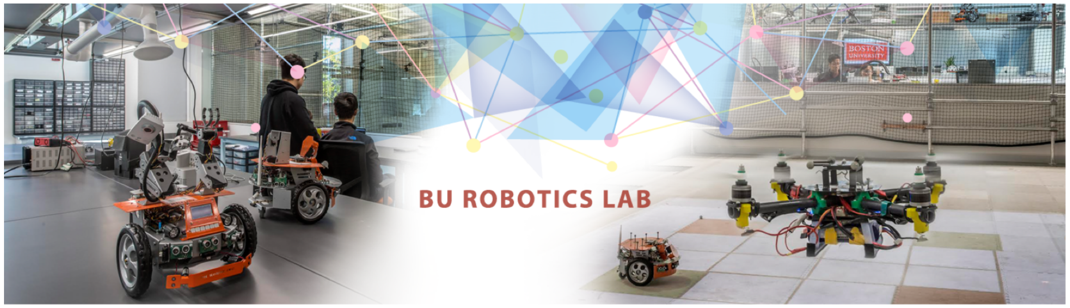


BOSTON UNIVERSITY

Formal Synthesis of Control Strategies for Dynamical Systems

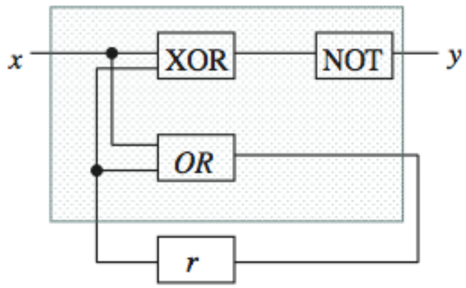
Calin Belta

Tegan Family Distinguished Professor
Mechanical Engineering, Systems Engineering,
Electrical and Computer Engineering

Boston University

A textbook problem in formal methods

Process

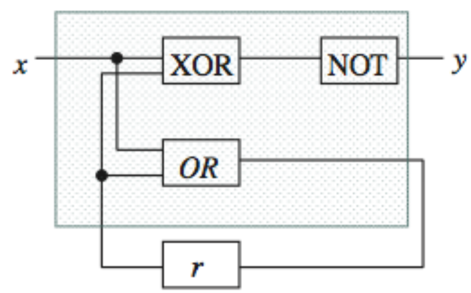


C. Bayer and J-P Katoen, Principles of Model Checking, MIT Press, 2008

A textbook problem in formal methods

Specification: “If x is set infinitely often, then y is set infinitely often.”

Process



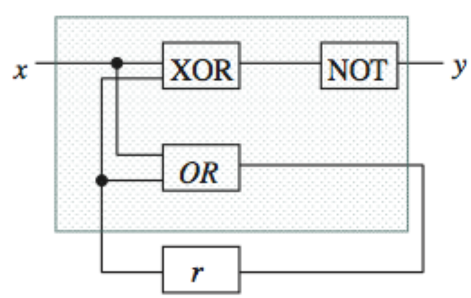
C. Bayer and J-P Katoen, Principles of Model Checking, MIT Press, 2008

A textbook problem in formal methods

Specification: "If x is set infinitely often, then y is set infinitely often."

Check if all the possible behaviors of the circuit satisfy the specification

Process



C. Bayer and J-P Katoen, Principles of Model Checking, MIT Press, 2008

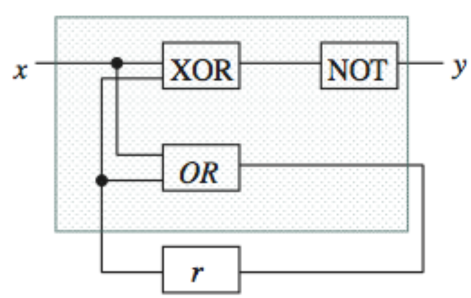
A textbook problem in formal methods

Specification: "If x is set infinitely often, then y is set infinitely often."

Formalization

Temporal Logic Formula $\Box\Diamond x \rightarrow \Box\Diamond y$

Process



C. Bayer and J-P Katoen, Principles of Model Checking, MIT Press, 2008

A textbook problem in formal methods

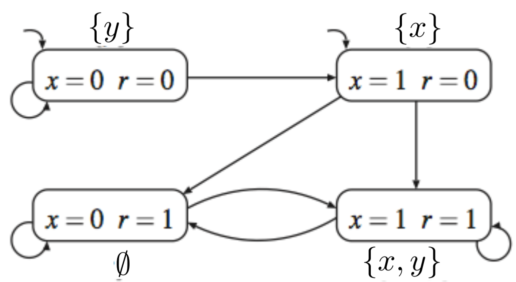
Specification: "If x is set infinitely often, then y is set infinitely often."

Formalization

Temporal Logic Formula

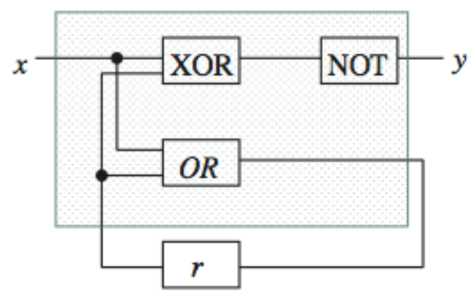
$$\Box\Diamond x \rightarrow \Box\Diamond y$$

Model



Mathematical modeling

Process



C. Bayer and J-P Katoen, Principles of Model Checking, MIT Press, 2008

A textbook problem in formal methods

Specification: “If x is set infinitely often, then y is set infinitely often.”

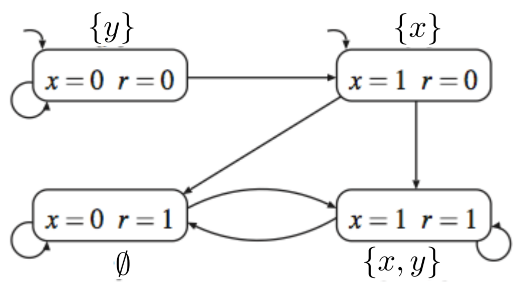
Formalization

Temporal Logic Formula

$$\Box\Diamond x \rightarrow \Box\Diamond y$$

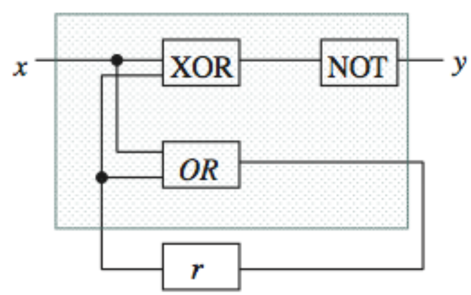
Model checking (verification)

Model



Mathematical modeling

Process



C. Bayer and J-P Katoen, Principles of Model Checking, MIT Press, 2008

A textbook problem in dynamics

Process

S. Sastry – Nonlinear Systems: analysis, stability, and control, Springer, 1999

A textbook problem in dynamics

Specification: “drive from A to B.”

Process

A

B

S. Sastry – Nonlinear Systems: analysis, stability, and control, Springer, 1999

A textbook problem in dynamics

Specification: “drive from A to B.”

Generate a robot control strategy

Process

A

B

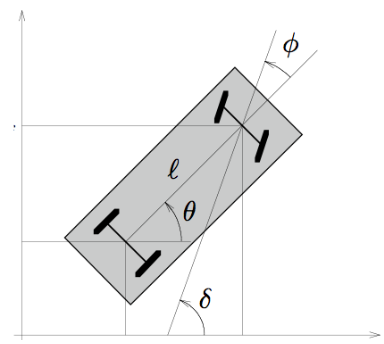
S. Sastry – Nonlinear Systems: analysis, stability, and control, Springer, 1999

A textbook problem in dynamics

Specification: “drive from A to B.”

Model

$$\begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{\theta} \\ \dot{\phi} \end{bmatrix} = \begin{bmatrix} \cos\theta \\ \sin\theta \\ \tan\phi/\ell \\ 0 \end{bmatrix} v_1 + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} v_2$$



Mathematical modeling

Process

B

A

S. Sastry – Nonlinear Systems: analysis, stability, and control, Springer, 1999

A textbook problem in dynamics

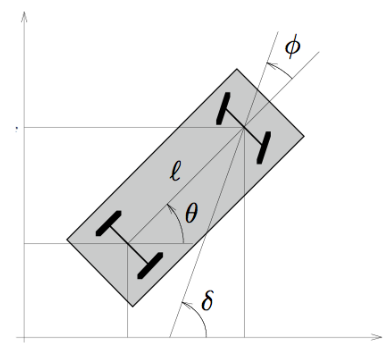
Specification: “drive from A to B.”

Formalization

Stabilization Problem: “make B an asymptotically stable equilibrium”

Model

$$\begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{\theta} \\ \dot{\phi} \end{bmatrix} = \begin{bmatrix} \cos\theta \\ \sin\theta \\ \tan\phi/\ell \\ 0 \end{bmatrix} v_1 + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} v_2$$



Mathematical modeling

Process

A

B

S. Sastry – Nonlinear Systems: analysis, stability, and control, Springer, 1999

A textbook problem in dynamics

Specification: "drive from A to B."

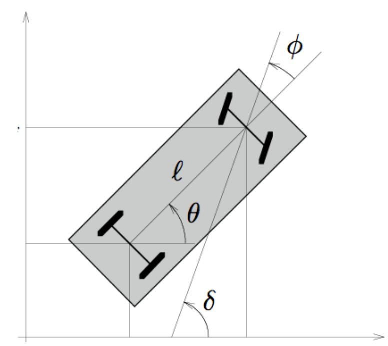
Formalization

Stabilization Problem: "make B an asymptotically stable equilibrium"

Control

Model

$$\begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{\theta} \\ \dot{\phi} \end{bmatrix} = \begin{bmatrix} \cos\theta \\ \sin\theta \\ \tan\phi/\ell \\ 0 \end{bmatrix} v_1 + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} v_2$$



Mathematical modeling

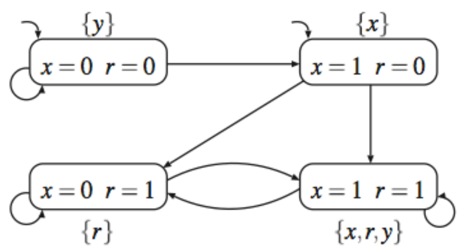
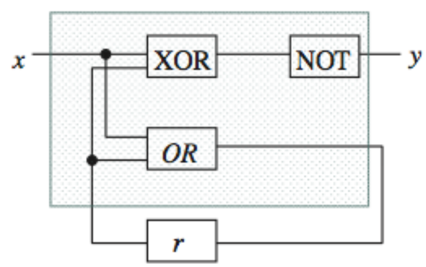
Process

A

B

S. Sastry – Nonlinear Systems: analysis, stability, and control, Springer, 1999

Formal methods vs. dynamics

Specification	"If x is set infinitely often, then y is set infinitely often."	"Drive from A to B."
Model		$\begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{\theta} \\ \dot{\phi} \end{bmatrix} = \begin{bmatrix} \cos\theta \\ \sin\theta \\ \tan\phi/\ell \\ 0 \end{bmatrix} v_1 + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} v_2$
Process		

Formal methods vs. dynamics

Specification

"If x is set infinitely often, then y is set infinitely often."

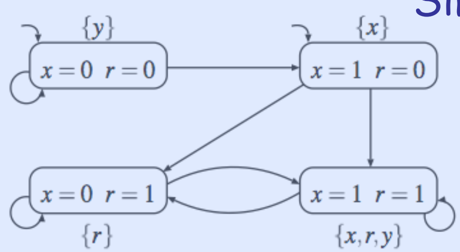
Complex

"Drive from A to B."

Simple

Model

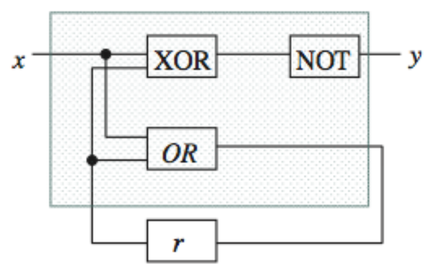
Simple



Complex

$$\begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{\theta} \\ \dot{\phi} \end{bmatrix} = \begin{bmatrix} \cos\theta \\ \sin\theta \\ \tan\phi/\ell \\ 0 \end{bmatrix} v_1 + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} v_2$$

Process



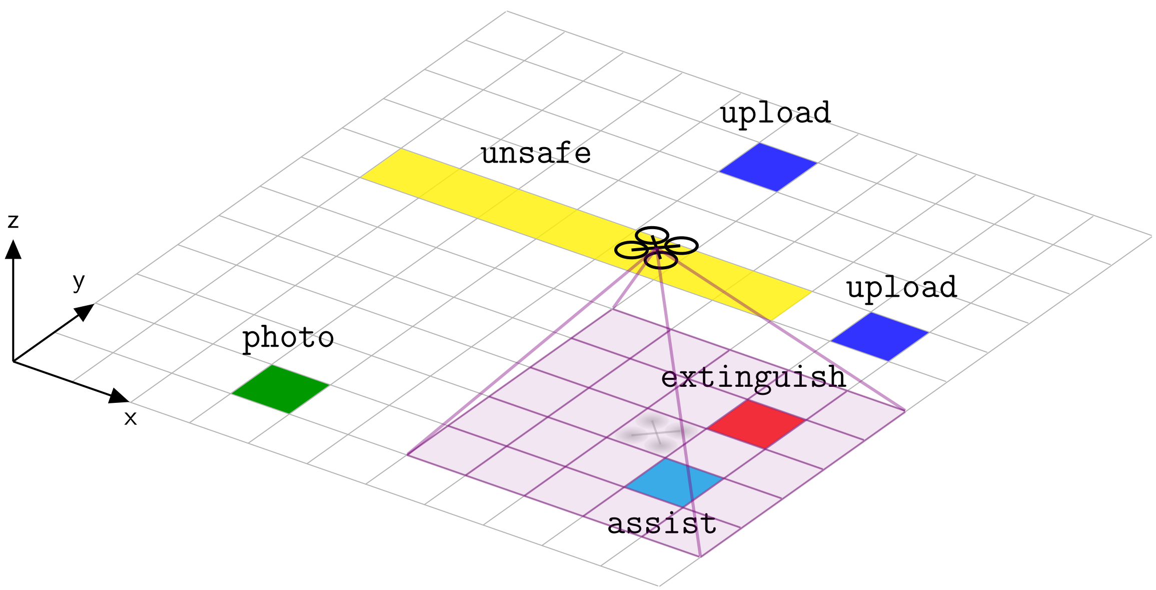
Need for formal methods in dynamical systems

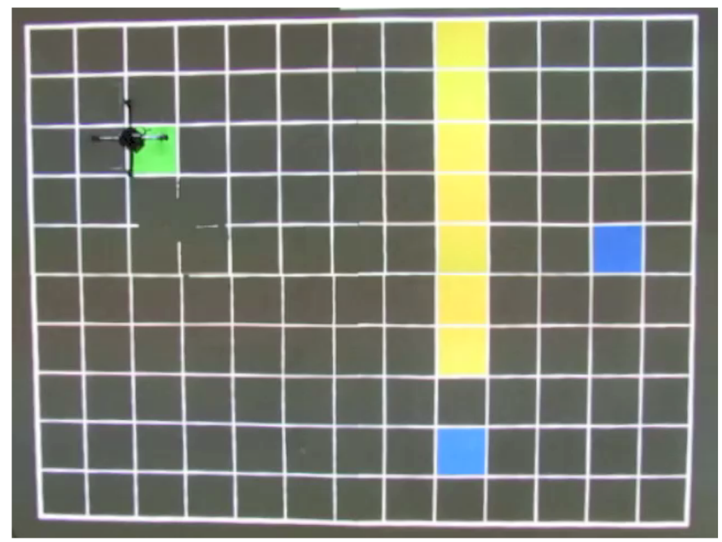
Spec: **Off-line:** "Keep taking photos and upload current photo before taking another photo. **On-line:** Unsafe regions should always be avoided. If fires are detected, then they should be extinguished. If survivors are detected, then they should be provided medical assistance. If both fires and survivors are detected locally, priority should be given to the survivors."

- Ideal controllers and sensors
- Known map
- Perfect localization

?

Vehicle Control Strategy





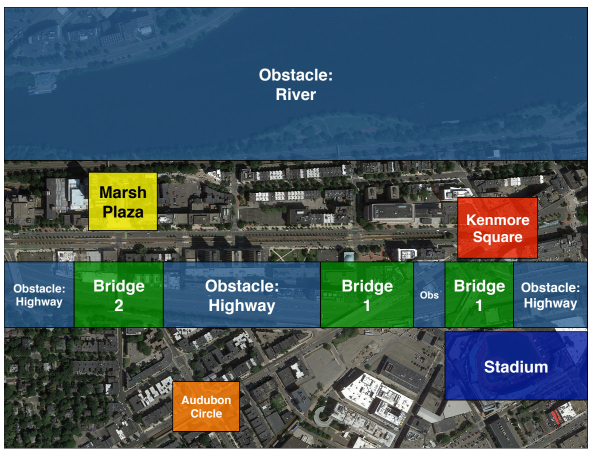
Solution later in this talk

Ulusoy, Belta, RSS 2013, IJRR 2014

Need for formal methods in dynamical systems

Spec: Maximize the probability of satisfying: "Always avoid all obstacles and Visit Marsh Plaza, Kenmore Square, Fenway Park, and Audubon Circle infinitely often and Bridge 2 should only be used for Northbound travel and Bridges 1 should only be used for Southbound travel. Uncertainty should always be below 0.9 m^2 and when crossing bridges it should be below 0.6 m^2."

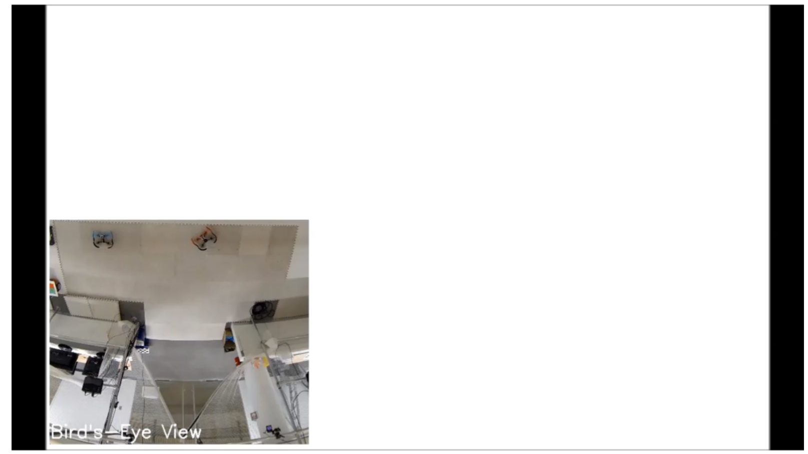
? Vehicle Control / Communication Strategies



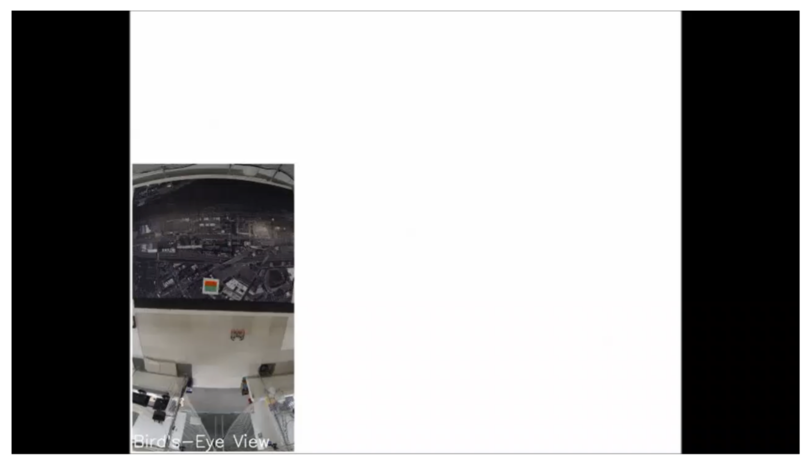
- Noisy controllers and sensors
- Unknown map
- Probabilistic localization

Example later in the talk

E. Cristofalo, et.al., *ISER* 2016.
C. I. Vasile et.al., CDC 2016



Map unknown environment



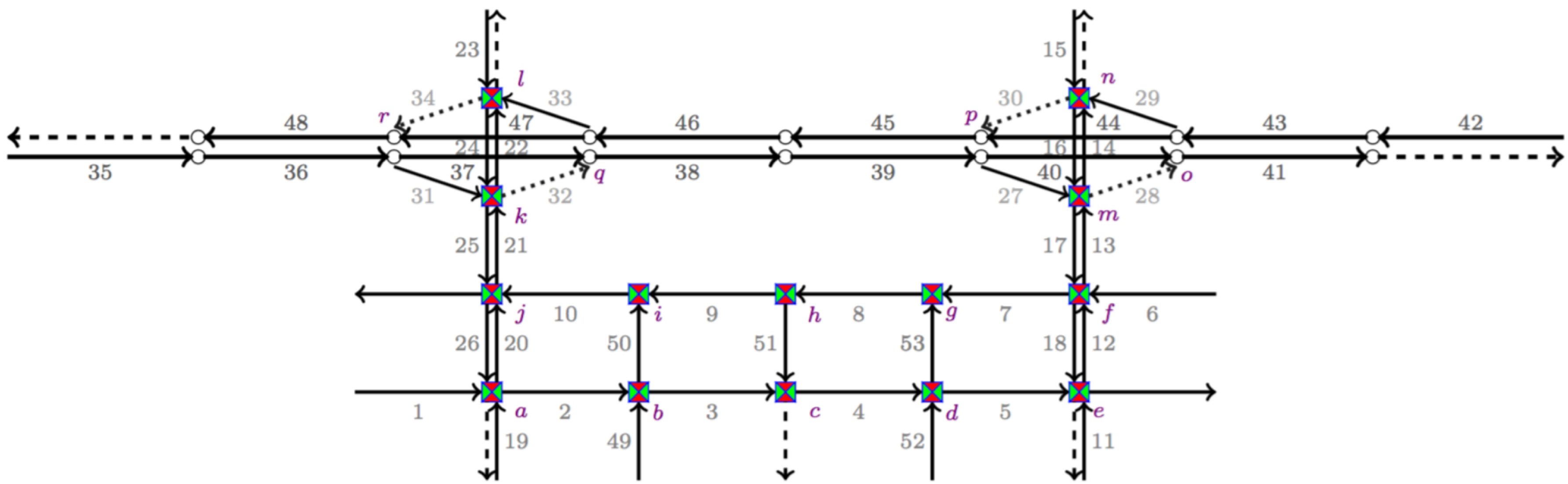
Localization and control

Need for formal methods in dynamical systems

Spec:
- always the network is not congested
- each queue at a junction will be actuated at least once every two minutes
- whenever the number of vehicles on a link exceeds 40, within 3 min it should decreases below 20

?

Traffic light and ramp meter control strategies



Example later in the talk

Coogan, et.al.,, ACC 2015, IEEE TCNS 2016
Sadradini, Belta, ACC 2016, CDC 2016
Coogan, Arcak, Belta, ACC 2016, CSM 2017

Outline

TL verification and control for finite systems

Conservative TL control for **small & simple** dynamical systems

Conservative TL control for **large & complex** dynamical systems

Less conservative *optimal* TL control for **small & simple** dynamical systems

Less conservative TL control for **large & (possibly) complex** dynamical systems

Less conservative *optimal* TL control for **large & simple** dynamical systems

Limitation

TL = Temporal Logic

Outline

TL verification and control for finite systems

Conservative TL control for **small & simple** dynamical systems

Conservative TL control for **large & complex** dynamical systems

Less conservative *optimal* TL control for **small & simple** dynamical systems

Less conservative TL control for **large & (possibly) complex** dynamical systems

Less conservative *optimal* TL control for **large & simple** dynamical systems

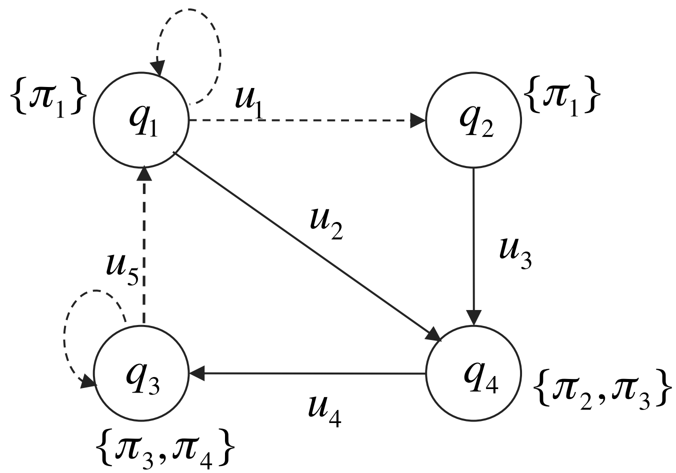
Limitation

TL = Temporal Logic

TL verification and control for finite systems

Finite system

(Fully-observable) nondeterministic (non-probabilistic) labeled transition systems with finitely many states, actions (controls), and observations (properties)



TL verification and control for finite systems

Linear Temporal Logic (LTL)

Syntax

$$\Diamond \pi_2 \qquad \Diamond \Box (\pi_3 \wedge \pi_4) \qquad (\pi_1 \vee \pi_2) U \pi_4$$

eventually

always

until

TL verification and control for finite systems

Linear Temporal Logic (LTL)

Syntax

$$\Diamond \pi_2 \qquad \Diamond \Box (\pi_3 \wedge \pi_4) \qquad (\pi_1 \vee \pi_2) U \pi_4$$

eventually always until

Semantics

Word: $\{\pi_1\}\{\pi_2, \pi_3\}\{\pi_3, \pi_4\}\{\pi_3, \pi_4\} \cdots$

TL verification and control for finite systems

Linear Temporal Logic (LTL)

Syntax

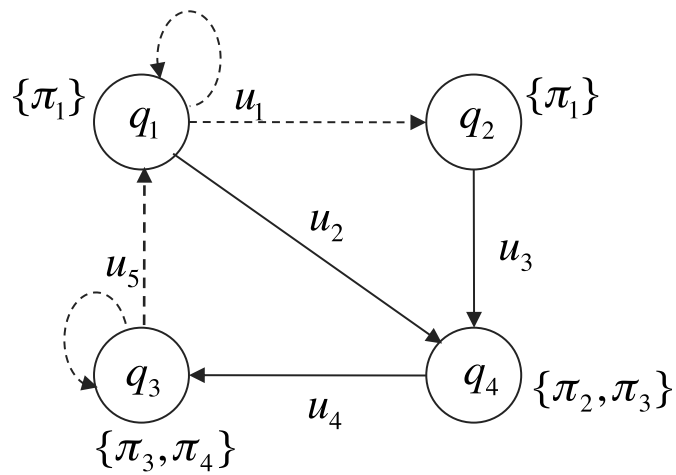
$$\Diamond \pi_2 \qquad \Diamond \Box (\pi_3 \wedge \pi_4) \qquad (\pi_1 \vee \pi_2) U \pi_4$$

eventually   always   until

Semantics

Run (trajectory): $q_1, q_4, q_3, q_3, \ldots$

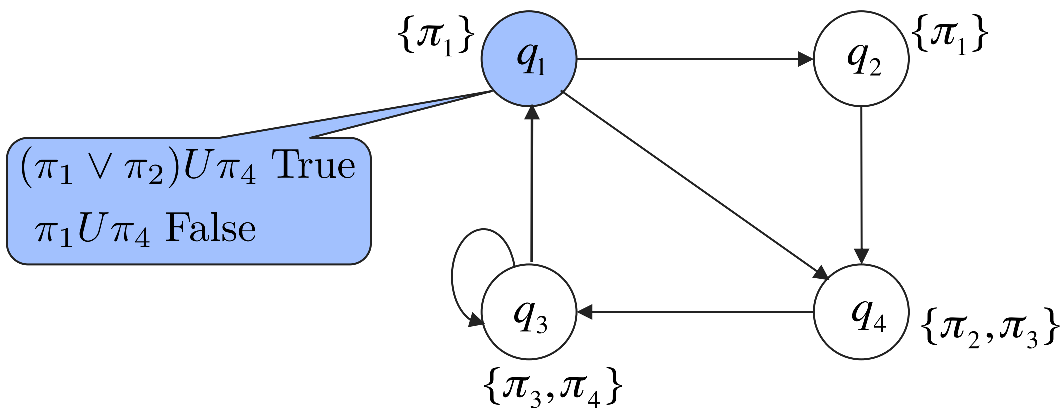
Word: $\{\pi_1\}\{\pi_2, \pi_3\}\{\pi_3, \pi_4\}\{\pi_3, \pi_4\} \cdots$



TL verification and control for finite systems

LTL verification (model checking)

Given a transition system and an LTL formula over its set of propositions, check if the language (i.e., all possible words) of the transition system starting from all initial states satisfies the formula.

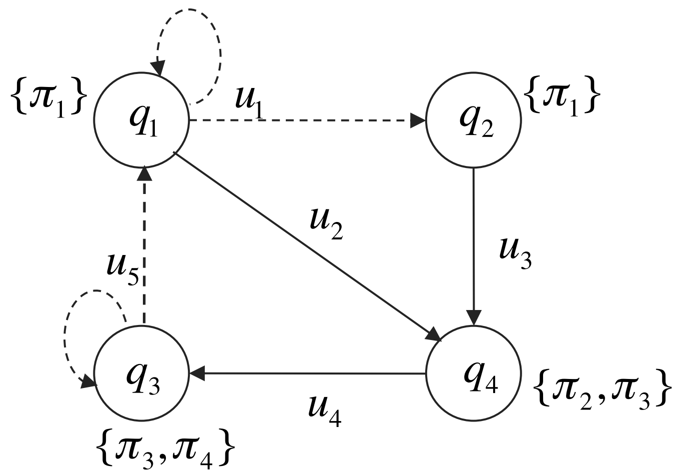


SPIN, NuSMV, PRISM, …

TL verification and control for finite systems

LTL control (synthesis)

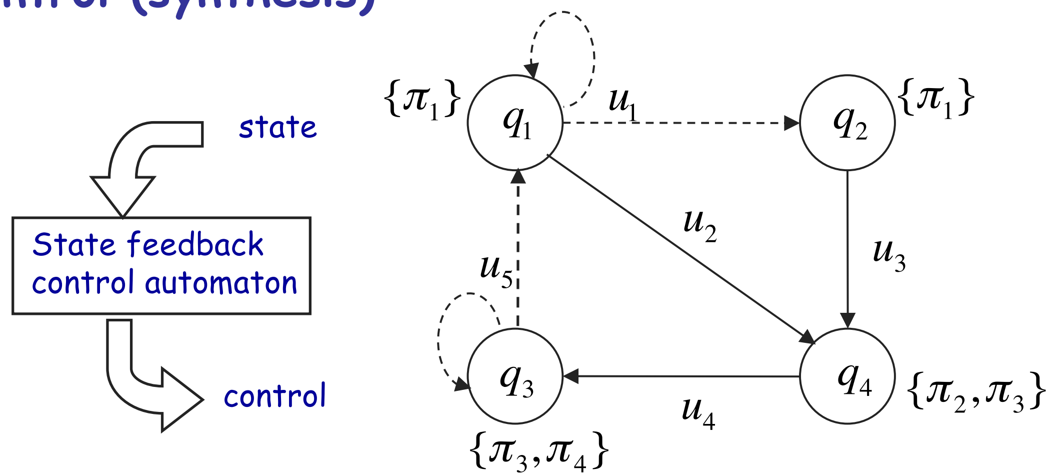
Given a transition system and an LTL formula over its set of propositions, find a set of initial states and a control strategy for all initial states such that the produced language of the transition system satisfies the formula.



Did not receive much attention until recently!

TL verification and control for finite systems

LTL control (synthesis)



Rabin game!

Particular cases:

- LTL without "eventually always": Buchi game
- LTL without "always" (syntactically co-safe LTL): the automaton is an FSA

Extensions

Optimal Temporal Logic Control for Finite Deterministic Systems
Optimal Temporal Logic Control for Finite MDPs
Temporal Logic Control for POMDPs
Temporal Logic Control and Learning

Outline

TL verification and control for finite systems

Conservative TL control for **small & simple** dynamical systems

Conservative TL control for **large & complex** dynamical systems

Less conservative *optimal* TL control for **small & simple** dynamical systems

Less conservative TL control for **large & (possibly) complex** dynamical systems

Less conservative *optimal* TL control for **large & simple** dynamical systems

Limitation

TL = Temporal Logic

Outline

TL verification and control for finite systems

Conservative TL control for **small & simple** dynamical systems

Conservative TL control for **large & complex** dynamical systems

Less conservative *optimal* TL control for **small & simple** dynamical systems

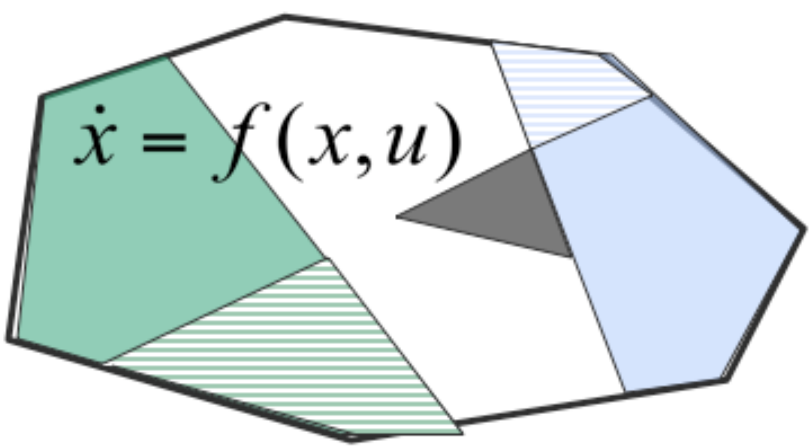
Less conservative TL control for **large & (possibly) complex** dynamical systems

Less conservative *optimal* TL control for **large & simple** dynamical systems

Limitation

TL = Temporal Logic

Conservative TL control for **small & simple** dynamical systems

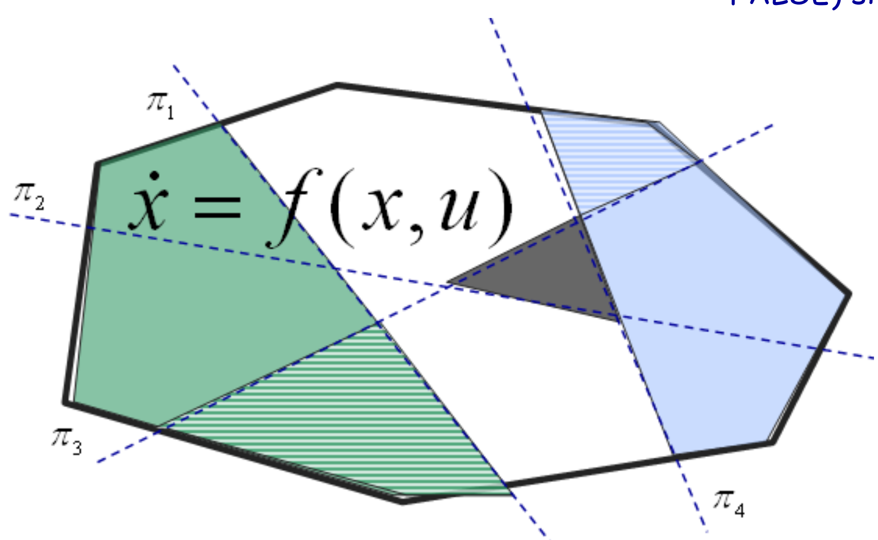


$\longleftrightarrow$

"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 TL control for **small & simple** dynamical systems

"(pi2 = TRUE and pi4 = FALSE and pi3 = FALSE) should never happen. Then pi4 = TRUE and then pi1 = TRUE should happen. After that, (pi3 = TRUE and pi4 = TRUE) and then (pi1 = TRUE and pi3 = FALSE) should occur infinitely often."

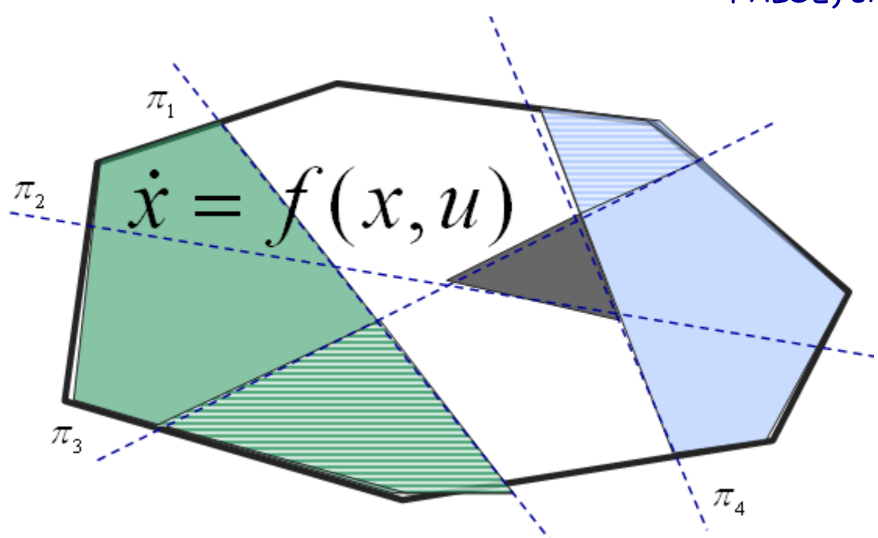


"Avoid the grey region for all times. Visit the blue region, then the green region, and then keep surveying the striped blue and green regions, in this order."

Conservative TL control for **small & simple** dynamical systems

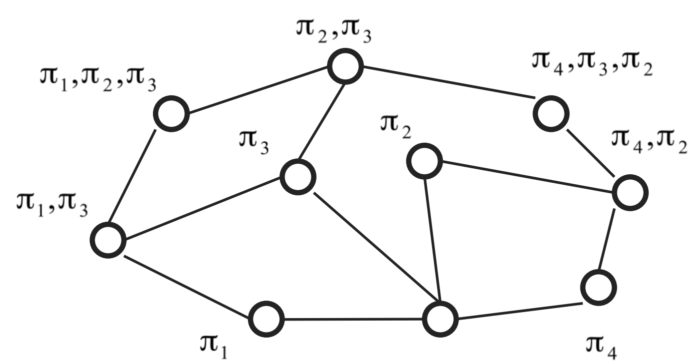
$$\Box\neg(\pi_2 \wedge \neg\pi_4 \wedge \neg\pi_3)) \wedge$$
$$\Diamond(\pi_4 \wedge \Diamond(\pi_1 \wedge \Diamond$$
$$(\Box\Diamond((\pi_3 \wedge \pi_4) \wedge \Diamond(\pi_1 \wedge \neg\pi_3)))))$$

"(pi2 = TRUE and pi4 = FALSE and pi3 = FALSE) should never happen. Then pi4 = TRUE and then pi1 = TRUE should happen. After that, (pi3 = TRUE and pi4 = TRUE) and then (pi1 = TRUE and pi3 = FALSE) should occur infinitely often."



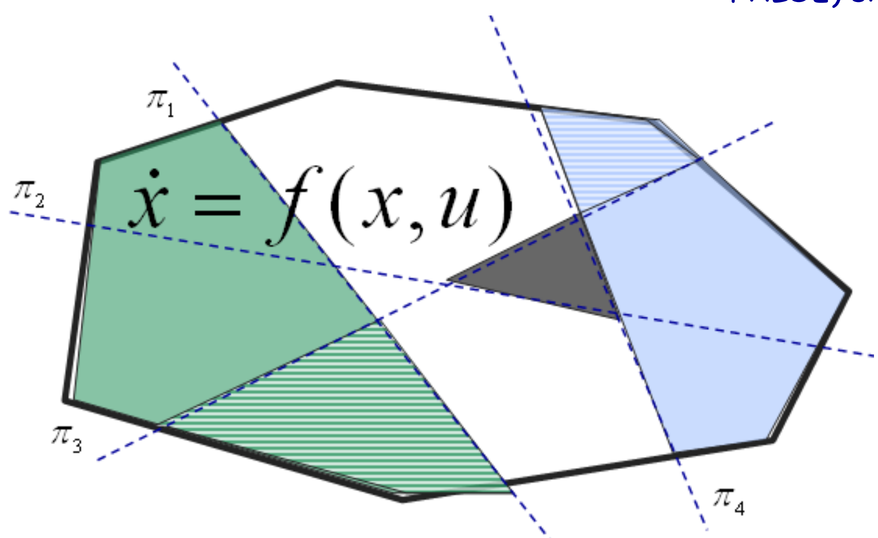
"Avoid the grey region for all times. Visit the blue region, then the green region, and then keep surveying the striped blue and green regions, in this order."

Conservative TL control for **small & simple** dynamical systems



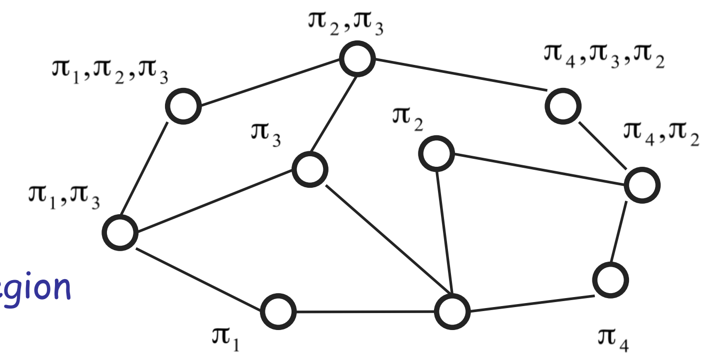
$$\Box\neg(\pi_2 \wedge \neg\pi_4 \wedge \neg\pi_3)) \wedge$$
$$\Diamond(\pi_4 \wedge \Diamond(\pi_1 \wedge \Diamond$$
$$(\Box\Diamond((\pi_3 \wedge \pi_4) \wedge \Diamond(\pi_1 \wedge \neg\pi_3)))))$$

"(pi2 = TRUE and pi4 = FALSE and pi3 = FALSE) should never happen. Then pi4 = TRUE and then pi1 = TRUE should happen. After that, (pi3 = TRUE and pi4 = TRUE) and then (pi1 = TRUE and pi3 = 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."

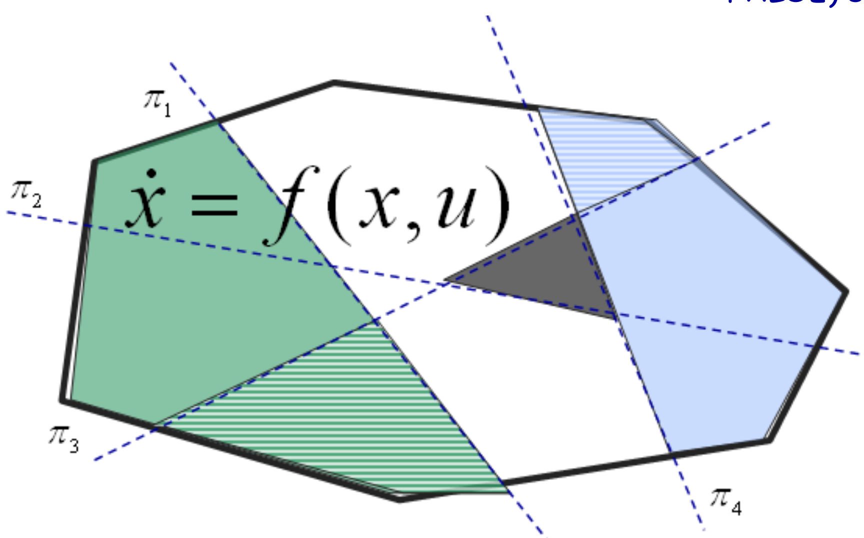
Conservative TL control for **small & simple** dynamical systems



$$\Box\neg(\pi_2 \wedge \neg\pi_4 \wedge \neg\pi_3)) \wedge \Diamond(\pi_4 \wedge \Diamond(\pi_1 \wedge \Diamond (\Box\Diamond((\pi_3 \wedge \pi_4) \wedge \Diamond(\pi_1 \wedge \neg\pi_3)))))$$

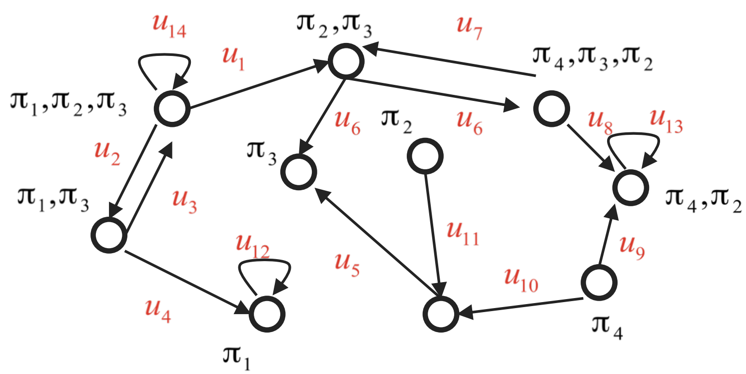
"(pi2 = TRUE and pi4 = FALSE and pi3 = FALSE) should never happen. Then pi4 = TRUE and then pi1 = TRUE should happen. After that, (pi3 = TRUE and pi4 = TRUE) and then (pi1 = TRUE and pi3 = FALSE) should occur infinitely often."

Assume that in each region we can check for the existence of / construct feedback controllers driving all states in finite time to a subset of facets (including the empty set – controller making the region an invariant)



"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."

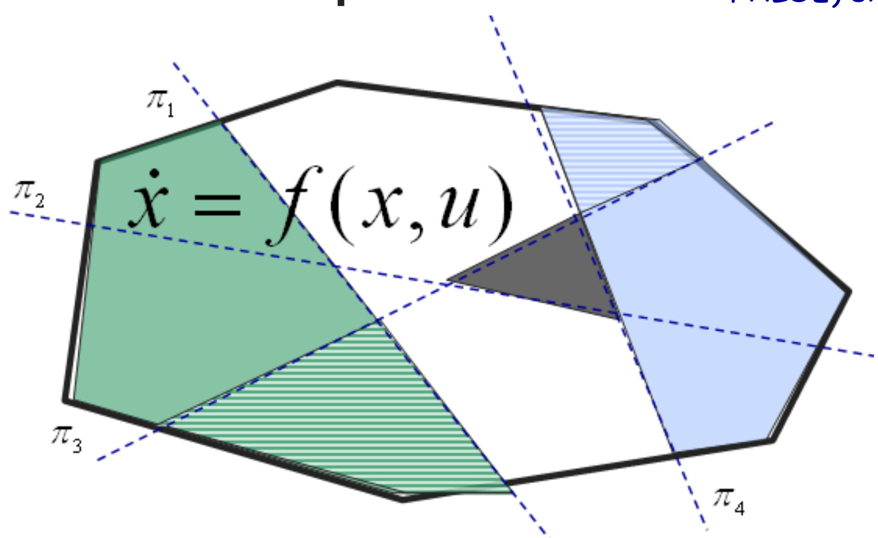
Conservative TL control for **small & simple** dynamical systems



$$\Box\neg(\pi_2 \wedge \neg\pi_4 \wedge \neg\pi_3)) \wedge$$
$$\Diamond(\pi_4 \wedge \Diamond(\pi_1 \wedge \Diamond$$
$$(\Box\Diamond((\pi_3 \wedge \pi_4) \wedge \Diamond(\pi_1 \wedge \neg\pi_3)))))$$

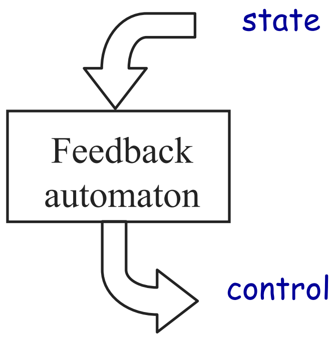
"(pi2 = TRUE and pi4 = FALSE and pi3 = FALSE) should never happen. Then pi4 = TRUE and then pi1 = TRUE should happen. After that, (pi3 = TRUE and pi4 = TRUE) and then (pi1 = TRUE and pi3 = FALSE) should occur infinitely often."

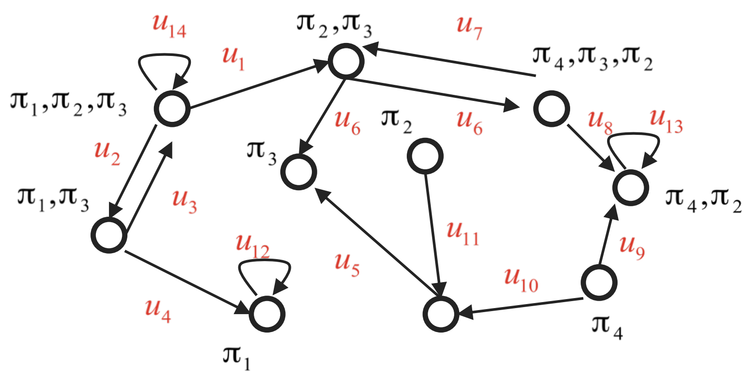
Abstraction (bisimulation)



"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 TL control for **small & simple** dynamical systems

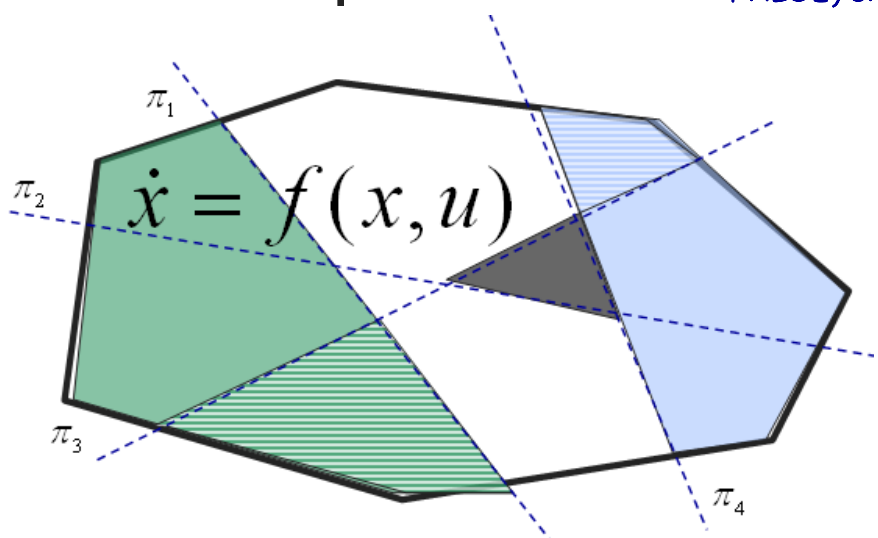




$$\Box\neg(\pi_2 \wedge \neg\pi_4 \wedge \neg\pi_3)) \wedge$$
$$\Diamond(\pi_4 \wedge \Diamond(\pi_1 \wedge \Diamond$$
$$(\Box\Diamond((\pi_3 \wedge \pi_4) \wedge \Diamond(\pi_1 \wedge \neg\pi_3)))))$$

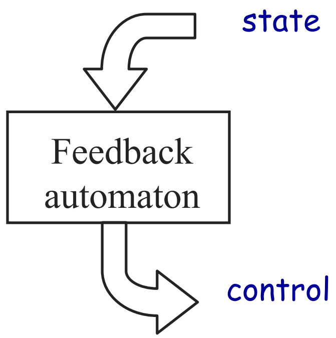
"(pi2 = TRUE and pi4 = FALSE and pi3 = FALSE) should never happen. Then pi4 = TRUE and then pi1 = TRUE should happen. After that, (pi3 = TRUE and pi4 = TRUE) and then (pi1 = TRUE and pi3 = FALSE) should occur infinitely often."

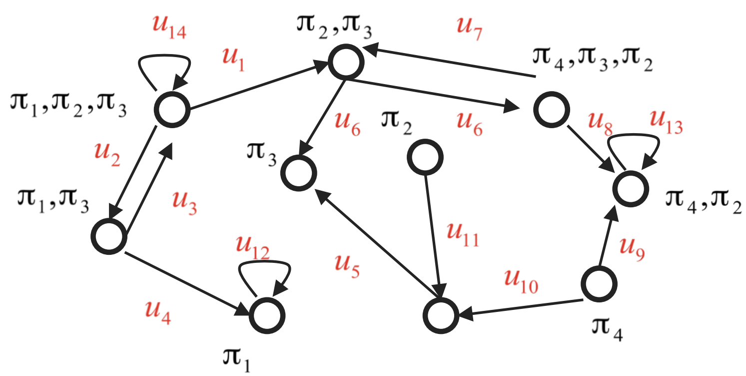
Abstraction (bisimulation)



"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 TL control for **small & simple** dynamical systems



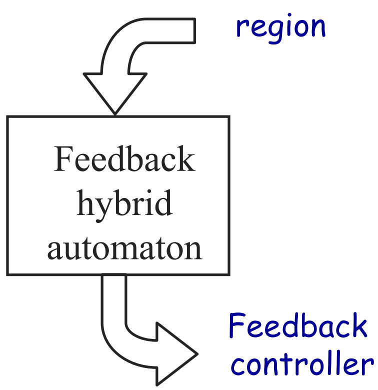


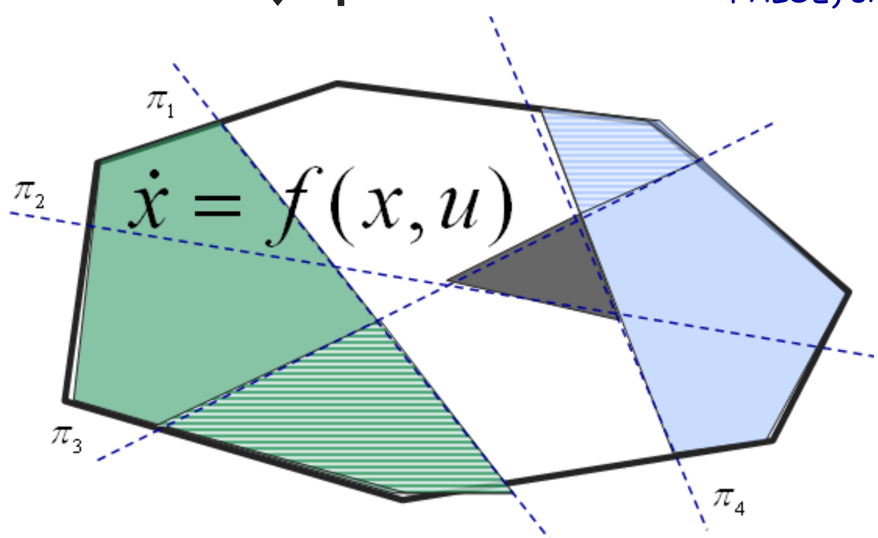
$$\Box\neg(\pi_2 \wedge \neg\pi_4 \wedge \neg\pi_3)) \wedge \Diamond(\pi_4 \wedge \Diamond(\pi_1 \wedge \Diamond(\Box\Diamond((\pi_3 \wedge \pi_4) \wedge \Diamond(\pi_1 \wedge \neg\pi_3)))))$$

"(pi2 = TRUE and pi4 = FALSE and pi3 = FALSE) should never happen. Then pi4 = TRUE and then pi1 = TRUE should happen. After that, (pi3 = TRUE and pi4 = TRUE) and then (pi1 = TRUE and pi3 = FALSE) should occur infinitely often."

Refinement

Abstraction (bisimulation)





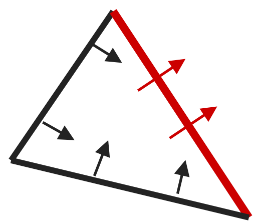
"Avoid the grey region for all times. Visit the blue region, then the green region, and then keep surveying the striped blue and green regions, in this order."

Conservative TL control for **small & simple** dynamical systems

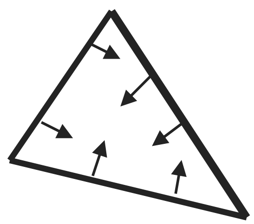
Dynamics and partitions allowing for easy construction of bisimilar abstractions

Library of controllers for polytopes

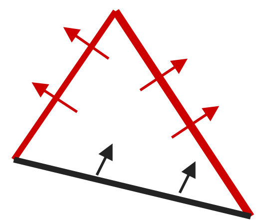
$\dot{x} = Ax + b + Bu \qquad x \in \Re^n \qquad u \in U \subset \Re^m \qquad U$ polyhedral



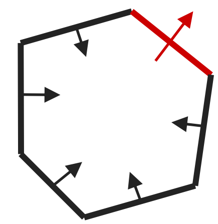
Control-to-facet



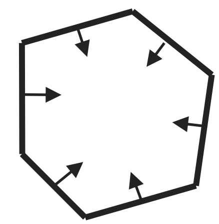
Stay-inside



Control-to-set-of-facets

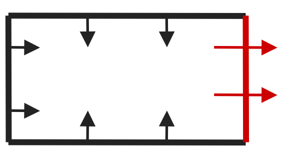


Control-to-face

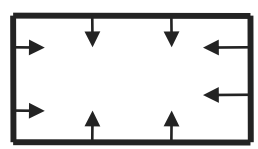


Stay-inside

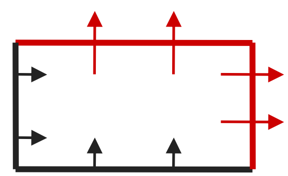
$$\dot{x} = g(x) + Bu \qquad x \in \Re^n \qquad g(x) = \sum_{i_1,\dots,i_N \in \{0,1\}} c_{i_1,\dots,i_N} x_1^{i_1} \dots x_n^{i_n} \qquad u \in U \subset \Re^m$$



Control-to-facet



Stay-inside



Control-to-set-of-facets

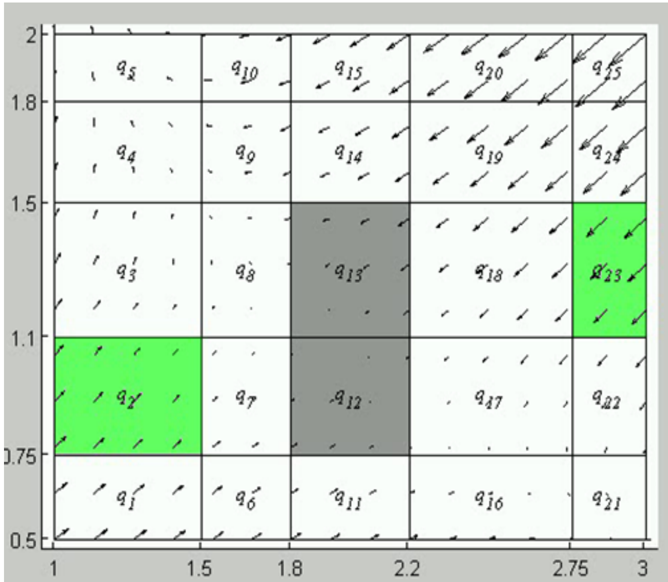
- checking for existence of controllers amounts to checking the non-emptiness of polyhedral sets in U
- if controllers exist, they can be constructed everywhere in the polytopes by using simple formulas

L.C.G.J.M. Habets and J. van Schuppen, Automatica 2005

M. Kloetzer, et.al, CDC 2006

C. Belta and L.C.G.J.M. Habets, IEEE TAC, 2006

Conservative TL control for small & simple dynamical systems

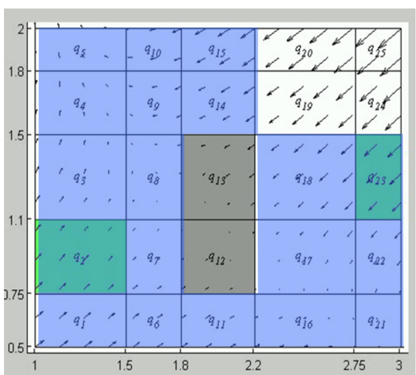


Multi-affine dynamics

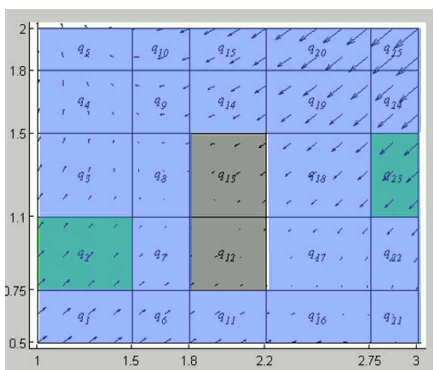
$$\dot{x}_1 = 2 - x_1 x_2 + u_1$$
$$\dot{x}_2 = 1 + x_2 - x_1 x_2 + u_2,$$
$$x \in [1,3] \times [0.5, 2],$$
$$u \in [-1.5, 1.5] \times [-1.5, 1.5]$$

"visit the green regions, in any order, while avoiding the grey regions"

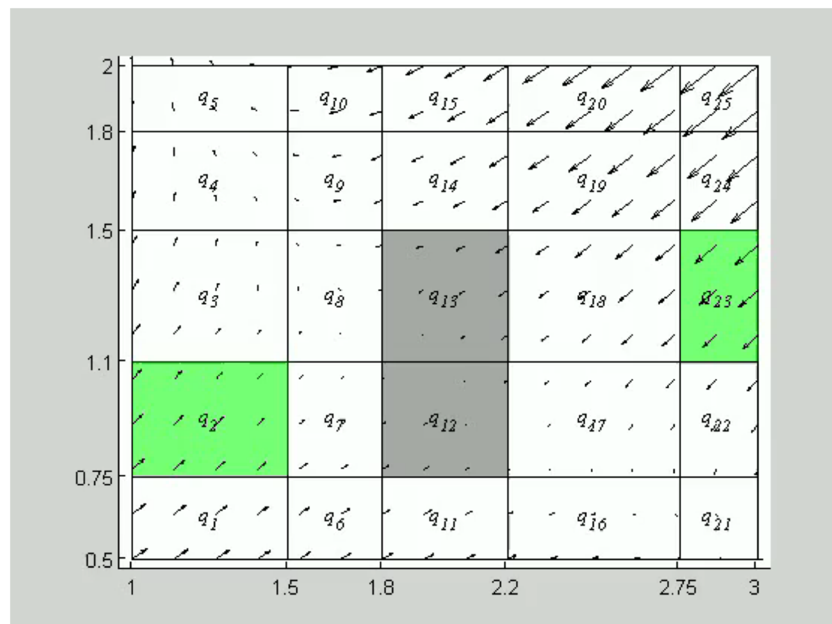
$$\Diamond q_2 \wedge \Diamond q_{25} \wedge \Box \neg (q_{12} \vee q_{13})$$



Control to one facet
Deterministic quotient



Control to sets of facets
Non-deterministic quotient



Initial states from which control strategies exist

Outline

TL verification and control for finite systems

Conservative TL control for **small & simple** dynamical systems

---

Conservative TL control for **large & complex** dynamical systems

Less conservative *optimal* TL control for **small & simple** dynamical systems

Less conservative TL control for **large & (possibly) complex** dynamical systems

Less conservative *optimal* TL control for **large & simple** dynamical systems

Limitation

TL = Temporal Logic

Outline

TL verification and control for finite systems

Conservative TL control for **small & simple** dynamical systems

Conservative TL control for **large & complex** dynamical systems

Less conservative *optimal* TL control for **small & simple** dynamical systems

Less conservative TL control for **large & (possibly) complex** dynamical systems

Less conservative *optimal* TL control for **large & simple** dynamical systems

Limitation

TL = Temporal Logic

Conservative TL control for **large & complex** dynamics

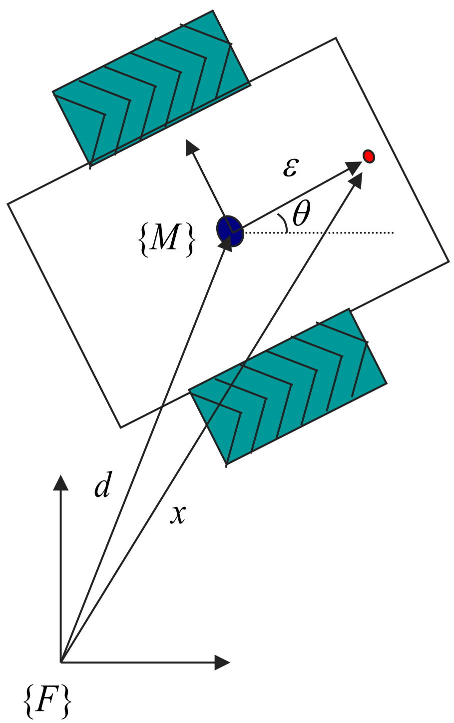
Mapping complex dynamics to simple dynamics: I/O linearization

Fully actuated point

$$\dot{x} = u \qquad u \in U$$

U can be derived from W

$$\dot{x} = REw \quad \Updownarrow \quad w = E^{-1}R^{T}u \qquad E = \begin{bmatrix} 1 & 0 \\ 0 & \varepsilon \end{bmatrix}$$

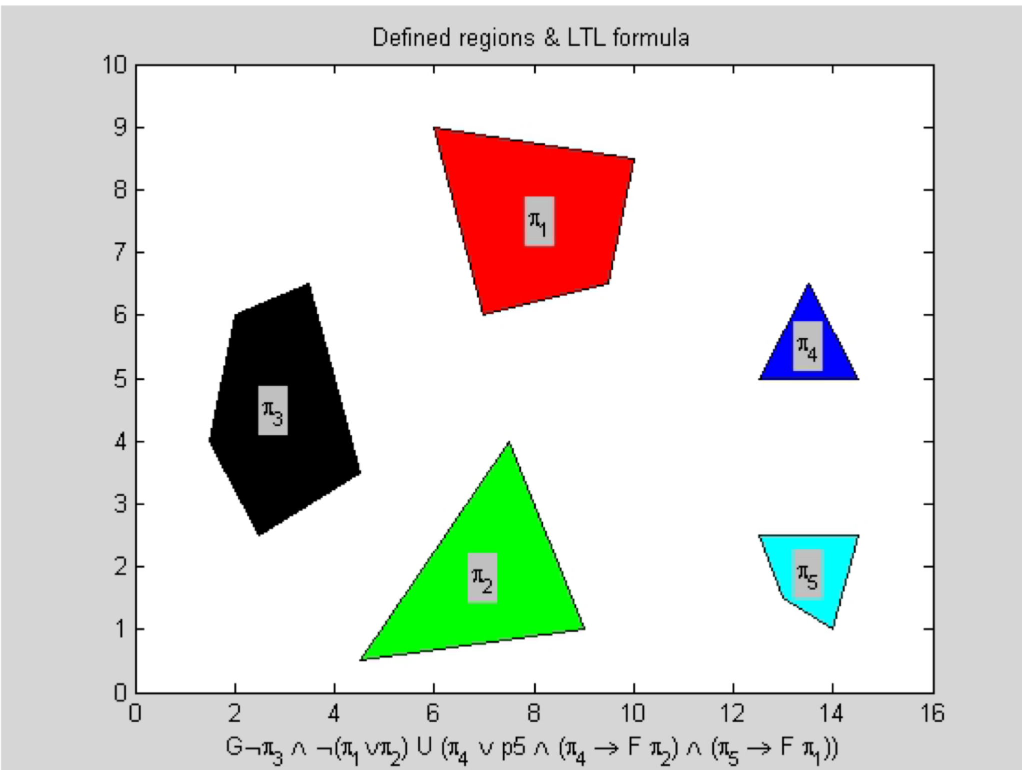


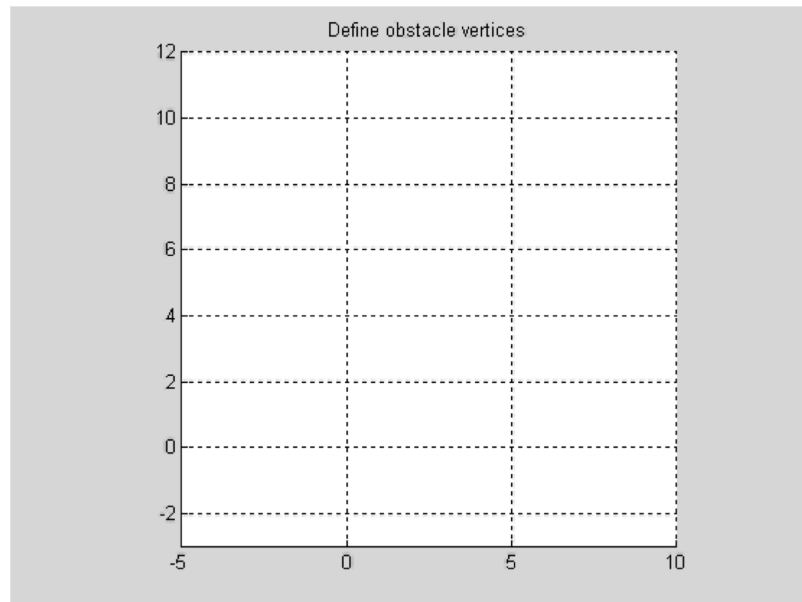
$$\begin{bmatrix} \dot{d}_x \\ \dot{d}_x \\ \dot{\theta} \end{bmatrix} = \begin{bmatrix} \cos\theta \\ \sin\theta \\ 0 \end{bmatrix} w_1 + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} w_2 \qquad w = \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} \in W$$

J. Desai, J.P. Ostrowski, and V. Kumar. ICRA, 1998.

Conservative TL control for **large & complex** dynamics

"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."





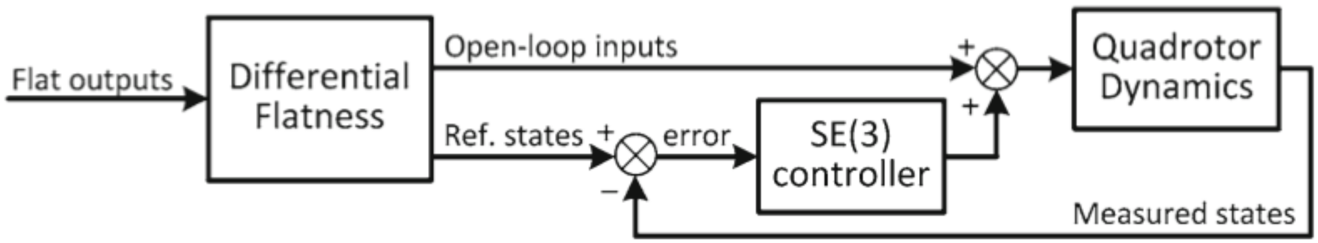
Conservative TL control for **large & complex** dynamics

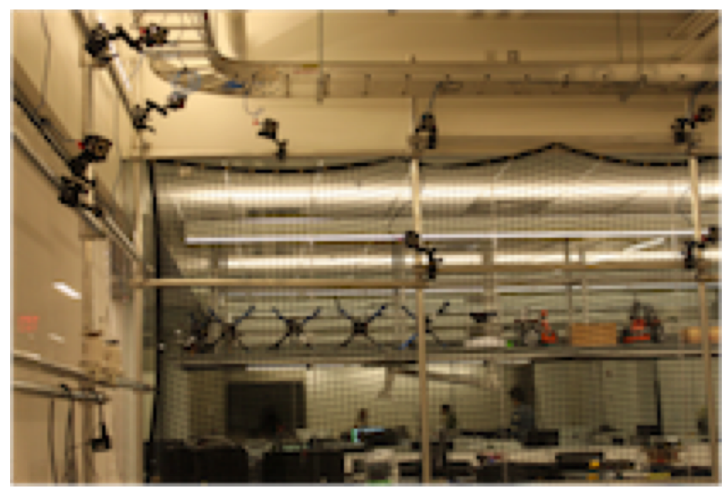
Mapping complex dynamics to simple dynamics: differential flatness

Quadrotor dynamics

- Nonlinear control system with 12 states (position, rotation, and their derivatives) with 4 inputs (total thrust force from rotors and 3 torques)
- Differentially flat with 4 flat outputs (position and yaw)
- Up to four derivatives of the flat output and necessary to compute the original state and input

Mellinger and Kumar, 2011.; Hoffmann, Waslander, and Tomlin, 2008.; Leahy, Zhou, Vasile, Schwager, Belta, 2015



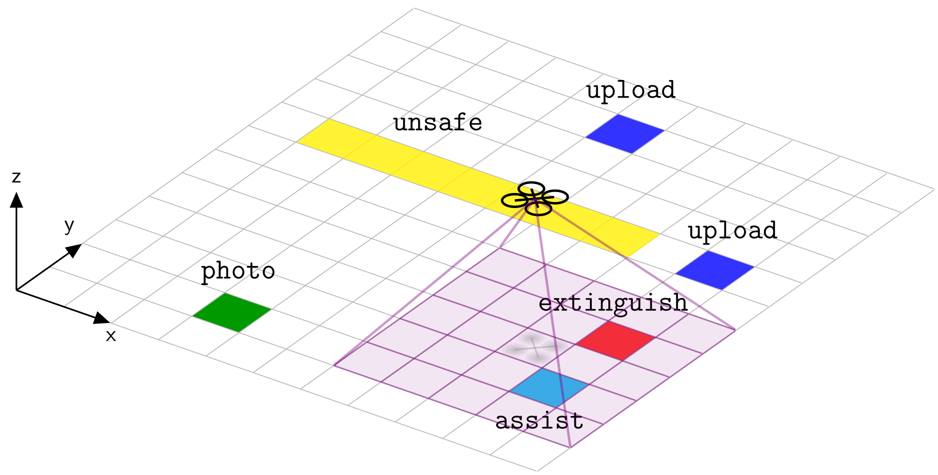


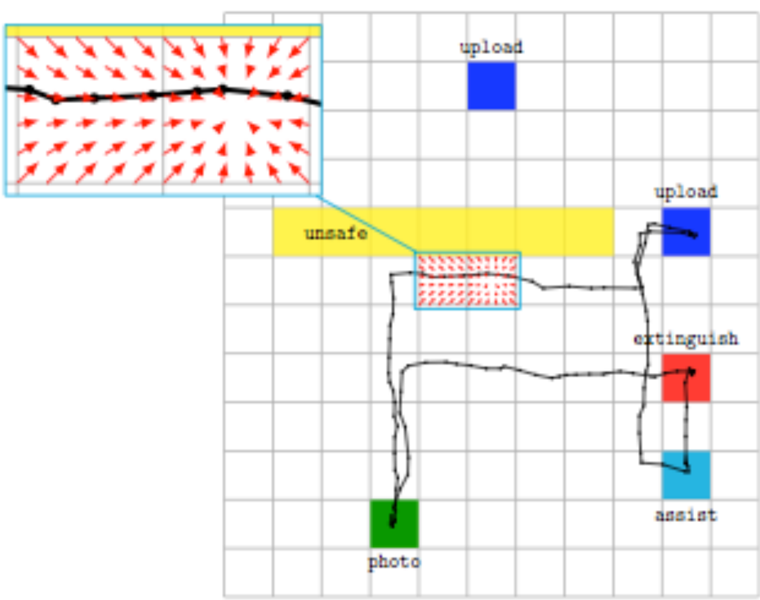
http://sites.bu.edu/robotics/

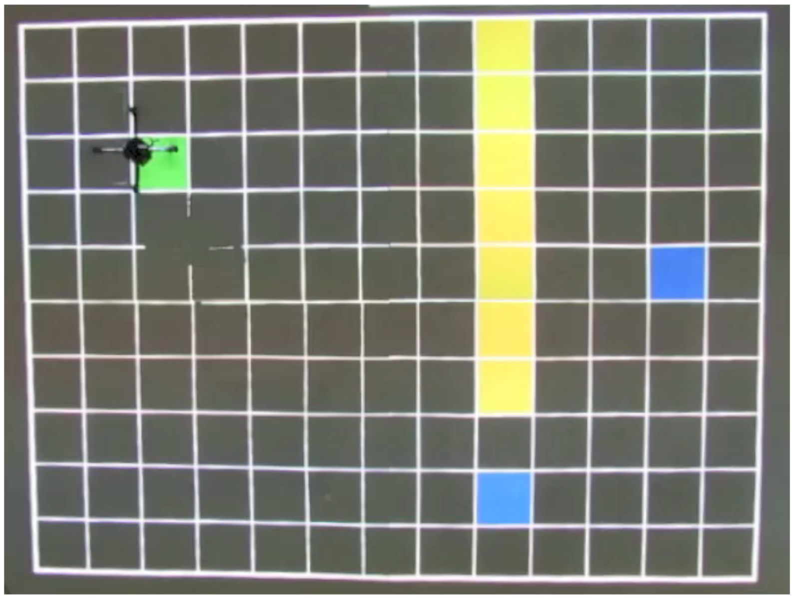
Conservative TL control for large & complex dynamics

Persistent surveillance with global and local specs

Global spec: "Keep taking photos and upload current photo before taking another photo. Unsafe regions should always be avoided. **Local spec:** 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."



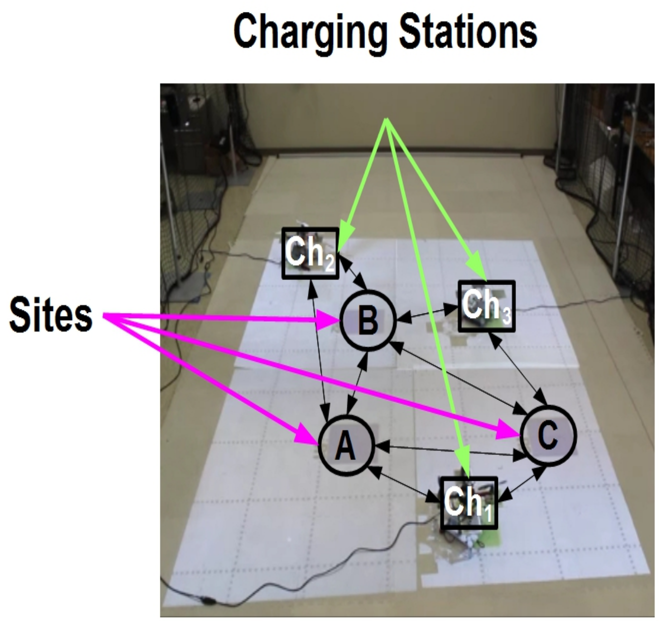


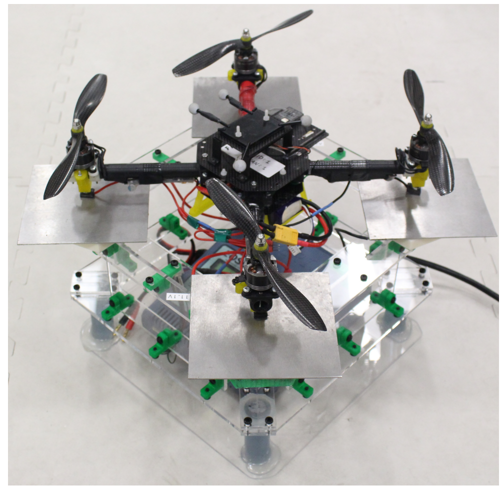


Ulusoy, Belta, RSS 2013, IJRR 2014

Conservative TL control for **large & complex** dynamics

Persistent surveillance with deadlines and resource constraints





Additional constraints:
- operation time
- charging time
- timed temporal specs

Mission Specification: Time Window Temporal Logic (TWTL)

"Service site **A** for **2** time units within **[0, 30]** and site **C** for **3** time units within **[0, 19]**. In addition, within **[0, 56]**, site **B** needs to be serviced for **2** time units followed by either **A** or **C** for **2** time units within **[0, 10]**."

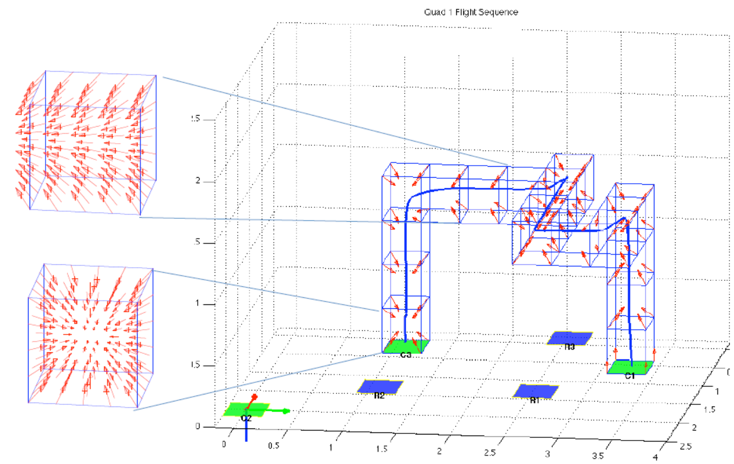
$$\phi_{tw} = [H^2 A]^{[0,30]} \wedge [H^2 B[H^2 A \vee C]^{[0,10]}]^{[0,58]} \wedge [H^3 C]^{[0,19]}$$

Vasile, Aksaray, Belta, Theoretical Computer Science, 2017

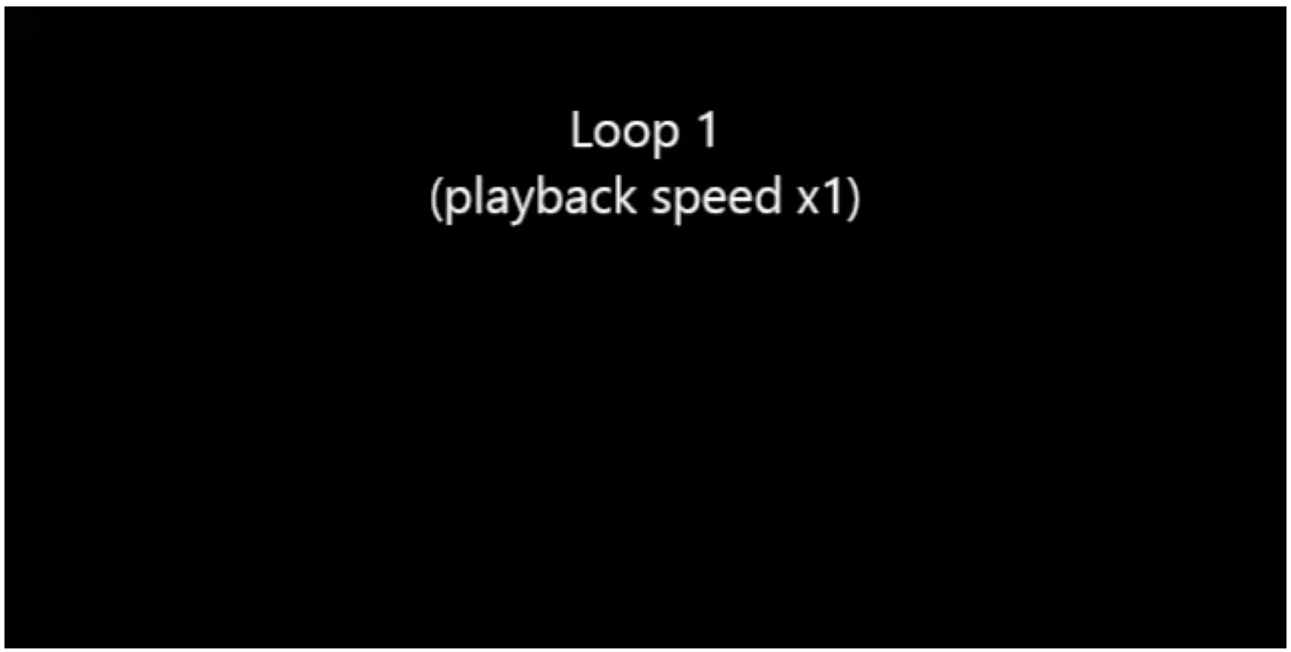
Vasile and Belta, Robotics: Science and Systems (RSS) 2014

Conservative TL control for **large & complex** dynamics

Persistent surveillance with deadlines and resource constraints



"Service site ***A*** for **2** time units within **[0, 30]** and site ***C*** for **3** time units within **[0, 19]**. In addition, within **[0, 56]**, site **B** needs to be serviced for **2** time units followed by either ***A*** or ***C*** for **2** time units within **[0, 10]**."



Vasile, Aksaray, Belta, Theoretical Computer Science, 2017 (accepted)

Vasile and Belta, Robotics: Science and Systems (RSS) 2014

Outline

TL verification and control for finite systems

Conservative TL control for **small & simple** dynamical systems

Conservative TL control for **large & complex** dynamical systems

---

Less conservative *optimal* TL control for **small & simple** dynamical systems

Less conservative TL control for **large & (possibly) complex** dynamical systems

Less conservative *optimal* TL control for **large & simple** dynamical systems

Limitation

TL = Temporal Logic

Outline

TL verification and control for finite systems

Conservative TL control for **small & simple** dynamical systems

Conservative TL control for **large & complex** dynamical systems

Less conservative *optimal* TL control for **small & simple** dynamical systems

Less conservative TL control for **large & (possibly) complex** dynamical systems

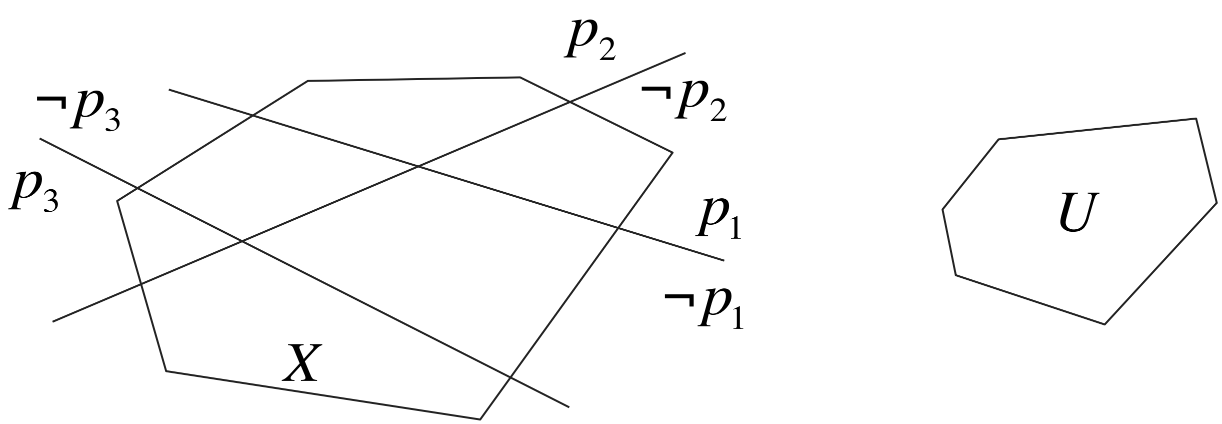
Less conservative *optimal* TL control for **large & simple** dynamical systems

Limitation

TL = Temporal Logic

Less conservative TL control for **small and simple** dynamics

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



Problem Formulation: Find a set of initial states and a state-feedback control strategy such that all trajectories of the closed loop system originating there satisfy an scLTL formula over a set of linear predicates

Language-guided Approach:
- Automaton-based partitioning and iterative refinement
- Polyhedral Lyapunov functions used to construct polytope-to-polytope controllers
- Solution is complete! (modulo linear partition and polyhedral Lyapunov functions)

E. Aydin Gol, M. Lazar, C. Belta., HSCC 2012, IEEE TAC 2014

Less conservative TL control for **small and simple** dynamics

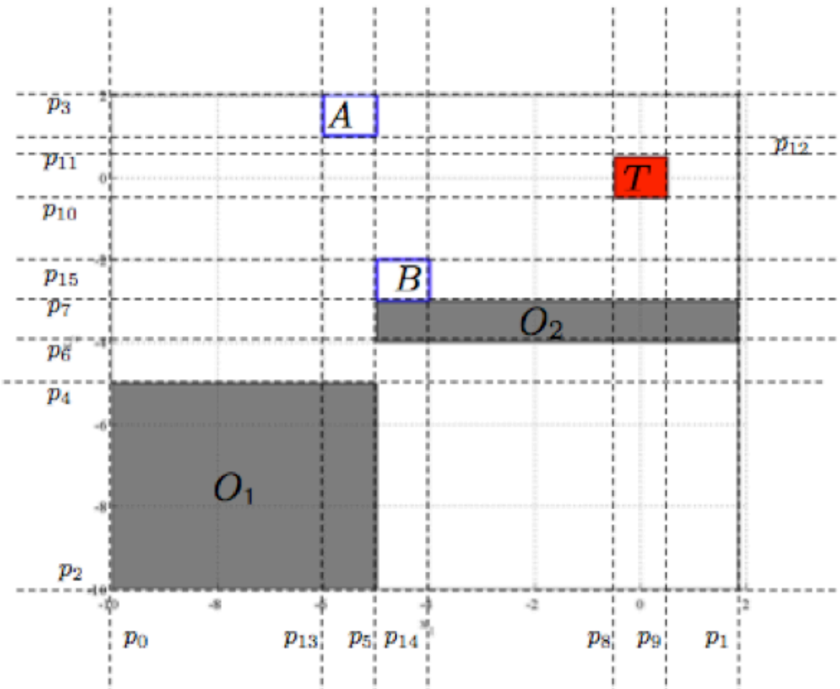
Example

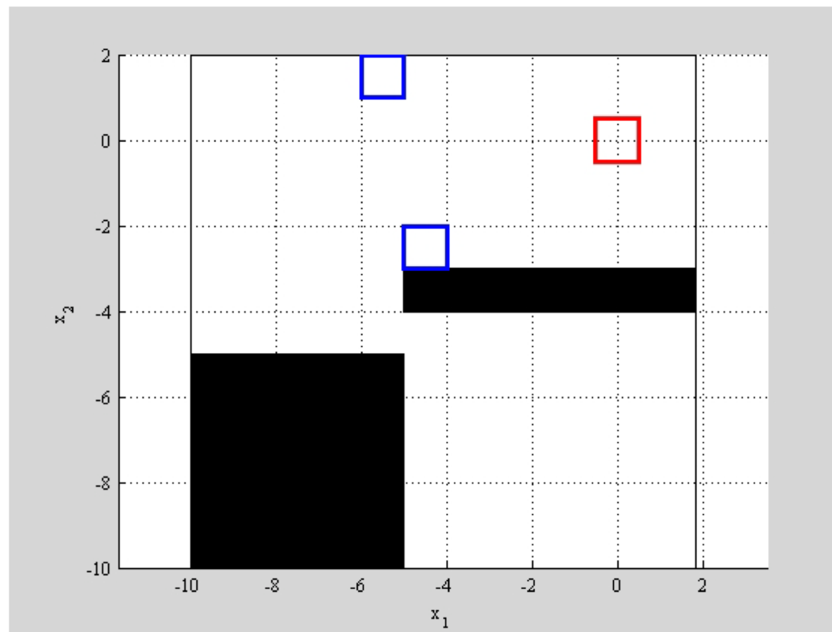
$$x_{k+1} = Ax_k + Bu_k, \quad x_k \in \mathbb{X},\ u_k \in \mathbb{U}.$$

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

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

$$\Phi_2 = ((p_0 \wedge p_1 \wedge p_2 \wedge p_3 \wedge \neg(p_4 \wedge p_5) \wedge \neg(\neg p_5 \wedge \neg p_6 \wedge p_7)) \,\mathcal{U}\, (\neg p_8 \wedge p_9 \wedge \neg p_{10} \wedge p_{11})) \wedge (\neg(\neg p_8 \wedge p_9 \wedge \neg p_{10} \wedge p_{11}) \,\mathcal{U}\, ((p_5 \wedge \neg p_{12} \wedge \neg p_{13}) \vee (\neg p_5 \wedge \neg p_7 \wedge p_{14} \wedge p_{15})))$$



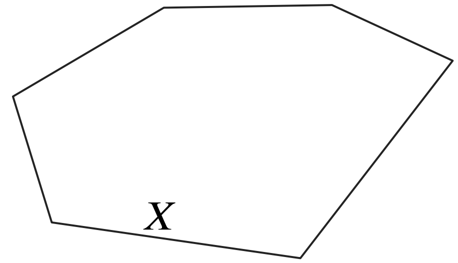


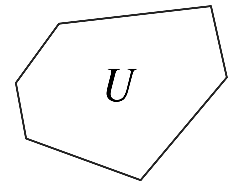
E. Aydin Gol, M. Lazar, C. Belta., HSCC 2012, IEEE TAC 2014

Less conservative *optimal* TL control for **small and simple** dynamics

Optimal TL 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:

$x_0^r, x_1^r \dots$

$u_0^r, u_1^r, \dots$

Observation horizon : N

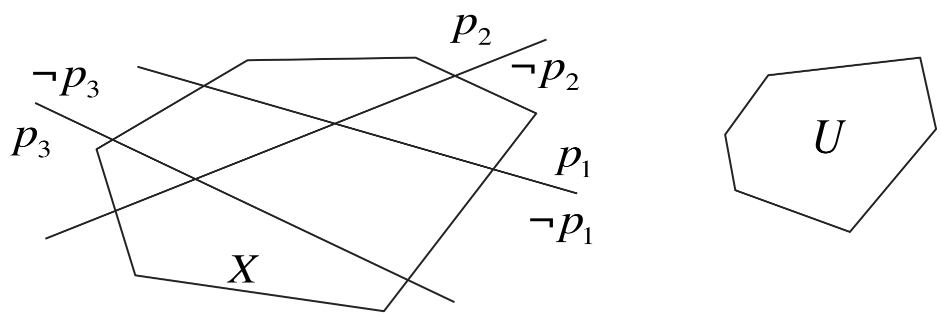
$$C(x_k, \mathbf{u}_k) = (x_{k+N} - x_{k+N}^r)^\top L_N (x_{k+N} - x_{k+N}^r) + \sum_{i=0}^{N-1} \left\{ (x_{k+i} - x_{k+i}^r)^\top L (x_{k+i} - x_{k+i}^r) + (u_{k+i} - u_{k+i}^r)^\top R (u_{k+i} - u_{k+i}^r) \right\},$$

Standard Model Predictive Control
(MPC, Receding Horizon)

Less conservative *optimal* TL control for small and simple dynamics

Optimal TL 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:

$x_0^r, x_1^r \dots$

$u_0^r, u_1^r, \dots$

Observation horizon : N

$$C(x_k, \mathbf{u}_k) = (x_{k+N} - x_{k+N}^r)^\top L_N (x_{k+N} - x_{k+N}^r) + \sum_{i=0}^{N-1} \left\{ (x_{k+i} - x_{k+i}^r)^\top L (x_{k+i} - x_{k+i}^r) + (u_{k+i} - u_{k+i}^r)^\top R (u_{k+i} - u_{k+i}^r) \right\},$$

Standard Model Predictive Control (MPC, Receding Horizon)

Problem Formulation: Find an optimal state-feedback control strategy such that the trajectory originating at x_0 satisfies an scLTL formula over linear predicates p_i

Language-guided MPC Approach:

- Work on the refined automaton from the above TL control problem
- Enumerate paths of length given by the horizon and compute the costs.
- Terminal constraints ensuring the acceptance condition of the automaton: Lyapunov-like energy function
- Solve QP to find the optimal path

E. Aydin Gol, M. Lazar, C. Belta, Automatica 2015

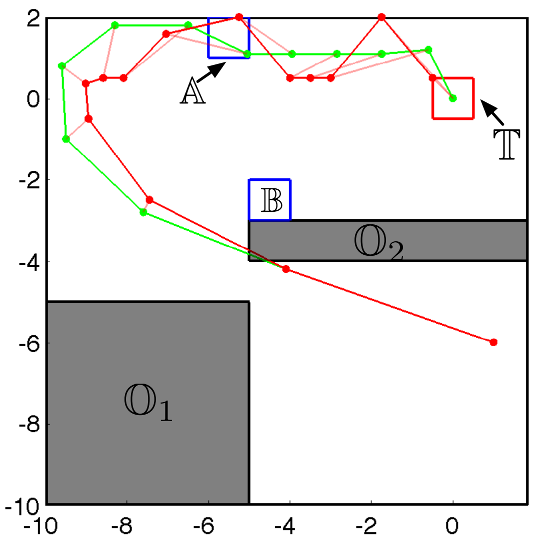
Less conservative *optimal* TL control for **small and simple** dynamics

Example

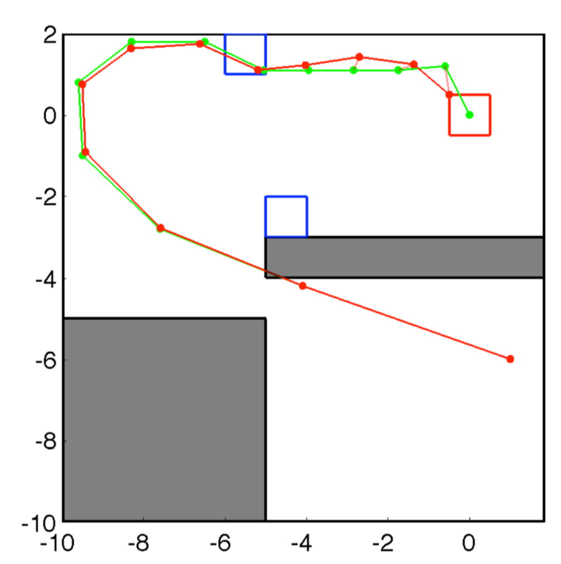
$$x_{k+1} = Ax_k + Bu_k, \quad x_k \in \mathbb{X},\ u_k \in \mathbb{U}$$

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

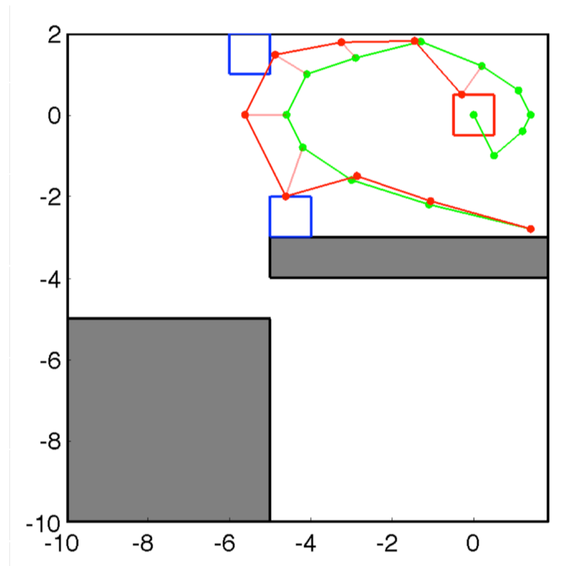
- "Visit region A or region B before reaching the target while always avoiding the obstacles"
- Minimize the quadratic cost with $L=L_N=0.5I_2$, $R=0.2$



N = 2
total cost = 29.688



N = 4
total cost = 0.886



N = 6
total cost = 5.12

Reference trajectory violates the specification

Reference trajectory
Controlled trajectory

E. Aydin Gol, M. Lazar, C. Belta, Automatica 2015

Outline

TL verification and control for finite systems

Conservative TL control for **small & simple** dynamical systems

Conservative TL control for **large & complex** dynamical systems

Less conservative *optimal* TL control for **small & simple** dynamical systems

---

Less conservative TL control for **large & (possibly) complex** dynamical systems

Less conservative *optimal* TL control for **large & simple** dynamical systems

Limitation

TL = Temporal Logic

Outline

TL verification and control for finite systems

Conservative TL control for **small & simple** dynamical systems

Conservative TL control for **large & complex** dynamical systems

Less conservative *optimal* TL control for **small & simple** dynamical systems

Less conservative TL control for **large & (possibly) complex** dynamical systems

Less conservative *optimal* TL control for **large & simple** dynamical systems

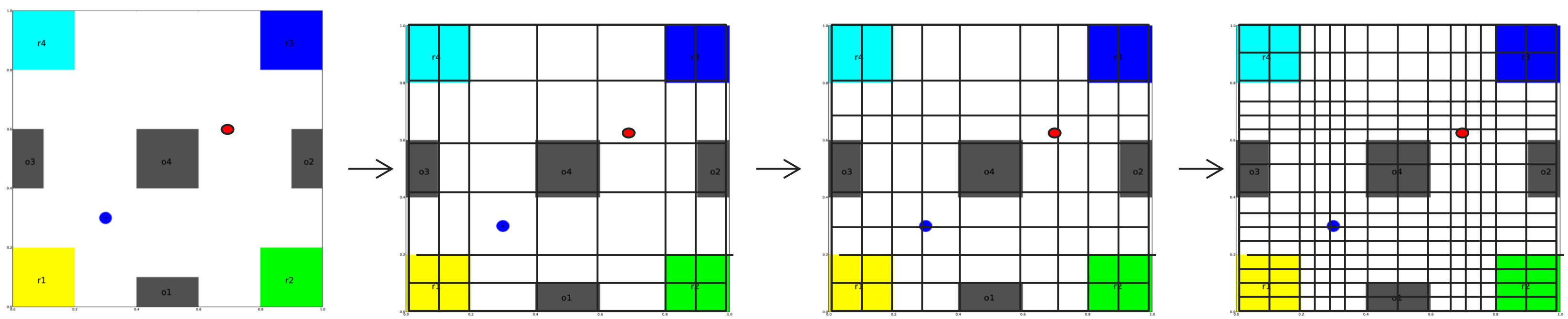
Limitation

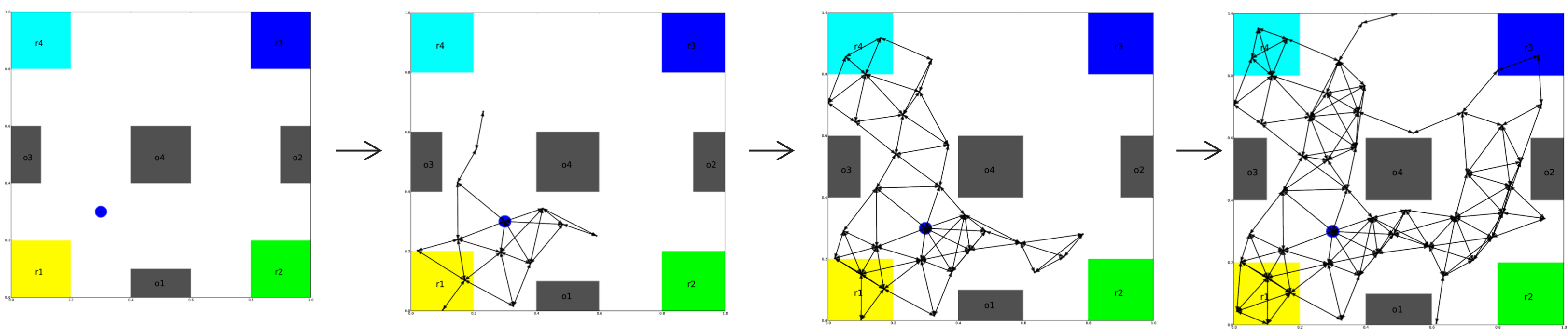
TL = Temporal Logic

Less conservative TL control for **large and complex** dynamics

Iterative Partition vs. Sampling in Motion Planning

Rapidly-exploring Random Trees (RRT) Steve LaValle, 1998
Rapidly-exploring Random Graphs (RRG) Karaman and Frazzoli, 2010





Only "go from A to B specs" can be handled with these techniques

Can we extend sampling-based techniques to temporal logic specs?

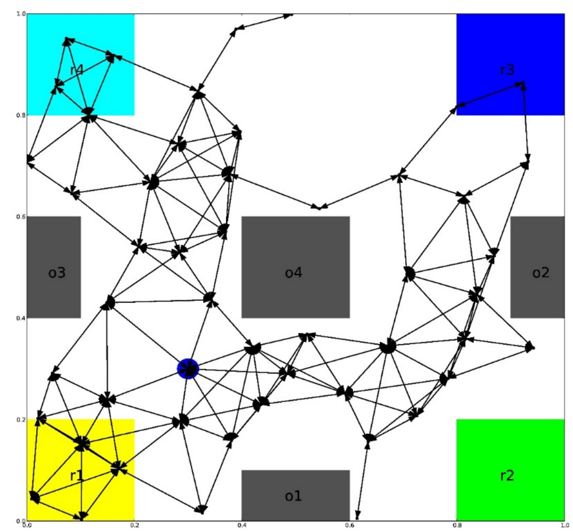
Less conservative TL control for **large and complex** dynamics

Construct a transition system that contains a path satisfying the formula

1. LTL formula is translated to a Büchi automaton;
2. A transition system is incrementally constructed from the initial configuration using an RRG[1]-based algorithm;
3. The product automaton is updated incrementally and used to check if there is a trajectory that satisfies the formula

Important Properties

- Probabilistically **complete**
- **Scales incrementally** (i.e., with the number of added samples at an iteration) - based on incremental Strongly Connected Component (SCC) algorithm [2]



[1]S. Karaman and E. Frazzoli. IJRR , 2011.

[2]Bernhard Haeupler, et al.. ACM Trans. Algorithms, 2012.

C. Vasile and C. Belta. IROS 2013

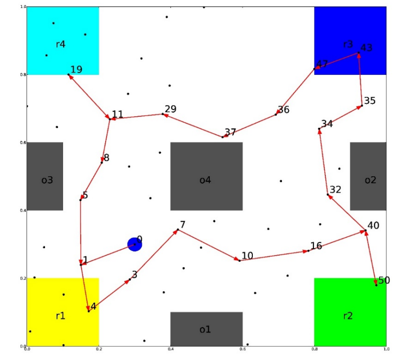
Less conservative TL control for **large and complex** dynamics

Case study 1: 2D configuration space, 20 runs

Average execution time: **6.954 sec**

"Visit regions *r1*, *r2*, *r3* and *r4* infinitely many times while avoiding regions *o1*, *o2*, *o3*, *o4* and *o5*"

$$\phi_1 = \mathbf{G}(\mathbf{F}r1 \wedge \mathbf{F}r2 \wedge \mathbf{F}r3 \wedge \mathbf{F}r4 \wedge \neg(o1 \vee o2 \vee o3 \vee o4))$$



Case study 2: 10-dimensional configuration space, 20 runs

Average execution time: **16.75 sec**

"Visit 3 regions *r1*, *r2*, *r3* infinitely often while avoiding obstacle *o1*

$$\phi_2 = \mathbf{G}(\mathbf{F}r1 \wedge \mathbf{F}r2 \wedge \mathbf{F}r3 \wedge \neg o1)$$

Case study 3: 20-dimensional configuration space, 20 runs

Average execution time: **7.45 minutes**

"Visit 2 regions (*r1*, *r2*) infinitely often"

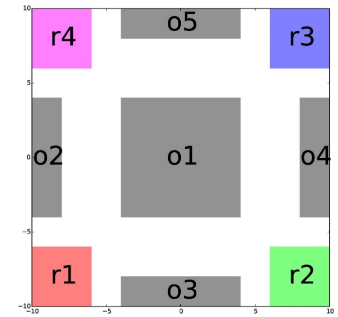
$$\phi_3 = \mathbf{G}(\mathbf{F}r1 \wedge \mathbf{F}r2)$$

Platform: Python2.7 on an iMac – 3.4 GHz Intel Core i7, 16GB of memory

C. Vasile and C. Belta. IROS 2013

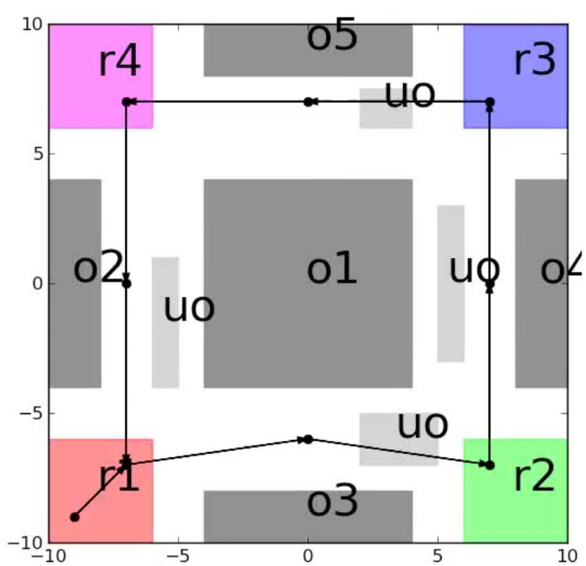
Less conservative TL control for large and complex dynamics

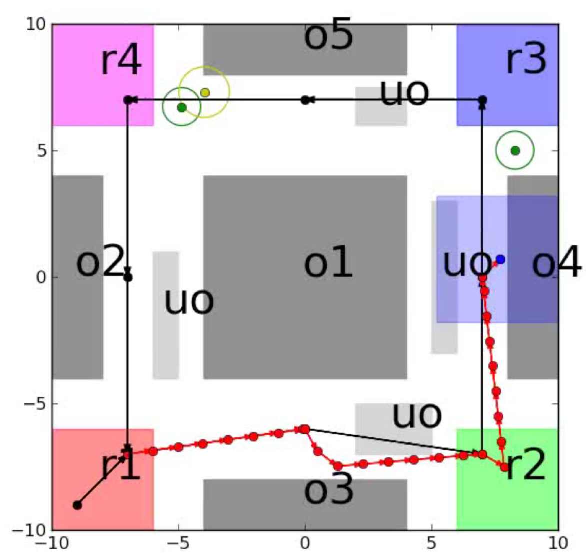
- **Global mission specification**: "visit regions *r1, r2, r3* and *r4* infinitely many times while avoiding regions *o1, o2, o3, o4* and *o5*"
- **Local mission specification**: "Extinguish *fires* and provide medical assistance to *survivors*, with priority given to *survivors*, while avoiding *unsafe areas*"



Off-line part: generate a global transition system that contains a path satisfying the global spec

On-line (reactive) part: generate a local plan that does not violate the global spec





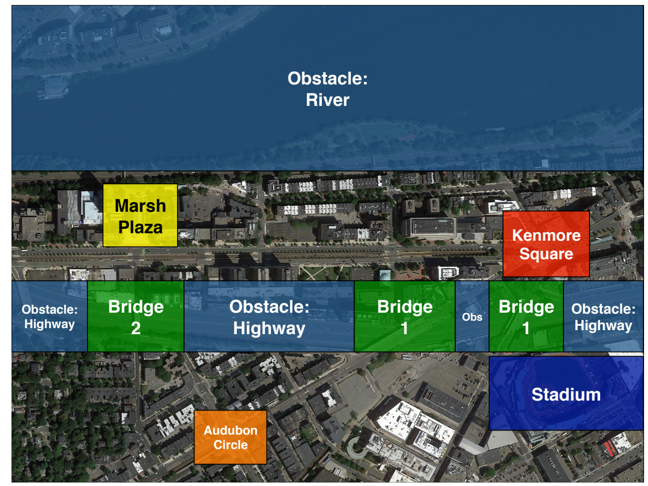
Fires and survivors are sensed locally. These service requests have given service radii.

C. Vasile and C. Belta, ICRA 2014

Less conservative TL control for **large and complex** dynamics

Spec: Maximize the probability of satisfying: "Always avoid all obstacles and Visit Marsh Plaza, Kenmore Square, Fenway Park, and Audubon Circle infinitely often and Bridge 2 should only be used for Northbound travel and Bridges 1 should only be used for Southbound travel. Uncertainty should always be below 0.9 m^2 and when crossing bridges it should be below 0.6 m^2."

- Noisy controllers and sensors
- Unknown map
- No GPS

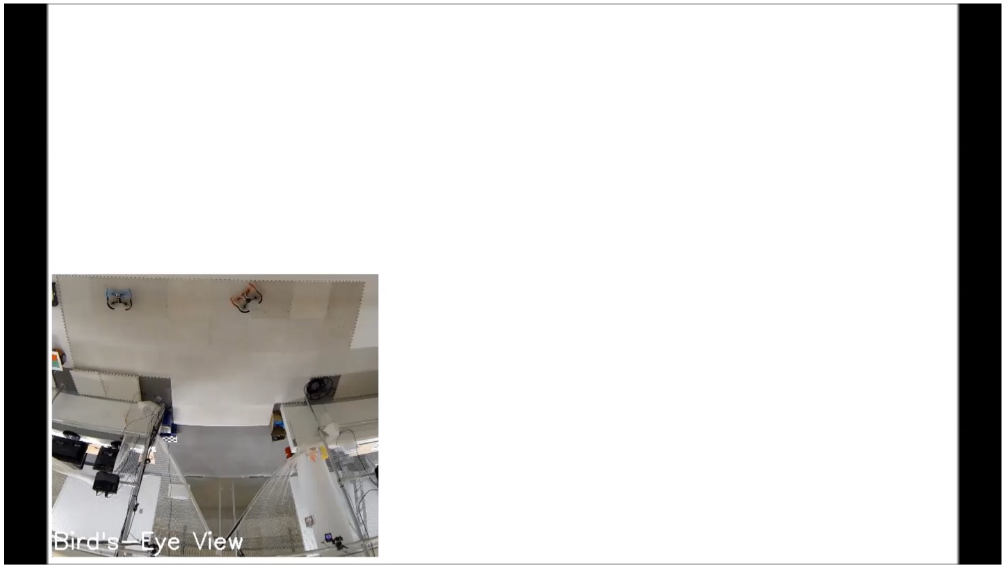


Approach:

- Generate a map of the unknown environment using purely vision and homography-based formation control with multiple quadrotors
- Label the map and define Gaussian Distribution Temporal Logic (GDTL) spec
- Synthesize control policy using GDTL - Feedback Information RoadMaps (GDTL-FIRM)
- Simultaneously track and localize the ground robot with a single aerial vehicle using a homography – based pose estimation and position-based visual servoing control

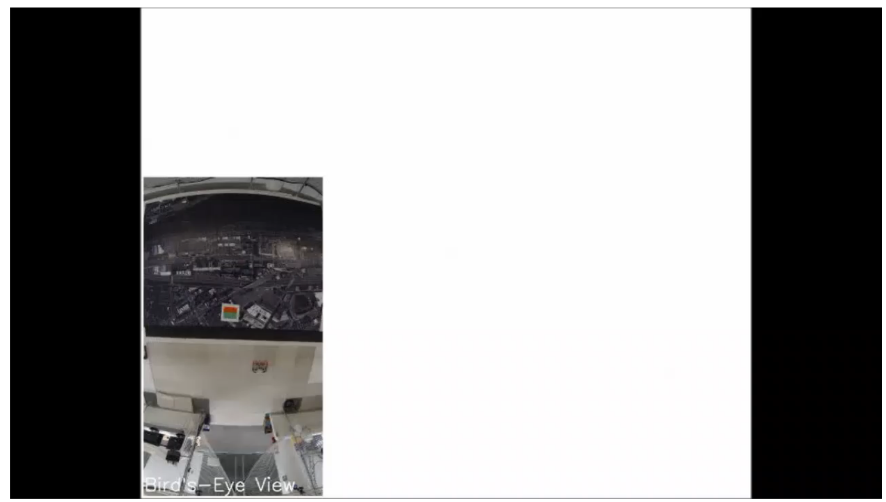
E. Cristofalo, K. Leahy, C.-I. Vasile, E. Montijano, M. Schwager and C. Belta, *ISER* 2016.
C. I. Vasile, K. Leahy, E. Cristofalo, A. Jones, M. Schwager and C. Belta, CDC 2016

Less conservative TL control for **large and complex** dynamics



Map unknown environment

Spec: "Always avoid all obstacles and Visit Marsh Plaza, **Kenmore Square**, **Fenway Park**, and **Audubon Circle** infinitely often and **Bridge 2** should only be used for Northbound travel and **Bridges 1** should only be used for Southbound travel. Uncertainty should always be below 0.9 m^2 and when crossing bridges it should be below 0.6 m^2."



Localization and control

E. Cristofalo, K. Leahy, C.-I. Vasile, E. Montijano, M. Schwager and C. Belta, *ISER* 2016.
C. I. Vasile, K. Leahy, E. Cristofalo, A. Jones, M. Schwager and C. Belta, CDC 2016

Outline

TL verification and control for finite systems

Conservative TL control for **small & simple** dynamical systems

Conservative TL control for **large & complex** dynamical systems

Less conservative *optimal* TL control for **small & simple** dynamical systems

Less conservative TL control for **large & (possibly) complex** dynamical systems

---

Less conservative *optimal* TL control for **large & simple** dynamical systems

Limitation

TL = Temporal Logic

Outline

TL verification and control for finite systems

Conservative TL control for **small & simple** dynamical systems

Conservative TL control for **large & complex** dynamical systems

Less conservative *optimal* TL control for **small & simple** dynamical systems

Less conservative TL control for **large & (possibly) complex** dynamical systems

Less conservative *optimal* TL control for **large & simple** dynamical systems

Limitation

TL = Temporal Logic

Less conservative *optimal* TL control for **large & simple** dynamics

Signal Temporal Logic: Boolean (Qualitative) and Quantitative Semantics

- Temporal operators are timed
- Semantics defined over signals
- Has qualitative semantics: real-valued function $\rho(s, \phi)$

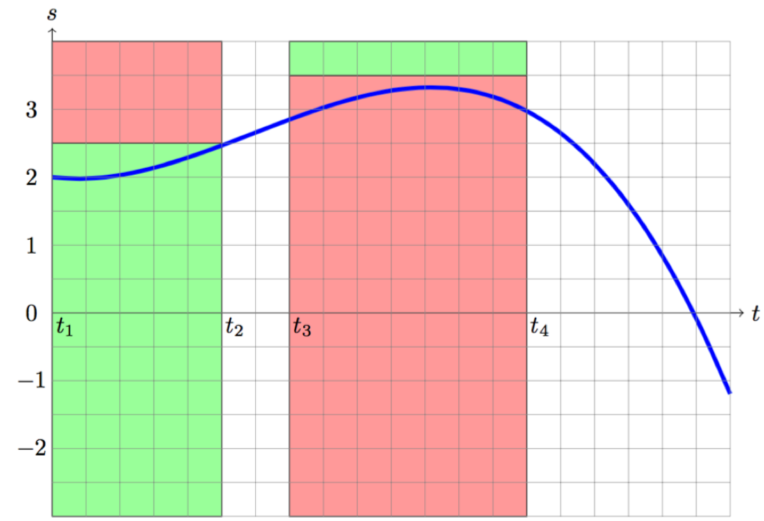
$$\square_{[t_1,t_2]}(s \leq 2.5) \qquad \lozenge_{[t_3,t_4]}(s > 3.5)$$

Boolean: True
Quantitative: 0.01

Boolean: False
Quantitative: -0.2

$$\square_{[t_1,t_2]}(s \leq 2.5) \wedge \lozenge_{[t_3,t_4]}(s > 3.5)$$

Boolean: False
Quantitative: -0.2



- Boolean satisfaction of STL formulae over linear predicates can be mapped to feasibility of mixed integer linear equalities / inequalities (MILP feasibility)
- Robustness is piecewise affine in the integer and continuous variables

Donze & Maler 2004, Fainekos et.al. 2009 Raman et. al, 2014 Sadraddini & Belta, 2015

Less conservative *optimal* TL control for **large & simple** dynamics

Optimal STL Control

$$\min_{u^H} J(x^H, u^H)$$ (any linear cost)

subject to

dynamics

$$x^+ = f(x, u)$$ (any MLD system, e.g., piecewise affine)

correctness

$x^H,\ u^H$ satisfy STL formula over linear predicates

Reduces to solving a MILP!

Less conservative *optimal* TL control for **large & simple** dynamics

Planar Robot Example

$$x^+ = x + u$$

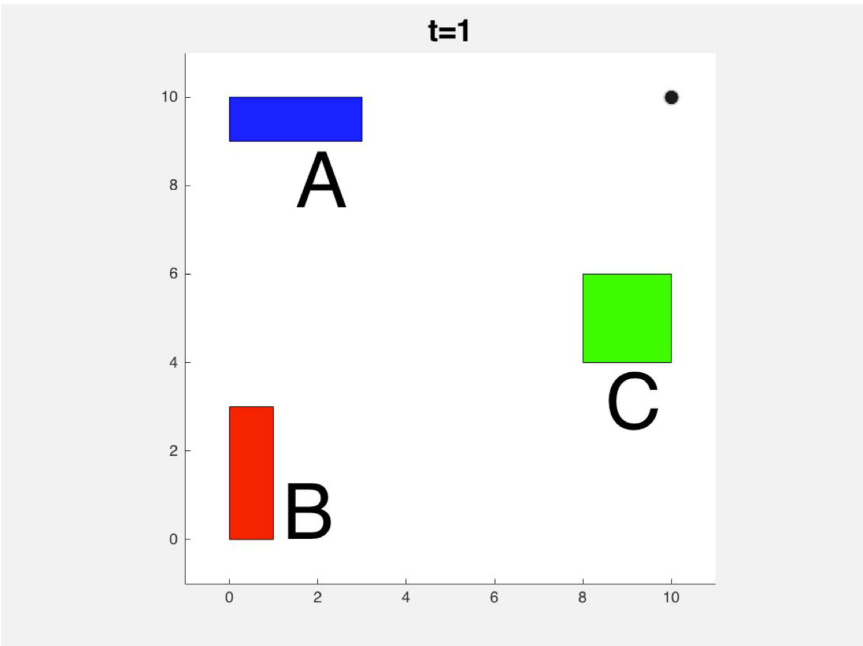
$$\varphi = \Box_{[40,50]} A \ \wedge \ \Diamond_{[0,40]} \Box_{[0,10]} B \ \wedge \ \Diamond_{[0,30]} C \qquad H = 50$$

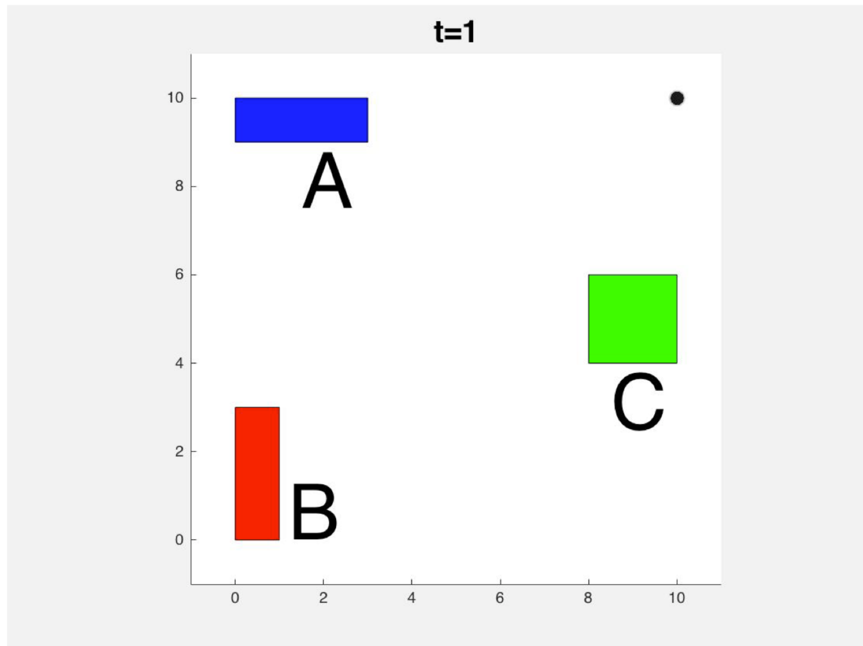
Minimum Fuel Only

$$J = \sum_{\tau=0}^{H-1} \left| u[\tau] \right|$$

Maximum robustness + Minimum fuel

$$J = -1000\rho + \sum_{\tau=0}^{H-1} \left| u[\tau] \right|$$





Sadraddini and Belta, Allerton Conference, 2015

Less conservative *optimal* TL control for **large & simple** dynamics

STL Model Predictive Control (MPC)

Repetitive tasks in infinite time: global STL formulas: $\Box_{[0,\infty]}\varphi$

$$u^H[t] = \text{argmin} \quad J(x^H[t], u^H[t])$$
$$\text{subject to} \quad x^+ = f(x,u)$$
$$x^H(t) \models \varphi \text{ over } H$$

$$J = J_c$$

$$J = \rho$$

$$J = -M(\rho - \|\rho\|) + J_c$$

M is a large number. When $\rho < 0$, effectively maximize $2M\rho$

Terminal constraints are guaranteed!

Sadraddini and Belta,, 2015

Less conservative *optimal* TL control for **large & simple** dynamics

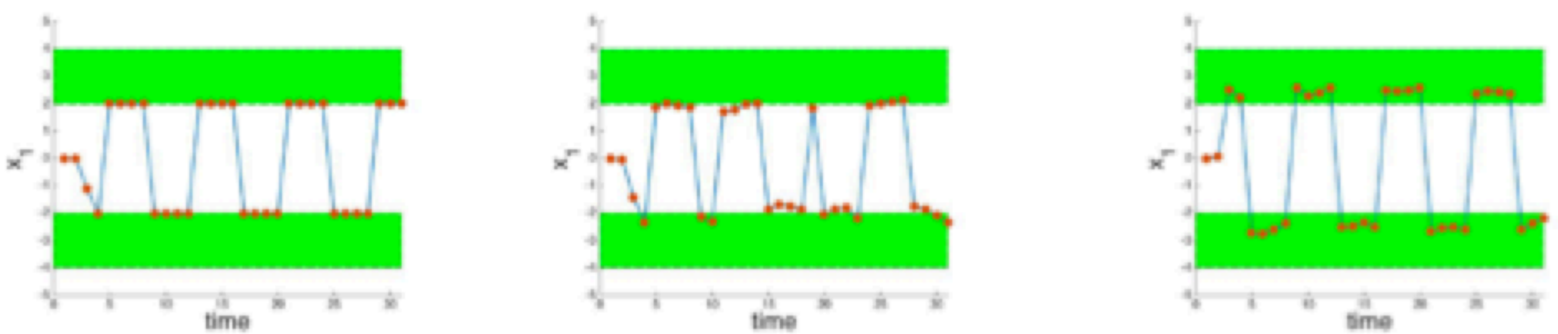
Example: Double Integrator

$$x^+ = \begin{pmatrix} 1 & 0.5 \\ 0 & 0.8 \end{pmatrix} x + \begin{pmatrix} 0 \\ 1 \end{pmatrix} + w$$

Spec: $\square_{[0,\infty]} \left(\lozenge_{[0,4]}((x_1 \leq 4) \wedge (x_1 \geq 2)) \wedge \lozenge_{[0,4]}((x_1 \geq -4) \wedge (x_1 \leq -2))\right)$

Minimize fuel consumption. If the spec becomes infeasible, maximize robustness.

$$J_c = \sum_{\tau=t}^{t+H-1} \left| u[\tau] \right|$$



a) $w[t] = 0$
MPC

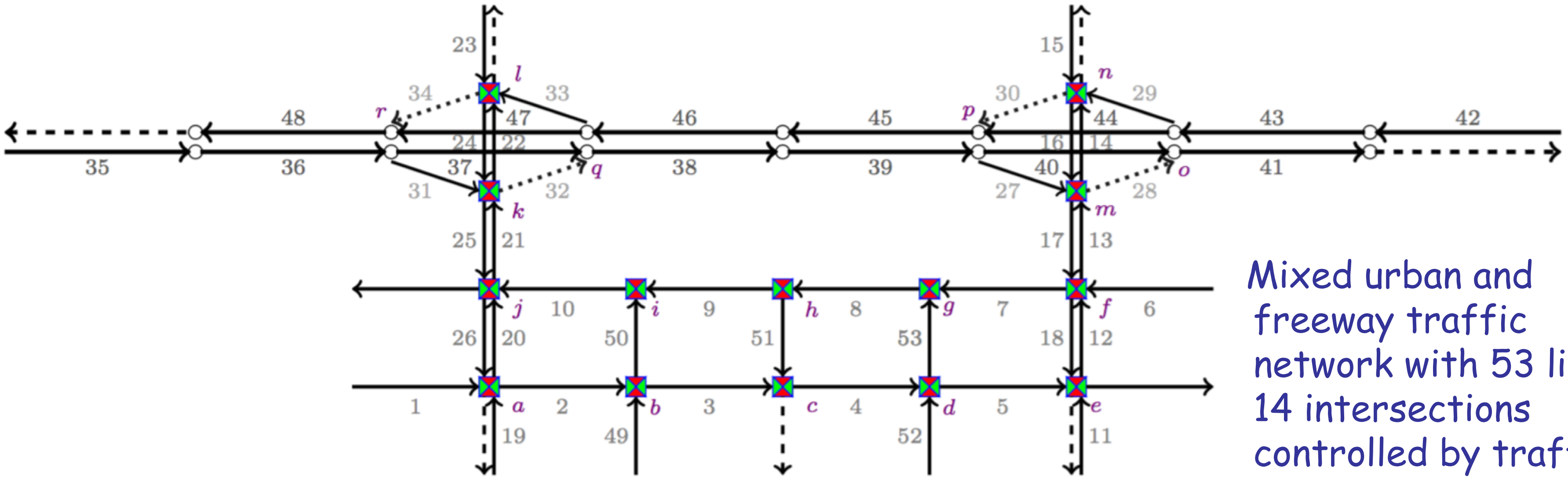
b) $\|w[t]\|_\infty \leq 0.2$
nominal MPC

c) $\|w[t]\|_\infty \leq 0.2$
robust MPC

Sadraddini and Belta 2015

Less conservative *optimal* TL control for **large & simple** dynamics

Example: Traffic network



Mixed urban and freeway traffic network with 53 links, 14 intersections controlled by traffic lights, 4 ramp meters

Model: discrete-time piecewise affine system

Spec: $\square_{[0,\infty]}\varphi$

$$\varphi = (x \in \Pi) \wedge \bigwedge_{l=49,50,\cdots,53} (x_l \geq 3) \Rightarrow \Diamond_{[0,3]}(x_l \leq 3)$$

Congestion free

If density ever reaches 3, then in 3 minutes should become less than 3

Cost: delay over a given horizon

Takes less than 5 sec. to compute a optimal robust control strategy (MILP in 212 dimensions)

Sadraddini and Belta 2016

Summary

- Automata (Buchi, Rabin) games can be adapted to produce conservative TL control strategies for simple and small dynamical systems
- The above can be extended to conservative strategies for large and complicated systems by using I/O linearization techniques
- Partition refinement can be used to reduce conservatism for simple and small dynamical systems -> connection between optimality and TL correctness
- **Sample-based techniques can be used to generate probabilistically complete TL strategies in high dimensions**
- **TL with quantitative semantics can be used for robust, provably-correct optimal control in high dimensions**

Acknowledgements

Cristian Vasile
(now at MIT)

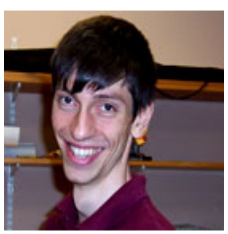
Sadra Sadraddini
(now at MIT)

Kevin Leahy
(now at Lincoln Lab, MIT)

Ebru Aydin Gol
(now at Google)

Austin Jones
(now at Lincoln Lab , MIT)

Derya Aksaray
(now at U. Minnesota)



Marius Kloetzer
(now at UT Iasi)

Alphan Ulusoy
(now at Mathworks)

Jana Tumova
(now at KTH)