Scalability in Formal Methods (from a CPS perspective)

Necmiye Ozay, EECS
University of Michigan, Ann Arbor

30 years of the Ramadge-Wonham Theory of Supervisory Control: A Retrospective and Future Perspectives Pre-conference Workshop, CDC 2017, Melbourne

Research partly funded by

Joint work with

For more recent results:
TuA09.6
WeC16.2
Formal methods for CPS

• Models for:
  – the system (usually hybrid/switched ODEs, with continuous/discrete inputs, disturbances and parametric uncertainty, sensors)
  – the environment (faults, external events)
• Formalized assumptions and requirements
  – linear temporal logic and its extensions
• Methods for verification and synthesis
  – algorithms that can process formal models and requirements to do analysis and control synthesis

Model-based approach

- Cyber-physical system
- Assumptions (on the unknowns, e.g., environment behavior)
- Requirements (on the system behavior)

System model
Formal specification

verification
synthesis

Correctness guarantee!
Scalability in Formal Methods

- For problems with continuous/hybrid dynamics two mainstream solution methodologies:
  - Abstraction-based: lift the problem to the discrete domain (use tools from DES or CS formal methods)
  - Continuous methods: apply fixed-point algorithms in the continuous domain or use functional deductive reasoning
  - Methods in between

- Fundamental problem: curse of dimensionality
  - Abstraction-based: # of discrete-states grows exponentially with continuous state dimension (state space explosion)
  - Continuous methods: set representations & manipulations in high dimensions is hard
Landscape of current methods*

Many factors affecting scalability:
- State-space dimension
- Complexity of the dynamics
- Complexity of the specifications
- Strength of conclusions (complete vs. sound)
- Accuracy of the results (correct vs. approximate)
- Ability to handle uncertainty, non-determinism
- etc.

* disclaimer: as any categorization, this will incomplete and inaccurate when done wrt few factors...
Verification landscape

Cyber-Physical

Large complexity gap induced by design process!!

Hybrid dynamics

NL w/ constraints

NL

LTI w/ constraints

LTI

Real-time SW

SW w/ branching

static linear SW

Boolean Satisfiability (SAT)/Satisfiability Modulo Theory (SMT)

Sum of squares

LMIs

Forward reachability (Flow*, C2E2, SpaceX, dReach)

Abstractation-based Verification (CEGAR)

Timed model checking (UPPAAL)

Model checkers (SPIN, NuXMV)

Static/syntax/non-functional

Stability

Finite time safety/reach avoid

LTL (infinite horizon)

STL/MTL

Sampling/simulation based falsification methods (Monte Carlo)
Synthesis for continuous/hybrid systems (incomplete list!)

- Hard state/input constraints, hybrid dynamics, complex specifications (e.g., temporal logics)
  - Belta, Fainekos, Girard, Liu, Pappas, Tabuada, Wongpirosarn, Zamani...
- Applications (with “small” state-space dim.)
  - Robotics, building thermal management, adaptive cruise control, aircraft subsystems, traffic control
Synthesis for continuous/hybrid systems (incomplete list!)

• Hard state/input constraints, hybrid dynamics, complex specifications (e.g., temporal logics)
  – Belta, Fainekos, Girard, Liu, Pappas, Tabuada, Wongpiroonsarn, Zamani...

• Applications (with “small” state-space dim.)
  – Robotics, building thermal management, adaptive cruise control, aircraft subsystems, traffic control

• “Medium”-scale systems
  – Monotonicity (Hafner & Del Vecchio 11, Coogan & Arcak 15)
  – Multi-scale abstractions for safety (Girard et al. 13)
  – Compositional synthesis (Nilsson & Ozay, Chen et al., Kim et al., Filippidis&Murray), incremental abstractions (Nilsson & Ozay)
Some examples of what we can do...

Compositional synthesis of **autonomous driving functions**:  
- Adaptive cruise control  
- Lane-keeping controller

\[
x_1^+ = A^1(x_2)x_1 + B^1u_1 + F^1(x_2),
\]

\[
x_2^+ = A^2(x_1)x_2 + B^2u_2 + F^2(x_1),
\]

Key idea: quantify the interdependence between subsystems and design robust controllers for subsystems separately

7D – nonlinear system  
with Stan Smith & Petter Nilsson, CDC 16

**Thermal management of fuel cells:**  
- Discrete and continuous actuators  
- Complex specifications  
- 5D-7D highly nonlinear system

Key idea: mixed monotonicity of dynamics and polarization curves – incremental abstraction - synthesis

with Liren Yang & Ford Research, ACC 17
Synthesis for continuous/hybrid systems (incomplete list!)

- Hard state/input constraints, hybrid dynamics, complex specifications (e.g., temporal logics)
  - Belta, Fainekos, Girard, Liu, Pappas, Tabuada, Wongpiyonsarn, Zamani...
- Applications (with “small” state-space dim.)
  - Robotics, building thermal management, adaptive aircraft subsystems, traffic control
- “Medium”-scale systems
  - Monotonicity (Hafner & Del Vecchio 11, Coogan & Arcak 15)
  - Multi-scale abstractions for safety (Girard et al. 13)
  - Compositional synthesis (Nilsson & Ozay, Chen et al., Kim et al., Filippidis&Murray), incremental abstractions (Nilsson & Ozay)
- “Large”-scale (but not synthesis)
  - Parametric verification of rectangular hybrid automata (Johnson & Mitra 12)
  - Abstractions of large collections of stochastic systems (Soudjani & Abate 15)

Recurring theme: structural properties
Large collections of systems

Example 1: Emergency response with a robotic swarm

- Deploy a large collection of robots (e.g., quadrotors, ground vehicles) for search and rescue mission
- Plan trajectories by taking dynamic constraints into account
- Requirements:
  - Sufficiently many robots in certain areas at any given time
  - Not too many robots in certain regions (danger zones)
  - Collision avoidance
  - Charging/reporting constraints
Large collections of systems

Example 2: Coordination of thermostatically controlled loads (TCLs)

- Thermostatically controlled loads (e.g., refrigerators, air conditioners, water heaters) for demand response
- Thermal dynamics can be controlled via ON/OFF switches
- Requirements:
  - Not too many TCLs ON at the same time (to avoid line overload)
  - Sufficiently many ON all the time (to utilize renewable energy)
  - Local temperature constraints (never out of desired temperature range)
Common structural properties

• Large number of systems, small number of classes
• Counting constraints: “how many in each mode?”, “how many in what region?”
• Identity of individual systems is not important

For simplicity, assume:
• dynamics are identical within each class
• (wlog) there is only one class
Mathematical formulation: TCLs

The temperature $\theta_i$ in a room with a TCL has dynamics

$$\dot{\theta}_i = \begin{cases} f_{on}(\theta_i), & \text{if TCL is on} \\ f_{off}(\theta_i), & \text{if TCL is off} \end{cases}$$

Suppose we have a collection of rooms with TCL’s $\{\theta_i\}_{i \in [N]}$.

- Customers: Want room temperature to be close to a desired temperature $\theta_i^{des}$, but small deviations are allowed.

$$\|\theta_i - \theta_i^{des}\| \leq \Delta \quad (1)$$

- Utility company: Wants to control aggregate demand, i.e. the number of TCLs that are on

$$\sum_{i=1}^{N} 1_{\{\text{TCL } i \text{ is on}\}} \quad (2)$$

Goal: Find a switching (i.e., on/off) strategy that exploits the flexibility in (1) so that (2) can be controlled.
Mathematical formulation: General

• $N$ identical switched system with $M$ modes:

$$\dot{x}_i(t) = f_{\sigma_i(t)}(x_i(t)), \quad \sigma_i : \mathbb{R} \mapsto [M],$$

• Mode-specific unsafe sets: $\mathcal{U}_m$, $m \in [M]

  • Equivalent to forced mode switches.

• Mode-counting bounds:

$$K_m \leq \sum_{i=1}^{N} 1_m(\sigma_i(t)) \leq \overline{K}_m \quad (3)$$

Want to synthesize a switching strategy $\sigma_i$ such that (3) satisfied over time.

**Structural property:** both the dynamics and the specification (counting constraints) are permutation invariant!
Solution overview

• Construct symbolic abstractions and aggregate dynamics and define “equivalent” problems on these structures
• (Analyze abstractions to understand fundamental limitations if any)
• An optimization-based solution approach
• Analysis of the solution approach
Abstraction of individual dynamics

- Assume dynamics are $\delta$-GAS with $KL$ functions $\beta_m$

$$\|\phi_t^m(x) - \phi_t^m(y)\|_\infty \leq \beta_m (\|x - y\|_\infty, t).$$ (4)
Abstraction of individual dynamics

• Assume dynamics are $\delta$-GAS with $KL$ functions $\beta_m$

\[
\|\phi^m_t(x) - \phi^m_t(y)\|_\infty \leq \beta_m (\|x - y\|_\infty, t). \tag{4}
\]

• With discretization in time ($\tau$) and space ($\eta$), an $\epsilon$-approximate bisimilar model is obtained if $\beta_m(\epsilon, \tau) + \frac{\eta}{2} \leq \epsilon$. 

Pola, Girard, Tabuada 08
Abstraction of individual dynamics

- Assume dynamics are $\delta$-GAS with $KL$ functions $\beta_m$

\[
\|\phi^m_t(x) - \phi^m_t(y)\|_\infty \leq \beta_m (\|x - y\|_\infty, t) .
\]

- With discretization in time ($\tau$) and space ($\eta$), an $\epsilon$-approximate bisimilar model is obtained if $\beta_m(\epsilon, \tau) + \frac{\eta}{2} \leq \epsilon$.

- Mode 1 abstraction
Abstraction of individual dynamics

- Assume dynamics are $\delta$-GAS with $KL$ functions $\beta_m$

$$\|\phi^m_t(x) - \phi^m_t(y)\|_\infty \leq \beta_m (\|x - y\|_\infty, t). \quad (4)$$

- With discretization in time ($\tau$) and space ($\eta$), an $\epsilon$-approximate bisimilar model is obtained if $\beta_m(\epsilon, \tau) + \frac{\eta}{2} \leq \epsilon$.

  - Mode 2 abstraction

mode-transition graph $G = (V, E)$
Some observations

- For a homogeneous collection, each system will have an identical mode-transition graph.
- Transition graphs are deterministic.

\[
\dot{x}_i(t) = f_i(t(x_i(t), d_i(t))),
\]

where \(d_i \in D\) (bounded parametric uncertainty or disturbance). If \(f_m(x, d)\) is \(L_m\)-Lipschitz in \(x\), and \(||f_m(x, d) - f_m(x, 0)|| \leq m\) for all \(d \in D\), then, with discretization in time (\(\Delta t, \delta\)) and space (\(\Delta s\)), an \(\varepsilon\)-approximate bisimilar model is obtained if

\[
\varepsilon \leq m L_m (\varepsilon L_m \Delta t + \delta)^2.
\]
Some observations

- For a homogeneous collection, each system will have an identical mode-transition graph
- Transition graphs are deterministic
- Consider mild heterogeneity

\[ \dot{x}_i(t) = f_{\sigma_i(t)}(x_i(t), d_i(t)), \quad \sigma_i : \mathbb{R} \rightarrow [M], \]

where \( d_i \in \mathcal{D} \) (bounded parametric uncertainty or disturbance). If \( f_m(x, d) \) is \( L_m \)-Lipschitz in \( x \), and

\[ \| f_m(x, d) - f_m(x, 0) \| \leq \delta_m \quad \text{for all} \quad d_i \in \mathcal{D}, \]

then, with discretization in time (\( \tau \)) and space (\( \eta \)), an \( \epsilon \)-approximate bisimilar model is obtained if

\[ \beta_m(\epsilon, \tau) + \frac{\delta_m}{L_m} (e^{L_m \tau} - 1) + \frac{\eta}{2} \leq \epsilon. \]
Aggregate dynamics on graph

Let $V = \{v_1, \ldots v_K\}$ denote the nodes of mode-transition graph $G = (V, E)$. Introduce the states $w_{k}^{m_1}$ and $r_{k}^{m_1,m_2}$.

- $w_{k}^{m}$ represents number of systems in mode $m$ at $v_k$.
- $r_{k}^{m_1,m_2}$ represents number of systems at $v_k$ that switch from $m_1$ to $m_2$.

The dynamics become

$$
(w_{k}^{m_1})^+ = \sum_{j \in N_k^{m_1}} \left( w_{j}^{m_1} + \sum_{m_2} r_{j}^{m_2,m_1} - r_{j}^{m_1,m_2} \right),
$$

- Constrained control actions:

$$
0 \leq \sum_{m_2} r_{k}^{m_1,m_2} \leq w_{k}^{m_1},
$$

- Compact description: $w^+ = Aw + Br$
**Theorem 1:**

Consider aggregate dynamics $\Sigma_{G} : \mathbf{w}^+ = A\mathbf{w} + B\mathbf{r}$ with safety and mode-counting constraints:

\[
\begin{align*}
  w^m_k(t) &= 0 \quad \forall k \in U_m, \quad (5) \\
  K_m &\leq \sum_{i \in [N]} w^m_i(t) \leq \overline{K}_m. \quad (6)
\end{align*}
\]

Then,

- if $\exists$ sequence of control inputs $\mathbf{r}^\omega$ for $\Sigma_{G}$ that enforce (5) and (6) with $U_m + B\epsilon$, then $\exists$ a solution to the original problem.
- if $\nexists$ a sequence of control input $\mathbf{r}^\omega$ for $\Sigma_{G}$ that enforces (5) and (6) with $U_m - B\epsilon$, then no solution to the original problem.

We will focus on aggregate dynamics. We need infinite horizon strategies!

**Solution strategy:** from a given initial state, steer the system, while respecting the constraints, to a **nice state** from which a periodic input suffices.
Solution strategy:

from a given initial state, steer the system, while respecting the constraints, to a **nice state** from which a periodic input suffices.

- **Prefix:** for a fixed horizon $T$, given initial state, we will steer the state at time $T$ to “**nice**” cycles
- **Suffix:** let individual systems circulate in the cycles

Mode-counting constraints

$$\Psi^m(C, \alpha) \geq K_m, \quad \Psi^m(C, \alpha) \leq K_m,$$

can be represented as linear constraints

$$K_m \mathbf{1} \leq Y^m_C \alpha \leq K_m \mathbf{1}$$

$Y^m_C$ is a circulant matrix.
Solution via linear programming

For cycles $C_1, \ldots, C_J$, required mode-counts $K_m$, horizon $T$

\[
\text{find } \alpha_1, \ldots, \alpha_J \text{ cycle assignments, } \\
r(0), \ldots, r(T - 1), \\
w(0), \ldots, w(T), \\
\text{s.t. } K_m < \sum_j \sum_{m_2} w^{m_2}_j(t) < K_m, \quad 0 < t < T - 1 \quad \text{mode-counting during prefix} \\
\sum_j \Lambda(w(t)) = \lambda_0, \\
w(t + 1) = Aw(t) + Br(t), \quad t = 0, \ldots, T - 1, \\
\sum r^{m_1,m_2}_j = w^{m_1}_j \quad \text{for all } j \in \bigcup_{i \in U_{m_1}} N^{m_1}_i, \\
\sum r^{m_2,m_1}_j = 0 \quad \text{for all } m_2 \in [M], j \in U_{m_1}, \quad \text{control constraints}.
\]

Feasibility problem with linear constraints:
- integrality constraints on the inputs (ILP)
- relaxing integrality (LP)

Number of constraints and variables are independent of the number of systems $N$!
Analysis

• **Integer solutions (ILP)**
  – **Completeness of prefix-suffix solutions:** There exists a finite T and some maximal cycle length L such that ILP with all cycles with length less than L provides a complete solution to the original problem
  – From any feasible ILP solution, we can extract a solution to the original problem

• **Non-integer solutions (LP):**
  – Enough to consider simple cycles
  – Gives certificates for non-existence of solutions

• **Rounding a non-integer solution:**
  – A non-integer solution over the cycles can be rounded to an integer feasible solution with mode counting loss at most

\[
\Psi^m(C, \alpha_{int}) \leq \Psi^m(C, \alpha_{avg}) + \frac{|C|}{4}
\]
Intuition behind cycles: TCLs

\[ \dot{\theta}_i = -a(\theta_i - \theta_a) - bP_m \]

\( \theta \): room temperature
\( \theta_a \): ambient temperature
\( P_m = 0 \) when OFF
\( P_m = 5.6 \) when ON

local safety
\( \theta_i \in [21.5, 23.5] \)

For an individual system if only local ON/OFF control is used (no demand response for extra switching), the temperature evolves as follows:

Parameters from Mathieu, Koch, Callaway, IEEE Trans. on Power Systems, 2013
Intuition behind cycles: TCLs

\[ \dot{\theta}_i = -a(\theta_i - \theta_a) - bP_m \]

\( \theta \): room temperature
\( \theta_a \): ambient temperature

\( P_m = 0 \) when OFF
\( P_m = 5.6 \) when ON

local safety
\( \theta_i \in [21.5, 23.5] \)

For an individual system if only local ON/OFF control is used (no demand response for extra switching), the temperature evolves as follows:

Roughly, cycles are defining new “bands” within the dead-band allowed by the local safety constraints. That is, we are changing the duty cycle.

Parameters from Mathieu, Koch, Callaway, IEEE Trans. on Power Systems, 2013
Results on TCLs

N = 10000 units

10000-D state-space with $2^{10000}$ modes!

\[
\dot{\theta}_i = -a(\theta_i - \theta_a) - bP_m
\]

$\theta$: room temperature

$\theta_a$: ambient temperature

$P_m = 0$ when OFF

$P_m = 5.6$ when ON

local safety

$\theta_i \in [21.5, 23.5]$

Parameters from Mathieu, Koch, Callaway, IEEE Trans. on Power Systems, 2013
Beyond mode counting

• Counting the agents in a region of state-space
• Time-evolution of counting constraints (counting LTL)
  \( \varphi ::= \text{True} \mid cp \mid \varphi_1 \land \varphi_2 \mid \neg \varphi \mid \bigcirc \varphi \mid \varphi_1 \mathcal{U} \varphi_2, \)
• \( cp = [\text{atom prop.}, \text{count}] \)
• Possible to count temporal specs
• Possible to encode asynchrony as well

With Yunus Emre Sahin & Petter Nilsson
ICCPS17
Summary: structure for scalability

- A control synthesis method for large collections of systems with counting constraints
  - exdy
  - wc
  - wi
  - ex

Preprints and more information available @ http://web.eecs.umich.edu/~necmiye/
Summary: structure for scalability

• A control synthesis method for large collections of systems with **counting constraints**
  – exploits the symmetry (*permutation invariance*) in the dynamics and in specifications
  – works across scales (10 to 10K or more systems)
  – with potential applications in different domains
  – extensions to asynchrony, counting temporal logic

• Current work
  – partial information
  – non-deterministic abstractions (for not incrementally stable systems), asynchronous switching
  – other types of symmetries that can be exploited
  – other approaches for scalability: decomposition, contracts

Preprints and more information available @ [http://web.eecs.umich.edu/~necmiye/](http://web.eecs.umich.edu/~necmiye/)