GLOBAL INITIATIVE OF ACADEMIC NETWORKS

भारतीय प्रौद्योगिकी संस्थान गुवाहाटी • Indian Institute of Technology Guwahati •

University of Illinois at Urbana-Champaign

Lecture 9: Formal Synthesis Part B

Sayan Mitra

Electrical & Computer Engineering

Coordinated Science Laboratory

University of Illinois at Urbana Champaign

Controller Synthesis for Linear Time-varying Systems with Adversaries

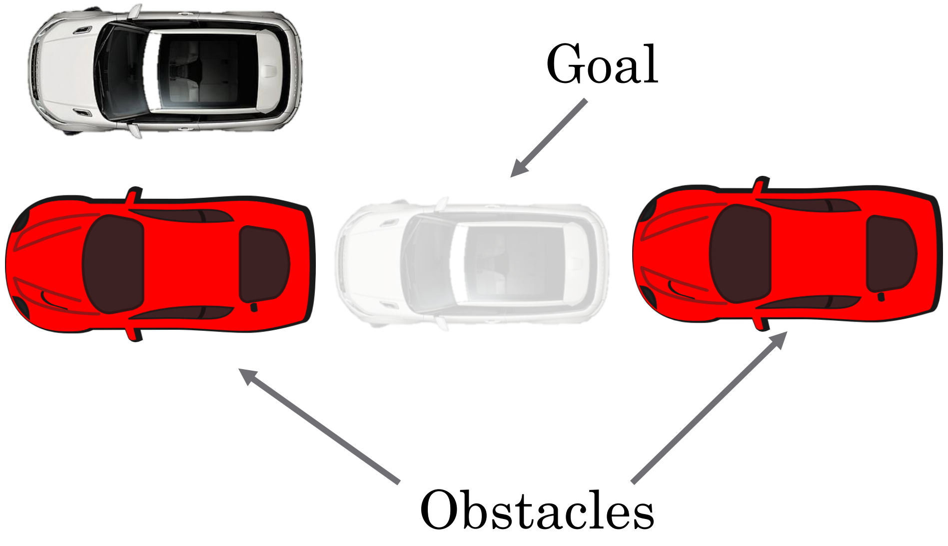
Zhenqi Huang[1], Yu Wang[1]

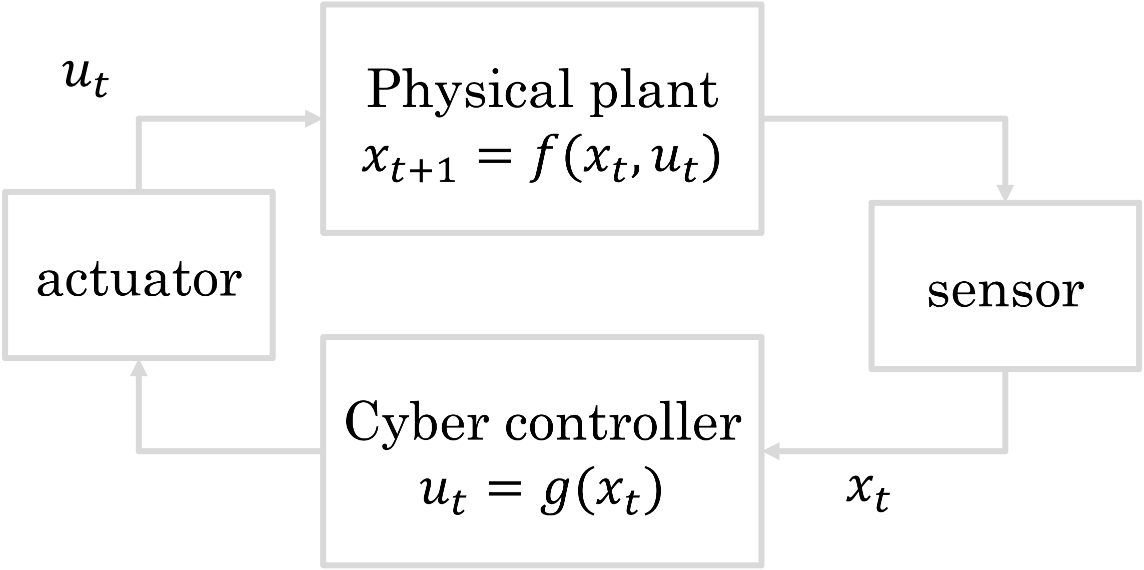
Sayan Mitra[1], Geir Dullerud[1], Swarat Chaudhuri[2]

[1]University of Illinois at Urbana-Champaign

[2]Rice University

Cyber-physical systems reach avoid



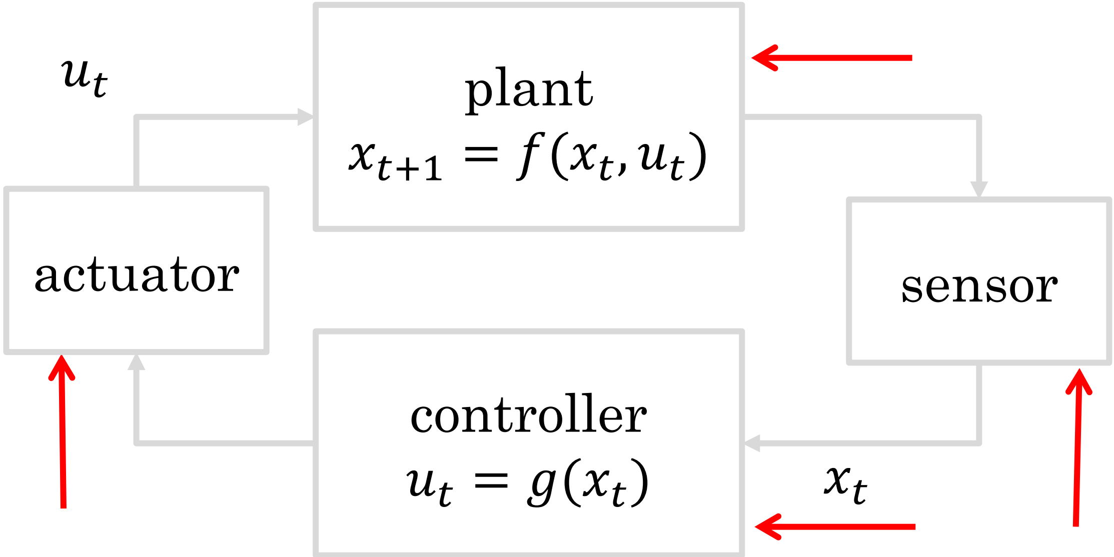


- Requirements:
  - reach goal while avoiding obstacles

x_t: state of plant, e.g. position, heading, velocity
u_t: control command, e.g. throttle, braking, steering

Cyber-physical systems and attack surface

- multi-faceted attack surface
  - error injection to sensor data
  - error injection to actuator command
  - uncertainty in dynamics

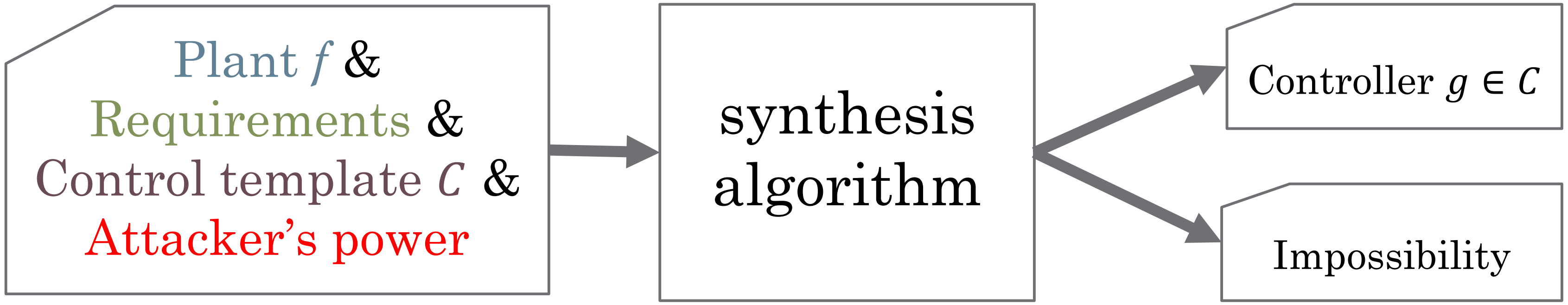


- E.g. spoofing speed sensor, GPS [Shoukry2013], [Warner2003]

- We abstract the attack as an additive error injected to the system
  - i.e. measurement = $x_t + a_t$

- We characterize the power of attacker as $b = \sum ||a_t||^2$

Controller synthesis algorithm



given a system *model*, *safe* and *goal*, find control such that all behaviors are safe and reach goal

- yes (controller strategy g)
- no (impossibility certificate "no controller exists")

Example: linearized helicopter dynamics

$$x_{t+1} = Ax_t + Bu_t + Ca_t$$

Variables	Components of Variables
x_t 16-dimentional	Cartesian Coordinates / Velocities
	Euler Angles / Velocities
	Flapping Angles
u_t 4-dimentional	Lateral / longitude Deflection
	Pedal / collective control input
a_t 4-dimentional	Additive error injected to each control input channal

Reach-avoid problem formulation

$$x_{t+1} = Ax_t + Bu_t + Ca_t$$

- A, B, C: matrices
- x_t: state at time t with $init$
- u_t: control input to be synthesized
- a_t: adversary input

- Denote $\xi(x_0, u, a, t)$ as the state visited at time t with initial state x_0, control input u and adversary input a

Find u, $\forall a$

$$\forall t \leq T. \xi(x_0, u, a, t) \in safe \wedge \xi(x_0, u, a, T) \in Goal$$

SMT solvers: quick overview

- First order logic formula have quantifiers over variables
  - Example: $\exists y \forall x. (x^2 \leq y + 1) \Rightarrow (\sin x > \cos(\log y))$
- Satisfiability modulo theories (SMT) solvers
  - Finding satisfying solutions for first order logic formula, or
  - Prove no solution satisfies the formula
  - E.g. Z3, CVC4, VeriT, dReal
- Perform best for quantifier-free bitvector/integer/linear arithmetic
  - Scales up to hundreds of real variables & thousands of constraints

- Handle nondeterminism by adversary
- Bounded controller synthesis
- Unbounded controller synthesis

Adversarial leverage

Goal:

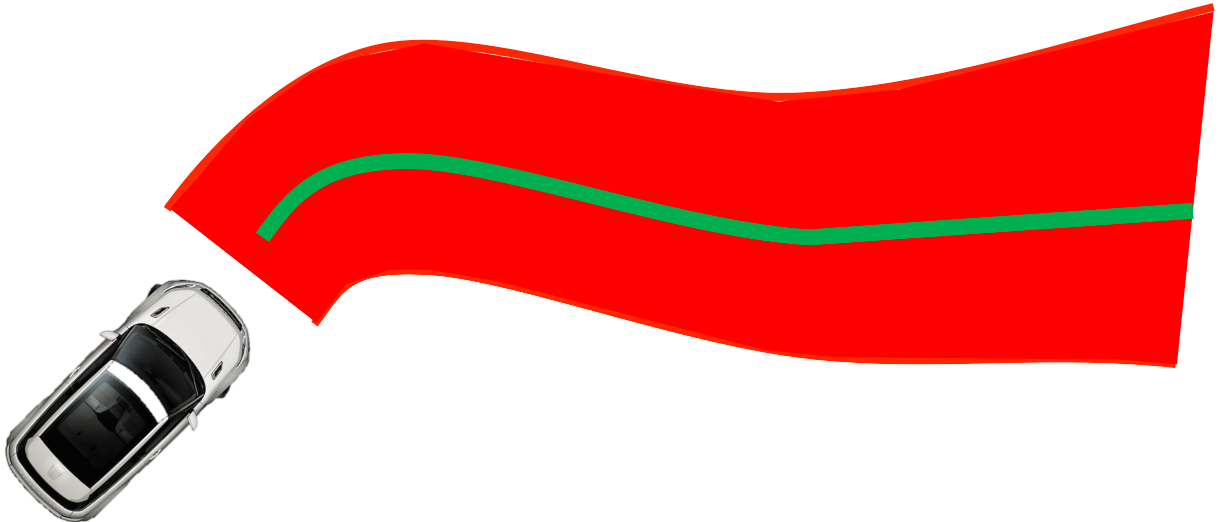
$$\exists u, \forall a, \forall t \leq T.\, \xi(x_0, u, a, t) \in safe \;\wedge\; \xi(x_0, u, a, T) \in Goal$$

Reachability for adversarial input :

$$\text{Reach}(x_0, u, t) = \{\, x \mid \exists a : x = \xi(x_0, u, a, t)\}$$

Adversarial leverage :

$$\text{Reach}(x_0, u, t) = \xi(x_0, u, 0, t) \oplus L(x_0, u, t)$$



Linear system with L2 attack budget

When the adversary's budget is $\sum||a_t||^2 \leq b$, in the linear system $x_{t+1} = Ax_t + Bu_t + Ca_t$.

The adversarial leverage is an ellipsoid independent of x_t and u_t

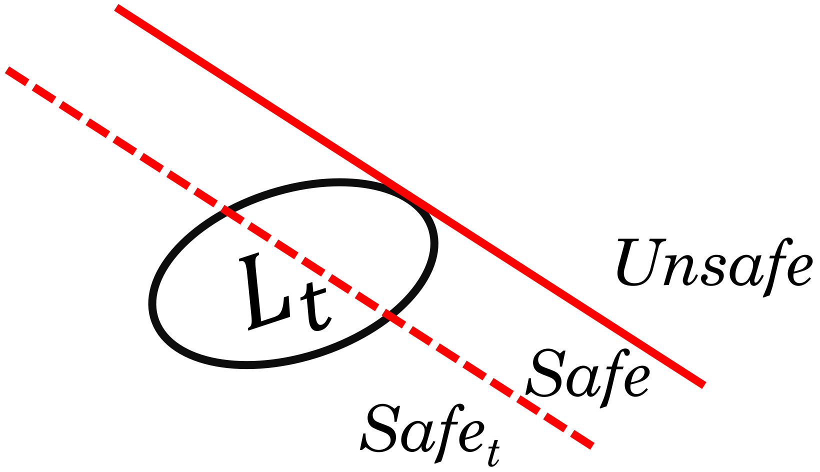
$$L_t = \{x \mid x^T W_t^{-1} x \leq b\},$$

where $W_t = \sum_{s=0}^{t-1} A^{t-s-1} C C^T (A^T)^{t-s-1}$

For general systems, $L(x_0, u, t)$ can be computed by reachability tools: flow*, breach, C2E2, et al.

Strengthened safe / goal set

- For each $t \leq T$, generate strengthened set $safe_t$ and $goal_t$:
  - $safe_t = safe \ominus L_t$
  - $goal_t = goal \ominus L_t$
- For ellipsoid adversarial leverage, $safe_t, goal_t$ computed by conic programming



Adversary-free synthesis

- Original problem:

$$\exists u\colon \forall a\colon \wedge_{t\leq T}\ \xi(x_0,u,a,t) \in safe \text{ and } \xi(x_0,u,a,T) \in Goal$$

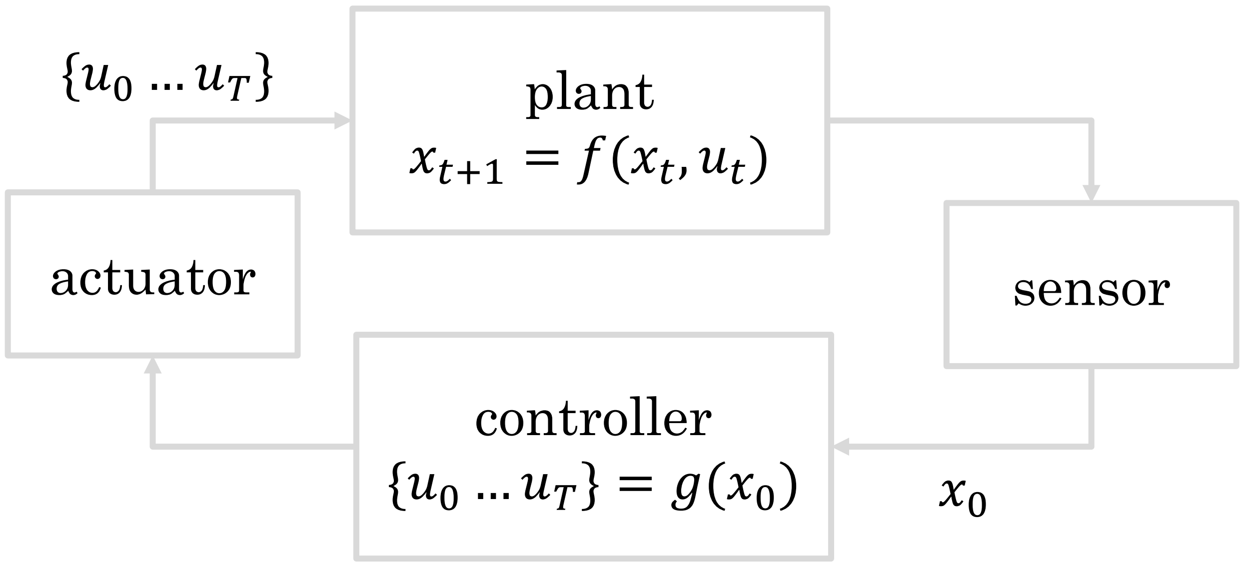
- Adversary-free synthesis:

$$\exists u : \wedge_{t\leq T}\ \xi(x_0,u,0,t) \in safe_t \text{ and } \xi(x_0,u,0,T) \in Goal_T$$

- **Theorem.** the adversary-free synthesis is equivalent to the original problem with adversary

- Handle nondeterminism by adversary
- Bounded controller synthesis
- Unbounded controller synthesis

Open-loop controller

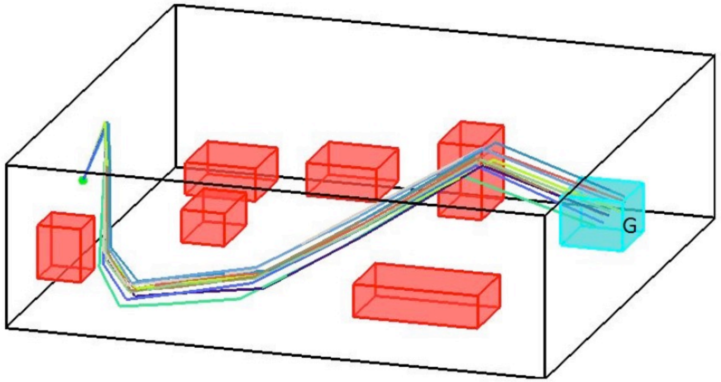


- For finite horizon $\{u_t\}_{t\leq T}$, the reach-avoid problem is equivalent to the satisfiability of the first-order theory

$$\exists u \wedge_{t\leq T} (\xi(x_0, u, 0, t) \in safe_t \wedge \xi(x_0, u, 0, T) \in Goal_T)$$

Application: helicopter autopilot

- Autopilot helicopter
  - 16D, 4 inputs
- $x_{t+1} = A_t x_t + B_t u_t + C_t a_t$
- Adv: $\sum |a_i|^2 \leq b$ intrusion budget constraints

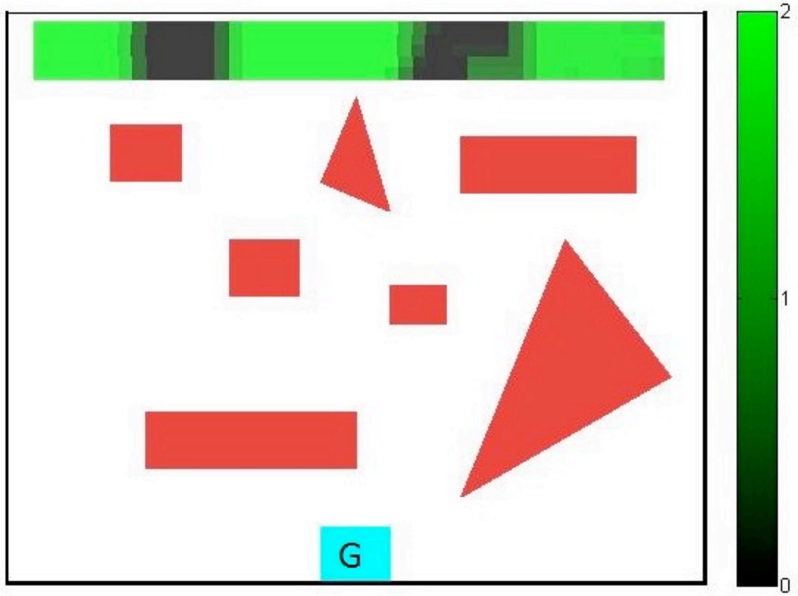


T	$\lvert\phi\rvert$	Result	R.time (s)
40	804	Unsat	2.79
80	3844	Sat	35.22
320	8964	Sat	532.5

Work best for short horizon T

Application: security budget

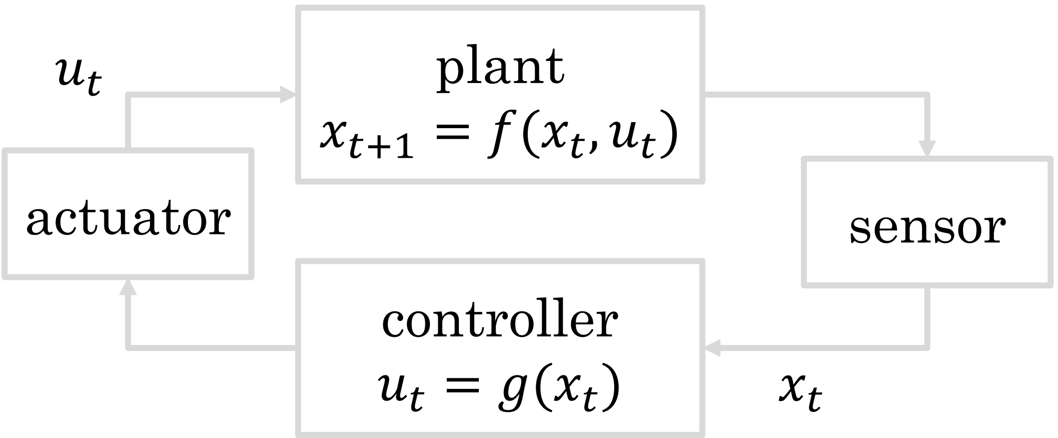
- Security budget determination
  - The minimum budget for adversary such that no safety control exists

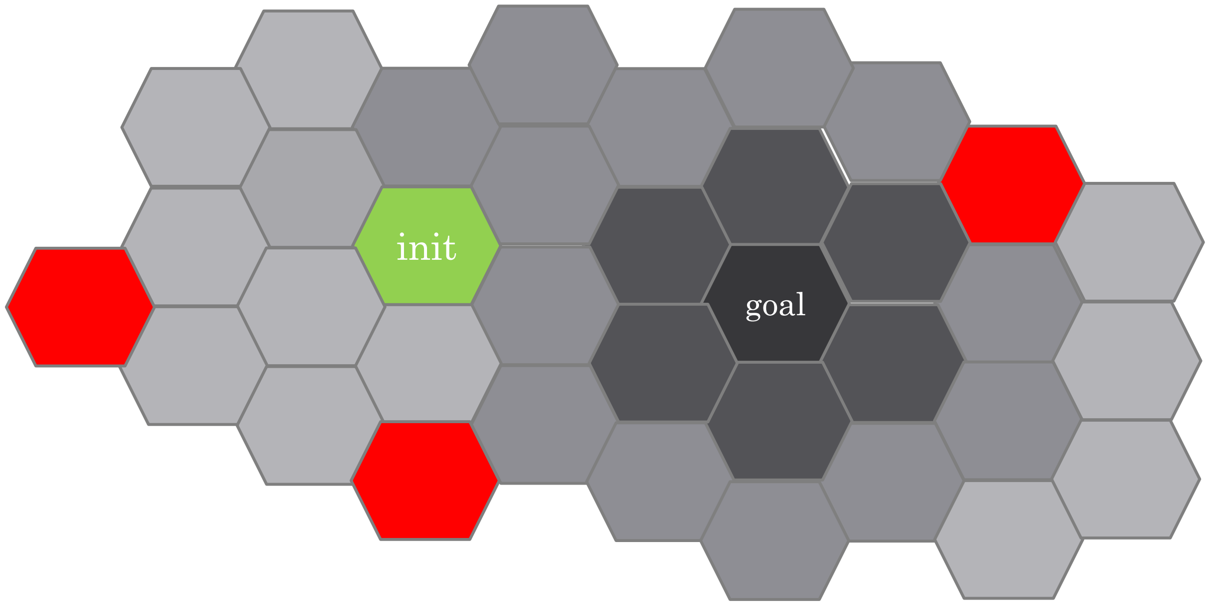


- Handle nondeterminism by adversary
- Bounded controller synthesis
- Unbounded controller synthesis

State-dependent controller as lookup table

- Lookup table controller:
  - ***P***: cover of the state space, sensor quantization or heuristic
  - g: $P \rightarrow U$
  - $post(C, g)$ denote the immediate reachable cells from $C \in \boldsymbol{P}$





Inductive synthesis rules [Huang15]

Find $g: \boldsymbol{P} \rightarrow U, \mathrm{V}: \mathbf{P} \rightarrow \mathbb{N}, k \in \mathbb{N}$ such that for all $C \in \boldsymbol{P}$

g: controller, V: ranking function

- (control invariant) $\mathrm{V}(init) = k \wedge V(C) \geq V\left(post(C, g)\right)$
- (safe) $V(C) \leq k \Rightarrow C \subseteq safe$
- (goal) $C \subseteq goal \Leftrightarrow V(C) = 0;$
- (progress) $0 < \mathrm{V}(C) \leq k \wedge V(C) > V(post^T(C, g))$

soundness & relative completeness of rules

- If the *post*() operator is computed accurately, the algorithm
  - (a) either finds control g and proof V or
  - (b) certifies that there exists no such controller in C, R.

- If the *post*() operator is computed with some bounded error ϵ, the algorithm whether or not there exists a controller that robustly solve the reach-avoid problem.

soundness & relative completeness of rules

- If the $post()$ operator is computed accurately, the algorithm
  - (a) either find control g and proof V or
  - (b) give a proof that there exists no such controller in C, R.

- If the $post()$ operator is computed with some bounded error ϵ, the algorithm whether or not there exists a controller
- the Given controller C and ranking function templates R, the problem M is robust if there exists $\epsilon > 0$:
  - *exists $g \in C, V \in R$ such that for any problem M' that is ϵ-close to M, the g, V solves the synthesis problem for M' with some k, OR*
  - *for none of the problems M' that are ϵ-close to M, have solutions to the synthesis problem with any $g \in C, V \in R$*

Application: path planning

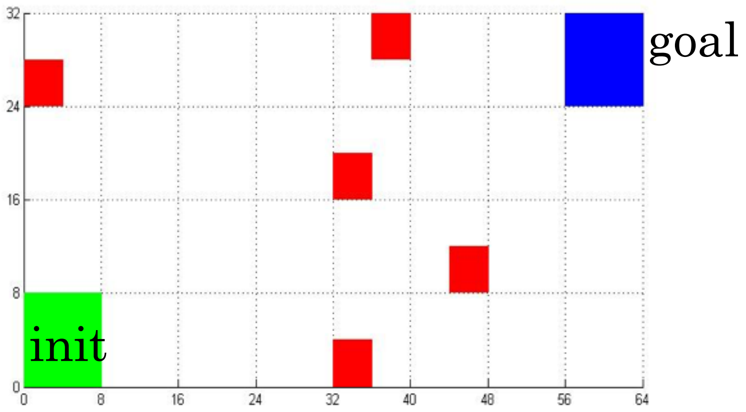
implemented using CVC4 SMT solver

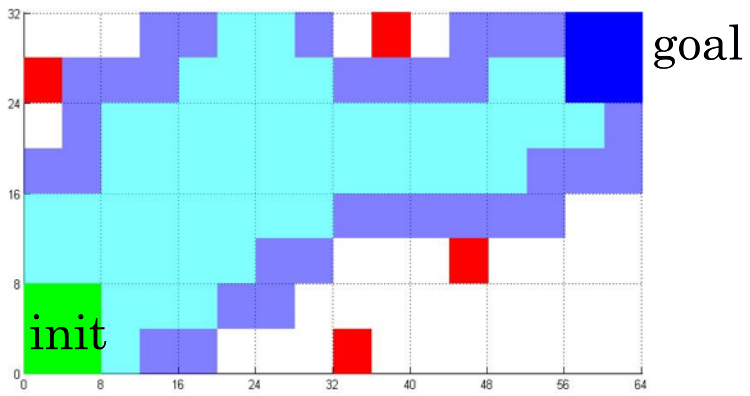
4D nonlinear vehicle navigation with noise and obstacles

C: regions in state space

$V: C \to \mathbb{N}$

768 cells, 3072 real-valued/boolean variables, solved in less than 10 minutes





Light (under) and dark (over) approximation of post

Summary and outlook

- We have developed a new class of synthesis algorithms for control systems under attacks
- The approach allows us to automatically characterize feasibility of control problems in terms of the strength of attackers
- We use SMT-solvers to compute both bounded and unbounded time controllers
- Ongoing: synthesis of attacks on power networks
  - goal: system unstable

Going forward

- Review the notes and slides (big gain)
- Choose your favorite application and model it
- Try to verify (connect with potential collaborators)
  - We are available if you are using C2E2 / DryVR
- Target venues: CAV, HSCC, TACAS, VMCAI
  - FMSD, IEEE TAC, ACM TECS, ACM CPS

Reach-avoid problem: a general class of synthesis problem

- Denote $\xi(x_0, u, a, t)$ as the state visited at time t with initial state x_0, control input u and adversary input a

- A reach-avoid problem is specified by a safe set and a goal set. We aim to solve:

Find $u, \forall a$

$$\forall t \leq T. \xi(x_0, u, a, t) \in safe \ \wedge \ \xi(x_0, u, a, T) \in Goal$$