Formal Synthesis with Learning of Environmental Dynamics

Calin Belta

Mechanical Engineering and Systems Engineering
Boston University

CPS: Medium: Collaborative Research: Efficient Control Synthesis and Learning in Distributed Cyber-Physical Systems
Big picture
1. Formal Synthesis
2. Formal Synthesis with Learning of Environmental Dynamics
Conservative Formal Synthesis for Dynamical Systems

Problem Formulation

*Given* a control system and a temporal logic specification over a set of regions, *find* initial states and feedback control strategies such that all the trajectories of the closed loop system satisfy the specification.

\[ \dot{x} = f(x, u) \]

“Avoid the grey region for all times. Visit the blue region, then the green region, and then keep surveying the striped blue and green regions, in this order.”
Avoid the grey region for all times. Visit the blue region, then the green region, and then keep surveying the striped blue and green regions, in this order.

“(\pi_2 = \text{TRUE and } \pi_4 = \text{FALSE and } \pi_3 = \text{FALSE}) should never happen. Then \pi_4 = \text{TRUE and then } \pi_1 = \text{TRUE should happen. After that, } (\pi_3 = \text{TRUE and } \pi_4 = \text{TRUE}) \text{ and then } (\pi_1 = \text{TRUE and } \pi_3 = \text{FALSE}) \text{ should occur infinitely often.}”

“ Avoid the grey region for all times. Visit the blue region, then the green region, and then keep surveying the striped blue and green regions, in this order.”
Conservative Formal Synthesis for Dynamical Systems

Approach

\[ \Box \neg (\pi_2 \land \neg \pi_4 \land \neg \pi_3) \land \\
\Diamond (\pi_4 \land \Diamond (\pi_1 \land \Diamond \\
(\Box \Diamond ((\pi_3 \land \pi_4) \land \Diamond (\pi_1 \land \neg \pi_3)))))) \]

“(\pi_2 = \text{TRUE} \text{ and } \pi_4 = \text{FALSE} \text{ and } \pi_3 = \text{FALSE}) \text{ should never happen. Then } \pi_4 = \text{TRUE} \text{ and then } \pi_1 = \text{TRUE} \text{ should happen. After that, } (\pi_3 = \text{TRUE} \text{ and } \pi_4 = \text{TRUE}) \text{ and then } (\pi_1 = \text{TRUE} \text{ and } \pi_3 = \text{FALSE}) \text{ should occur infinitely often.”}

“Avoid the grey region for all times. Visit the blue region, then the green region, and then keep surveying the striped blue and green regions, in this order.”
Avoid the grey region for all times. Visit the blue region, then the green region, and then keep surveying the striped blue and green regions, in this order.

\[ \square \neg (\pi_2 \land \neg \pi_4 \land \neg \pi_3) \] \land
\[ \Diamond (\pi_4 \land \Diamond (\pi_1 \land \Diamond \Diamond ((\pi_3 \land \pi_4) \land \Diamond (\pi_1 \land \neg \pi_3)))) \]

“\(\pi_2 = \text{TRUE} \text{ and } \pi_4 = \text{FALSE} \text{ and } \pi_3 = \text{FALSE}\) should never happen. Then \(\pi_4 = \text{TRUE} \text{ and then } \pi_1 = \text{TRUE} \text{ should happen. After that, } (\pi_3 = \text{TRUE} \text{ and } \pi_4 = \text{TRUE}) \text{ and then } (\pi_1 = \text{TRUE} \text{ and } \pi_3 = \text{FALSE}) \text{ should occur infinitely often.”

“\(\pi_2, \pi_3, \pi_4\)
**Conservative Formal Synthesis for Dynamical Systems**

**Approach**

In each region construct feedback controllers driving all states in finite time to a subset of facets (including the empty set - controller making the region an invariant) - this is only possible for simple dynamics and partitions.

\[
\Box \neg (\pi_2 \land \neg \pi_4 \land \neg \pi_3) \land \\
\Diamond (\pi_4 \land \Diamond (\pi_1 \land \Diamond \\
(\Box \Diamond ((\pi_3 \land \pi_4) \land \Diamond (\pi_1 \land \neg \pi_3)))))
\]

“(\pi_2 = \text{TRUE and } \pi_4 = \text{FALSE and } \pi_3 = \text{FALSE}) should never happen. Then \pi_4 = \text{TRUE and then } \pi_1 = \text{TRUE should happen. After that, (\pi_3 = \text{TRUE and } \pi_4 = \text{TRUE}) and then (\pi_1 = \text{TRUE and } \pi_3 = \text{FALSE}) should occur infinitely often.”

“Avoid the grey region for all times. Visit the blue region, then the green region, and then keep surveying the striped blue and green regions, in this order.”
Avoid the grey region for all times. Visit the blue region, then the green region, and then keep surveying the striped blue and green regions, in this order.

\( \Box \neg (\pi_2 \land \neg \pi_4 \land \neg \pi_3) \) \land
\( \Diamond (\pi_4 \land \Diamond (\pi_1 \land \Diamond (\Box \Diamond ((\pi_3 \land \pi_4) \land \Diamond (\pi_1 \land \neg \pi_3))))) \)

"(\pi_2 = \text{TRUE and } \pi_4 = \text{FALSE and } \pi_3 = \text{FALSE}) should never happen. Then \( \pi_4 = \text{TRUE} \) and then \( \pi_1 = \text{TRUE} \) should happen. After that, (\( \pi_3 = \text{TRUE} \) and \( \pi_4 = \text{TRUE} \)) and then (\( \pi_1 = \text{TRUE} \) and \( \pi_3 = \text{FALSE} \)) should occur infinitely often."

"Avoid the grey region for all times. Visit the blue region, then the green region, and then keep surveying the striped blue and green regions, in this order."
Avoid the grey region for all times. Visit the blue region, then the green region, and then keep surveying the striped blue and green regions, in this order.

\[ \square \neg (\pi_2 \land \neg \pi_4 \land \neg \pi_3) \] \land \\
\[ \Diamond (\pi_4 \land \Diamond (\pi_1 \land \Diamond (\Diamond ((\pi_3 \land \pi_4) \land \Diamond (\pi_1 \land \neg \pi_3))))) \]

“(\pi_2 = \text{TRUE} \text{ and } \pi_4 = \text{FALSE} \text{ and } \pi_3 = \text{FALSE}) \text{ should never happen. Then } \pi_4 = \text{TRUE} \text{ and then } \pi_1 = \text{TRUE} \text{ should happen. After that, } (\pi_3 = \text{TRUE} \text{ and } \pi_4 = \text{TRUE}) \text{ and then } (\pi_1 = \text{TRUE} \text{ and } \pi_3 = \text{FALSE}) \text{ should occur infinitely often.”

“\text{Avoid the grey region for all times. Visit the blue region, then the green region, and then keep surveying the striped blue and green regions, in this order.”}
Avoid the grey region for all times. Visit the blue region, then the green region, and then keep surveying the striped blue and green regions, in this order.
“Always avoid black. Avoid red and green until blue or cyan are reached. If blue is reached then eventually visit green. If cyan is reached then eventually visit red.”
Conservative Formal Synthesis for Dynamical Systems

**Global Spec:** “Keep taking photos and upload current photo before taking another photo.”

**Local Spec:** “Unsafe regions should always be avoided. If fires are detected, then they should be extinguished. If survivors are detected, then they should be provided medical assistance. If both fires and survivors are detected locally, priority should be given to the survivors.”

A potential, Lyapunov-like function is used to make sure that local decisions do not affect global correctness (analogy to terminal constraints in MPC).
Language-guided synthesis of control strategies

$$x_{k+1} = Ax_k + Bu_k, x_k \in X, u_k \in U$$

$X, U$ polytopes

**Problem Formulation:** Find $X_0 \subseteq X$ and a state-feedback control strategy such that all trajectories of the closed loop system originating at $X_0$ satisfy an LTL formula $\phi$ over the linear predicates $p_i$. 
Language-guided synthesis of control strategies

Example

\[ x_{k+1} = Ax_k + Bu_k, \quad x_k \in \mathbb{X}, \quad u_k \in \mathbb{U} \]

“Visit region A or region B before reaching the target while always avoiding the obstacles”

\[ A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0.5 \\ 1 \end{bmatrix} \]

\[ \Phi_2 = (\neg p_6 \land p_9 \land p_{10} \land p_{11}) \lor ((\neg p_8 \land p_9 \land p_{10} \land p_{11}) \lor (\neg p_8 \land p_9 \land p_{10} \land p_{11}) \lor (p_5 \land \neg p_{12} \land \neg p_{13}) \lor (\neg p_5 \land \neg p_7 \land p_{14} \land p_{15})) \]

E. Aydin Gol, M. Lazar, C. Belta, HSCC 2012
Optimal temporal logic control

\[ x_{k+1} = Ax_k + Bu_k, \quad x_k \in \mathbb{X}, u_k \in \mathbb{U} \]

Initial state: \( x_0 \)
Reference trajectories:
\[
\begin{align*}
&x^r_0, x^r_1 \ldots \\
u^r_0, u^r_1, \ldots
\end{align*}
\]
Observation horizon : \( N \)

\[ C(x_k, u_k) = (x_{k+N} - x^r_{k+N})^\top L_N (x_{k+N} - x^r_{k+N}) \]
\[ + \sum_{i=0}^{N-1} \left\{ (x_{k+i} - x^r_{k+i})^\top L (x_{k+i} - x^r_{k+i}) \right. \]
\[ \left. + (u_{k+i} - u^r_{k+i})^\top R (u_{k+i} - u^r_{k+i}) \right\}, \]
Optimal temporal logic control

\[ x_{k+1} = Ax_k + Bu_k, \quad x_k \in \mathbb{X}, \ u_k \in \mathbb{U}, \quad \neg p_3 \]

Initial state: \( x_0 \)

Reference trajectories:

\[ x_0^r, x_1^r \ldots \]

\[ u_0^r, u_1^r, \ldots \]

Observation horizon: \( N \)

\[ C(x_k, u_k) = (x_{k+N} - x_{k+N}^r)\top L_N (x_{k+N} - x_{k+N}^r) \]

\[ + \sum_{i=0}^{N-1} \left\{ (x_{k+i} - x_{k+i}^r)\top L (x_{k+i} - x_{k+i}^r) \right. \]

\[ \left. + (u_{k+i} - u_{k+i}^r)\top R (u_{k+i} - u_{k+i}^r) \right\}, \]

Syntactically co-safe LTL formula over linear predicates \( p_i \)

Problem Formulation: Find an optimal state-feedback control strategy such that the trajectory originating at \( x_0 \) satisfies the formula.
Optimal temporal logic control

Example

\[ x_{k+1} = Ax_k + Bu_k, \quad x_k \in X, \ u_k \in U \]

\[ A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0.5 \\ 1 \end{bmatrix} \]

“Visit region A or region B before reaching the target while always avoiding the obstacles”

E. Aydin Gol, M. Lazar, C. Belta, HSCC 2013
Temporal Logic Control with Learning of Environmental Events

Find an optimal policy such that (1) the robot mission is accomplished, and (2) the expected time in between consecutive satisfactions of the optimizing task is minimized.

Mission:

“Always eventually go back to Base, perform Pickup repeatedly, make sure Pickup and Delivery are executed in between two consecutive visits to base”

\[
\phi = GF(\text{Base}) \land GF(\text{Pickup}) \land G(\text{Base} \rightarrow \text{Base} \cup (\neg \text{Base} \cup \text{Pickup})) \land \\
G(\text{Pickup} \rightarrow ((\neg \text{Base}) \cup \text{Delivery}))
\]
**Assumption:** the environmental events generate a specific subclass of omega-regular language, called stochastic strictly k-local language, which (1) can be learned from positive samples, and (2) is rich enough to represent interesting door behavior.

**Theorem:** When time goes to infinity, the door controller approximation almost surely generates a language that is equal to the language generated by the real door controller.

Y. Chen, J. Tumova, C. Belta, ICRA 2012, IJRR 2013  
J. Heinz, “String extension learning, 2010"
Acknowledgements

Boston University

Ebru Aydin Gol
Yushan Chen
Dennis Ding (now at UTRC)
Jana Tumova (now at MIT)
Alphan Ulusoy

University of Delaware

Bert Tanner
Jeff Heinz

CPS: Medium: Collaborative Research: Efficient Control Synthesis and Learning in Distributed Cyber-Physical Systems