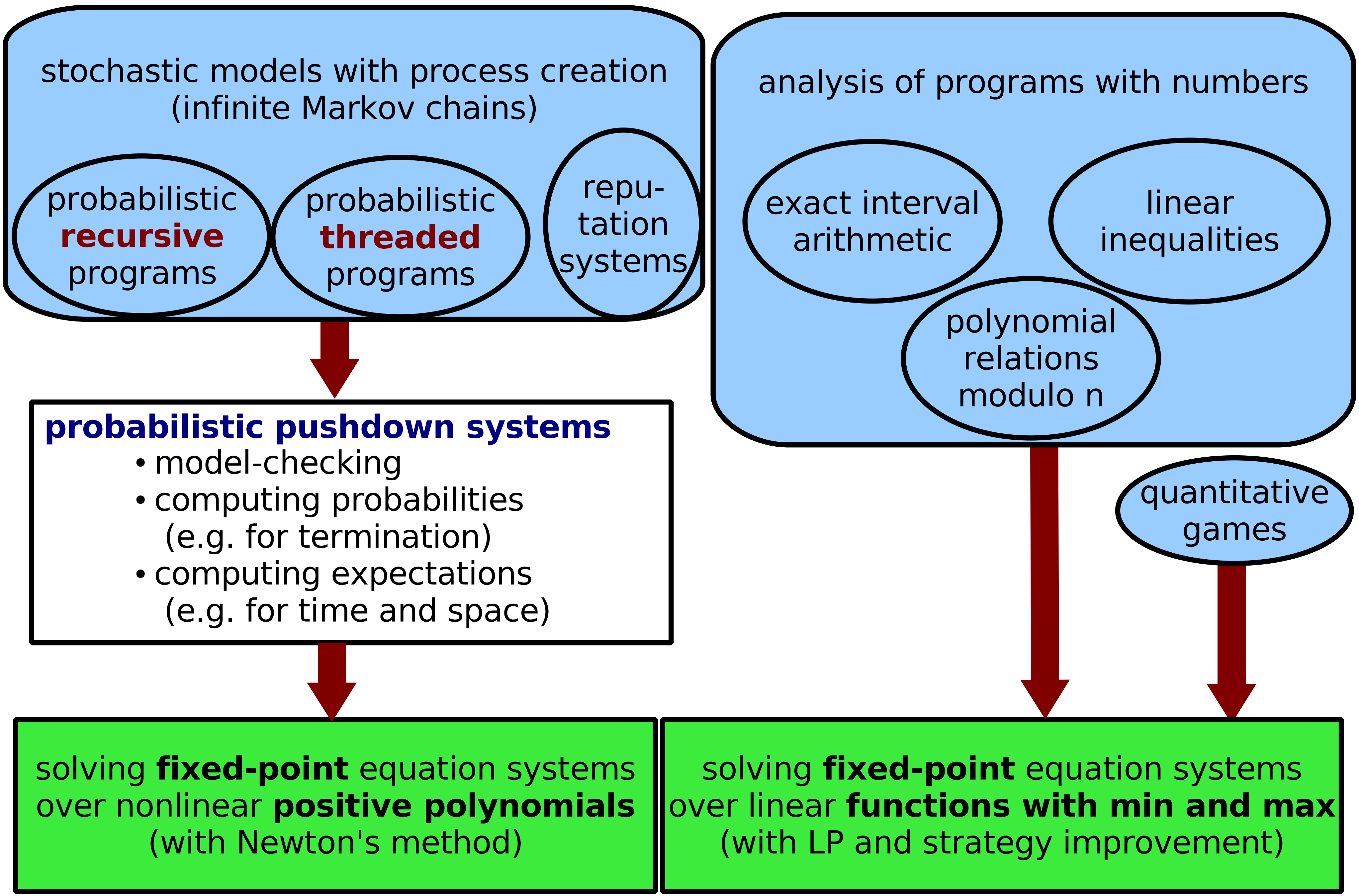
[4] Giordano. Pola, Manuela L. Bujorianu, John Lygeros and Maria Di Benedetto "Stochastic Hybrid Models: An Overview with Application to Air Traffic Management" In: 1st IFAC Conf. on Analysis and Design of Hybrid Systems, ADHS 2003, pp. 45-50, 2003

[5] M.C. Bujorianu and M.L. Bujorianu "Towards Hilbertian Formal Methods" Proceedings of Application of Concurrency to System Design ACSD'07, IEEE Computer Society Press, pp. 240-241, 2007

[6] M.C. Bujorianu and M.L. Bujorianu, and Savi Maharaj "Distributed Stochastic Hybrid Systems" In Horacek, P., Simandl, M. and Zitek, P., Proceedings of IFAC 2005, Elsevier Science Press 2005

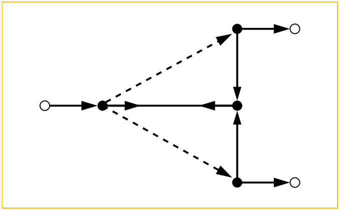
[7] Hybridge Distributed Control and Stochastic Analysis of Hybrid Systems Supporting Safety Critical Real-Time Systems Design http://www2.nlr.nl/public/hosted-sites/hybridge/

Quantitative Analysis at TU München
(Groups of Javier Esparza and Helmut Seidl)



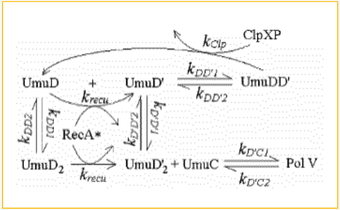
MLQA building blocks from CWI and TU/e

Stochastic Reo



- SOA and QoS
- Connector synthesis
- Dynamic adaptor modification

Formal cell processes



- Systems biology
- Stochastic process languages
- ODE vs. Gillespie vs. PCTL

stream calculus and coalgebra & control theory as discussed by Milad Niqui

Coalgebras

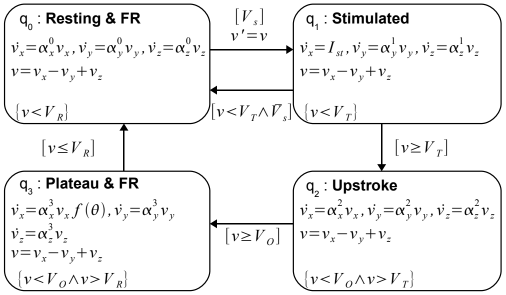
- Realisation of formal power series
- Stream calculus
- Exact arithmetic
- Coinduction
- (Bi)simulation & trace
- Temporal logic
- Automata

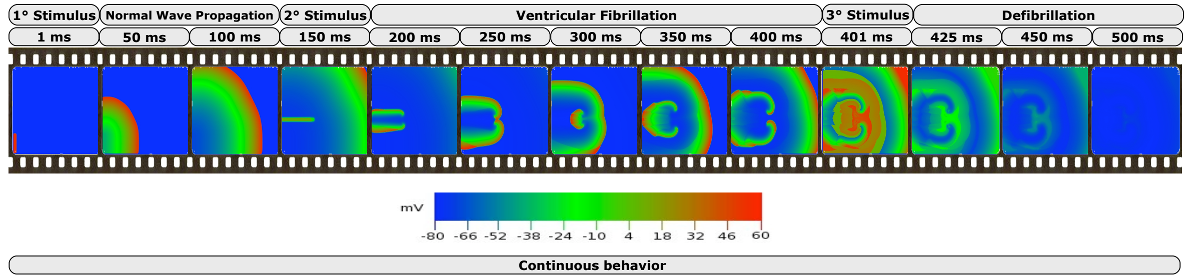
Embedded Systems

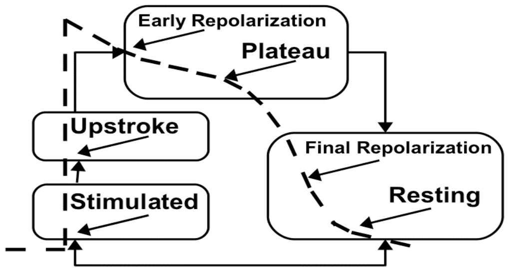
- Linear & rational systems
- Discrete event systems
- Continuous-time systems
- Smooth systems
- Hybrid systems

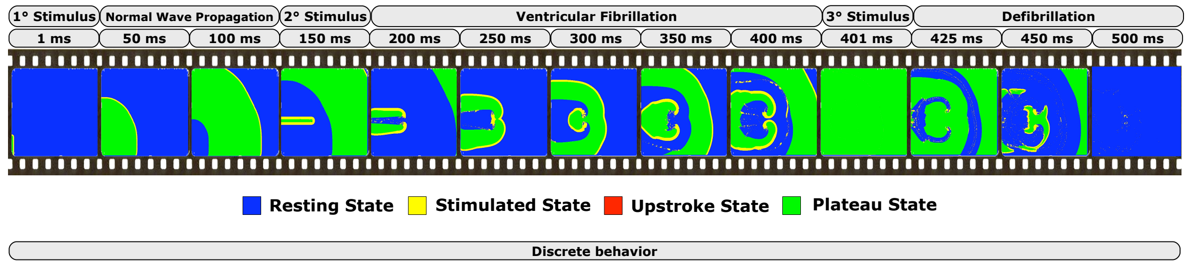
Service Oriented IT

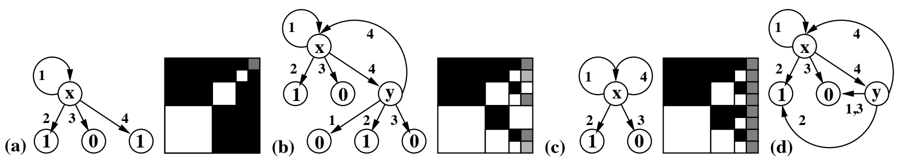
- Composition & hiding
- Coordination from outside
- Coinductive behaviour types
- Distributed systems

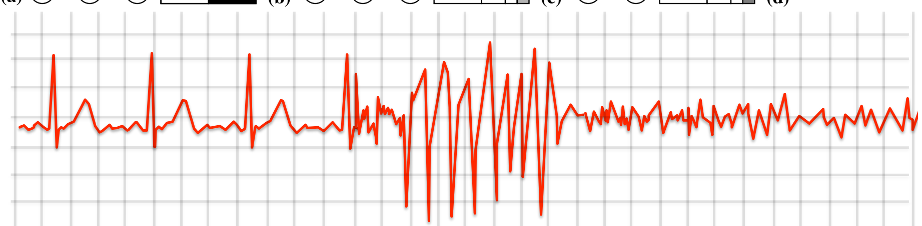








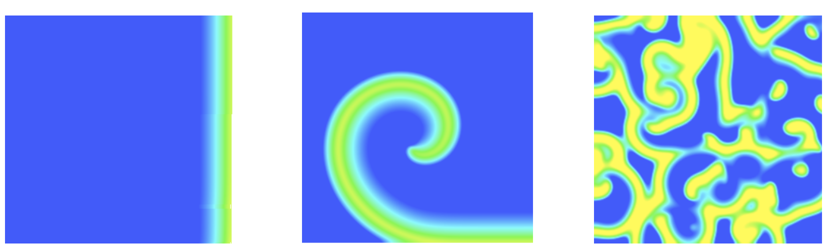




Normal Heart Rhythm

Ventricular Tachycardia

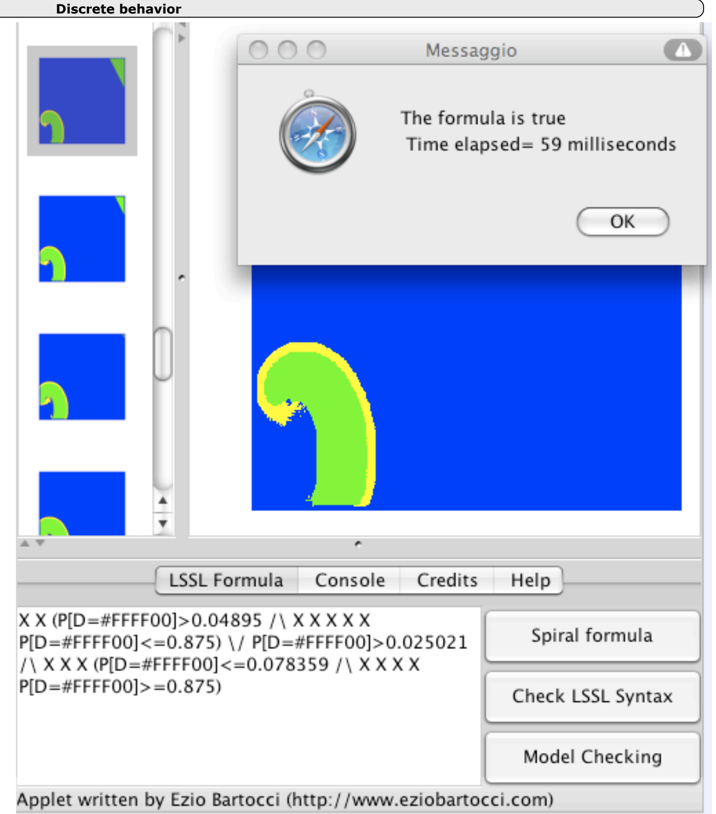
Ventricular Fibrillation



a) Normal Wave

b) Spiral Wave

c) Spiral Wave breakup



Henrikas Pranevicius,
professor, habil.dr.
Kaunas Univ. of Technology, Lithuania

www.vik.ktu.lt

PLA model = <Piece-linear Markov process,

aggregate system, controlling sequences>

PLA specification:

Verification | Simulation

Software tools for PLA:

- Verifier;
- Simulator;
- Automated model creator for Markov processes.

Applications:

- telecommunication protocols;
- business systems;
- biomedicine.

Modifications:

- hybridPLA;
- MarkovPLA;
- dynPLA.

Research Interests

- hybrid process calculi in the context of

Flying Sensors (Present)

- ▷ $n > 1$ picosatelites fulfill tasks using cooperative and dynamic trajectory coordination
- ▷ *some problems:* energy, complex algorithms, swarm behaviour
- ▷ to be sponsored by the DFG?

- stochastic process calculi in the context of

Analysis of Peer-to-Peer Algorithms (Past)

- ▷ modeling using a distributed stochastic process calculus
- ▷ specification using the markov chain based logic CSL
- ▷ verification by model checking after statespace reductions

General process algebraic specification

$$X = a \cdot b \cdot X + c \cdot X$$

Symbolic Translation of Stochastic Processes

General process algebraic specification

$$X = {}^{1}a \cdot {}^{2}b \cdot X + {}^{1}c \cdot X$$

Symbolic Translation of Stochastic Processes

General process algebraic specification

$$X = {}^{1}a \cdot {}^{2}b \cdot X + {}^{1}c \cdot X$$

Linear format

$$\begin{aligned} X(pc) = & \\ & pc = 1 \Rightarrow a \cdot X(2) \\ + & pc = 1 \Rightarrow c \cdot X(1) \\ + & pc = 2 \Rightarrow b \cdot X(1) \end{aligned}$$

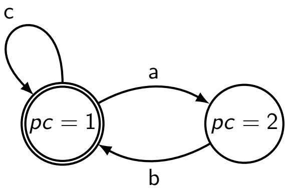
Symbolic Translation of Stochastic Processes

General process algebraic specification

$$X = {}^{1}a \cdot {}^{2}b \cdot X + {}^{1}c \cdot X$$

Linear format

$$\begin{aligned} X(pc) = \\ & pc = 1 \Rightarrow a \cdot X(2) \\ + & pc = 1 \Rightarrow c \cdot X(1) \\ + & pc = 2 \Rightarrow b \cdot X(1) \end{aligned}$$



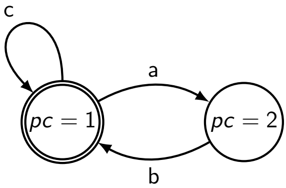
Symbolic Translation of Stochastic Processes

General process algebraic specification

$$X = {}^{1}a \cdot {}^{2}b \cdot X + {}^{1}c \cdot (0.5 : d \cdot X, 0.5 : e \cdot X)$$

Linear format

$$\begin{aligned} X(pc) = & \\ & pc = 1 \Rightarrow a \cdot X(2) \\ + & pc = 1 \Rightarrow c \cdot X(1) \\ + & pc = 2 \Rightarrow b \cdot X(1) \end{aligned}$$



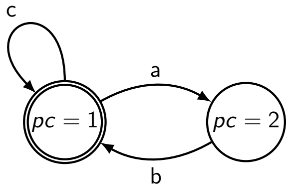
Symbolic Translation of Stochastic Processes

General process algebraic specification

$$X = {}^{1}a \cdot {}^{2}b \cdot X + {}^{1}c \cdot (0.5 : d \cdot X, 0.5 : e \cdot X)$$

Linear format

$$\begin{aligned} X(pc) = & \\ & pc = 1 \Rightarrow a \cdot X(2) \\ + & pc = 1 \Rightarrow c \cdot (0.5 : X(3), 0.5 : X(4)) \\ + & pc = 2 \Rightarrow b \cdot X(1) \end{aligned}$$



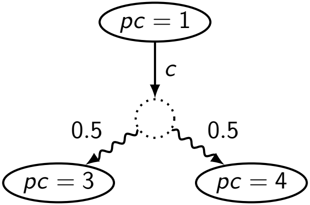
Symbolic Translation of Stochastic Processes

General process algebraic specification

$$X = {}^{1}a \cdot {}^{2}b \cdot X + {}^{1}c \cdot (0.5 : d \cdot X, 0.5 : e \cdot X)$$

Linear format

$$\begin{aligned} X(pc) = \; & \\ & pc = 1 \Rightarrow a \cdot X(2) \\ + \; & pc = 1 \Rightarrow c \cdot (0.5 : X(3), 0.5 : X(4)) \\ + \; & pc = 2 \Rightarrow b \cdot X(1) \end{aligned}$$



To use Model checking for Control design

Problem:
- Hybrid systems are undecidable
- Decidable models of CS are currently unusable

MLQA mission statement:

> "This spans [...] *resource usage* (e.g. 'the control system rotates and adjusts the windmill such that at least 60 % of the potential wind energy is utilised')."

- Highly non-linear system !
- Non-linear hybrid systems are undecidable
- State of the art: *Abstraction* to discrete system
- or to discrete-time or real-time system (*e.g.* timed automata)
- Problem: abstraction too coarse $\Longrightarrow$ unusable for most examples
- Badly need finer abstractions
- Good candidate: Priced timed automata
- Algorithms; tool support

Watch us in Aalborg...