Exploiting System Structure in Formal Synthesis

Murat Arcak
with Sam Coogan and Eric Kim

Electrical Engineering and Computer Sciences, UC Berkeley
This Talk: Formal synthesis, motivated by traffic control

Outline:

1. Finite abstraction for formal methods
   
   Exploiting a “mixed monotonicity” property for scalability.
   
   Application to a macroscopic traffic flow model.

2. Compositional synthesis for large networks
   
   Decoupled synthesis for subnetworks with supply and demand contracts.
1. Finite Abstraction for Formal Methods

Capture the underlying dynamics with a finite set of symbols and transitions between them. Methods exist for classes of systems (Tabuada, Girard, Pappas, Reissig, Abate, Belta, and others…)

Example: polyhedral computations for piecewise affine systems (Belta et al.)
Monotonicity and Mixed Monotonicity

The discrete-time system:

\[ x^+ = F(x) \quad x \in \mathcal{X} \]

is monotone if

\[ x_1 \leq x_2 \quad \implies \quad F(x_1) \leq F(x_2) \]

with respect to a partial order (standard order in this talk).

Monotonicity offers strong dynamical properties [Hirsch, Smith, Angeli, Sontag] but is restrictive in practice.

Necessary and sufficient condition for monotonicity:

\[ \frac{\partial F_i(x)}{\partial x_j} \geq 0 \quad \forall x \in \mathcal{X} \quad \forall i, j \]
Monotonicity and Mixed Monotonicity

\[ x^+ = F(x) \quad x \in \mathcal{X} \]

is mixed monotone if there exists a “decomposition function”

\[ f : \mathcal{X} \times \mathcal{X} \rightarrow \mathcal{X} \]

such that

\[ f(x, x) = F(x) \]

\[ x_1 \leq x_2 \implies f(x_1, y) \leq f(x_2, y) \]

\[ y_1 \leq y_2 \implies f(x, y_2) \leq f(x, y_1). \]

A sufficient condition for mixed monotonicity:

\[ \exists \delta_{ij} \in \{-1, 1\} \quad \text{s.t.} \quad \delta_{ij} \frac{\partial F_i(x)}{\partial x_j} \geq 0 \quad \forall i, j \]

Decomposition function: \[ F_i(\cdots, x_j, \cdots) \text{ if } \delta_{ij} = -1 \]
Mixed Monotonicity Allows Scalable Finite Abstraction

Two function evaluations tightly bound the one-step reach set:

Monotone:

\[ F(\begin{pmatrix} x_2 \\ x_1 \end{pmatrix}) \subseteq \]

Mixed Monotone:

\[ F(\begin{pmatrix} x_2 \\ x_1 \end{pmatrix}) \subseteq \]

This allows a scalable abstraction algorithm:

[Coogan, Arcak, 2015]
Traffic Flow: a Macroscopic Model

\[ x_{\ell}^+ = x_{\ell} + f_{\ell}^{\text{in}}(x) - f_{\ell}^{\text{out}}(x) =: F_{\ell}(x) \]

For each link \( \ell \):

Outgoing links:
\[ f_{\ell}^{\text{in}}(x, m) = \sum_{\ell \in \text{in}} \beta_{\ell k} f_{\ell}^{\text{out}}(x, m) \]

Incoming links:
\[ f_{\ell}^{\text{out}}(x, m) = s_{\ell}(m) \min \left\{ \Phi_{\ell}^{\text{out}}(x_{\ell}), \min_{k \in \text{out}} \frac{1}{\beta_{\ell k}} \Phi_{k}^{\text{in}}(x_{k}) \right\} \]
Traffic Flow is Mixed Monotone

\[ \delta_{ij} \frac{\partial F_i(x)}{\partial x_j} \geq 0 \quad \delta_{ij} = \begin{cases} -1 & \text{if } i \text{ and } j \text{ share tail node} \\ +1 & \text{otherwise} \end{cases} \]

Apply abstraction algorithm and add signaling states to transition model

Note: Standard monotonicity breaks down at splits

\[ f_1^{\text{out}} = \frac{1}{\beta_{12}} \Phi_2^{\text{in}}(x_2) \]

\[ f_3^{\text{in}} = \beta_{13} f_1^{\text{out}} = \frac{\beta_{13}}{\beta_{12}} \Phi_2^{\text{in}}(x_2) \]

\[ \Rightarrow \delta_{32} = -1 \]
Example: Signal Control for a Corridor

Temporal Logic Specifications:

- Each signal actuates cross street traffic infinitely often.
- Eventually, links 1, 2, 3, and 4 have fewer than 30 vehicles each.
- The signal at junction 4 must actuate cross street traffic for at least two sequential time-steps.

Naïve offset optimal policy

Correct-by-design policy
2. Compositional Synthesis for Large Networks

[Kim, Arcak, Seshia, 2015]

- “Contracts” between neighboring subnetworks to limit demand and guarantee adequate supply
- Neighbors’ promises allow decoupled subnetwork models with set valued maps
- Augment temporal logic specifications with own promises and synthesize controller for each subnetwork

\[
\phi_i^{\text{new}} = \phi_i^{\text{original}} \land \phi_i^{\text{supply}} \land \phi_i^{\text{demand}} \quad i = 1, 2, \ldots
\]
Neighbors’ Promises Allow Decoupled Models

Subnetwork 2 promises a minimum supply of $\sigma_{2}\text{contract}$ on link 5 and to limit its demand on link 4 by $\delta_{4}\text{contract}$ vehicles per period.

Decoupled subnet 1 model:

\[
f_2^{out}(x) = \min \left\{ \Phi_2^{out}(x_2), \frac{1}{\beta_{25}} \Phi_5^{in}(x_5) \right\}
\]

\[
\in \min \left\{ \Phi_2^{out}(x_2), \frac{1}{\beta_{25}} \sigma \right\}, \quad \sigma \in [\sigma_2\text{contract}, \sigma_2\text{best}]
\]

\[
f_4^{in}(x) = \beta_{74} \min \left\{ \Phi_7^{out}(x_7), \frac{1}{\beta_{78}} \Phi_8^{in}(x_8), \frac{1}{\beta_{74}} \Phi_4^{in}(x_4) \right\}
\]

\[
\in \beta_{74} \min \left\{ \Phi_4^{in}(x_4), \delta \right\}, \quad \delta \in [0, \delta_{4}\text{contract}]
\]
Restrictions on the Specification

I. Separability: \( \phi_{\text{network}} = \phi_{\text{subnet } 1} \land \cdots \land \phi_{\text{subnet } N} \)

Then the \( i \)th subproblem is: \( \phi_{\text{subnet } i} \land \phi_{\text{i}}^{\text{supply}} \land \phi_{\text{i}}^{\text{demand}} \)

II. Easier to satisfy \( \phi_{\text{subnet } i} \) when \( i \)'s neighbors promise more

This allows a systematic search for contract parameters.

Example: The class of specifications

\[
\phi_{\text{subnet } i} = \Box \theta \land \Diamond \Box \gamma \land \{ \land_{j=1, \ldots, L} \Box \Diamond \nu_j \} \land \{ \land_{j=1, \ldots, M} \Diamond \kappa_j \}
\]

has this property if the dynamics are monotone and the propositions \( \theta, \gamma, \nu_j, \kappa_j \) are true on lower sets:

\[
x \leq \bar{x} \text{ and } \bar{x} \in S \Rightarrow x \in S
\]
**Proof idea in a picture:**

If subnet 2 promises more supply on link 5, then link 2 occupancy drops. Likewise less occupancy on link 4 if less demand is promised.

**Why monotonicity matters:**

If subnet 1 promises more supply on link 4, this liberates more flow out of link 7 and causes higher occupancy on link 8 (contrary to fig. above).
Acknowledgment: NSF-CPS grant CNS1446145 and coworkers:

Sam Coogan  
Calin Belta  
Roberto Horowitz

Eric Kim  
Sanjit Seshia  
Alex Kurzhanskiy
Related Publications

Coogan and Arcak “Efficient finite abstraction of mixed monotone systems” – HSCC 2015


Coogan and Arcak “Freeway traffic control from linear temporal logic specifications” – ICCPS 2014

Kim, Arcak and Seshia “Compositional controller synthesis for vehicular traffic networks” – to be presented at this conference