Verified hybrid LQ control for autonomous spacecraft

Nicole Chan and Sayan Mitra
Coordinated Science Laboratory
University of Illinois at Urbana Champaign

Acknowledgements
Dr. R. Scott Erwin, NSF, AFRL

IEEE Conference on Decision and Control
Melbourne, December, 2017

A benchmark problem for verified control

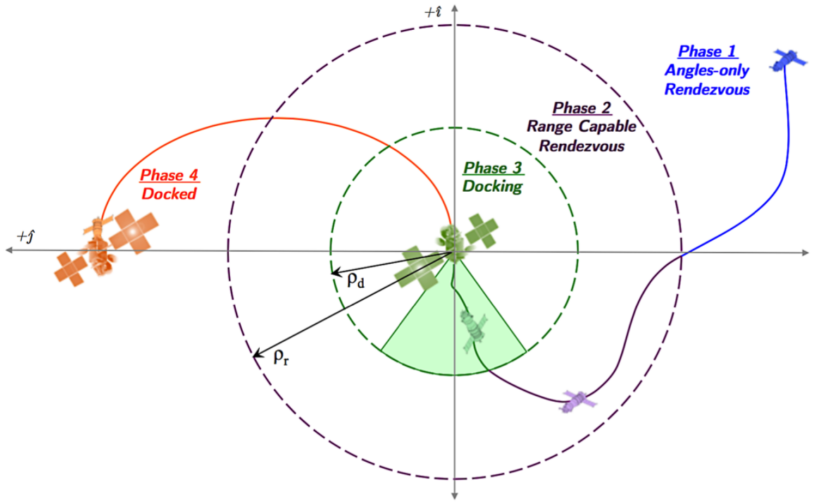
ARPOD problem: Automous rendezvous, proximity operation, and docking for spacecraft

[Jewison and Erwin, CDC 2016]

Hybrid dynamical system

Control design

Automatic safety verification



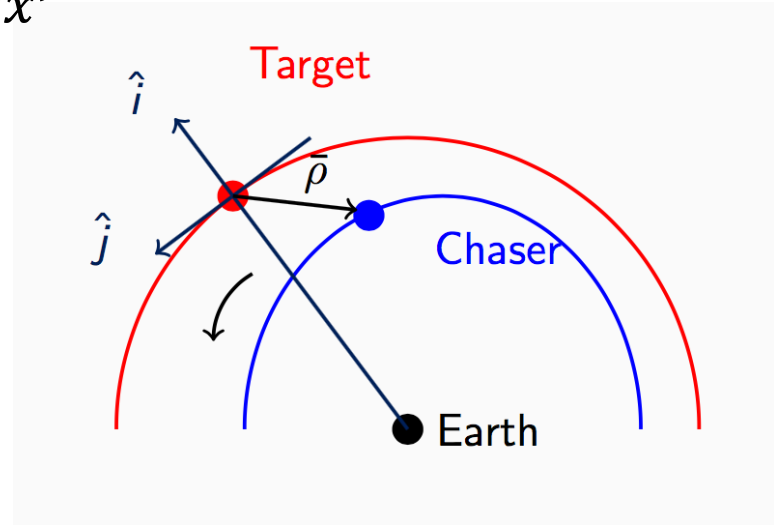
Plant model

State vector: $\bar{x} = [x, y, \dot{x}, \dot{y}]$

Input vector: $\bar{u} = [F_x, F_y]$

Separation: $\rho = \sqrt{x^2 + y^2}$

Angle of approach: $\theta = \arctan(\frac{y}{x})$



non-inertial relative coordinate frame with target located at the origin.

Underlying plant dynamics

Nonlinear

Derived from Kepler's laws and two-body problem

$$\ddot{x} = n^2 x + 2n\dot{y} + \frac{\mu}{r^2} - \frac{\mu}{r_c^3}(r + x) + \frac{F_x}{m_c}$$

$$\ddot{y} = n^2 y - 2n\dot{x} - \frac{\mu}{r_c^3} y + \frac{F_y}{m_c}$$

$r_c = \sqrt{(r + x)^2 + y^2}$, $n = \sqrt{\frac{\mu}{r^3}}$, μ, r, m_c are given constants

Linear

Clohessy-Wiltshire-Hill (CWH) equations

$$\ddot{x} = n^2 x + 2n\dot{y} + \frac{F_x}{m_c}$$

$$\ddot{y} = -2n\dot{x} + \frac{F_y}{m_c}$$

$$\dot{\bar{x}} = A\bar{x} + B\bar{u} = (A - BK)\bar{x}$$

Modes in hybrid dynamics

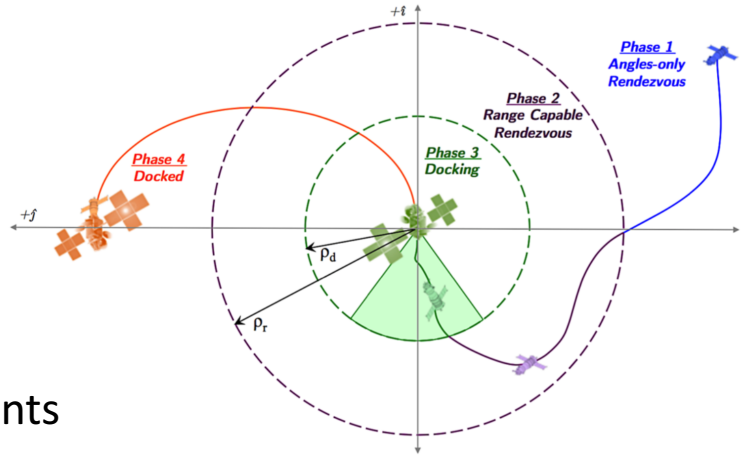
Phase 1: Only measure θ and not ρ; system is not observable. (not in paper)

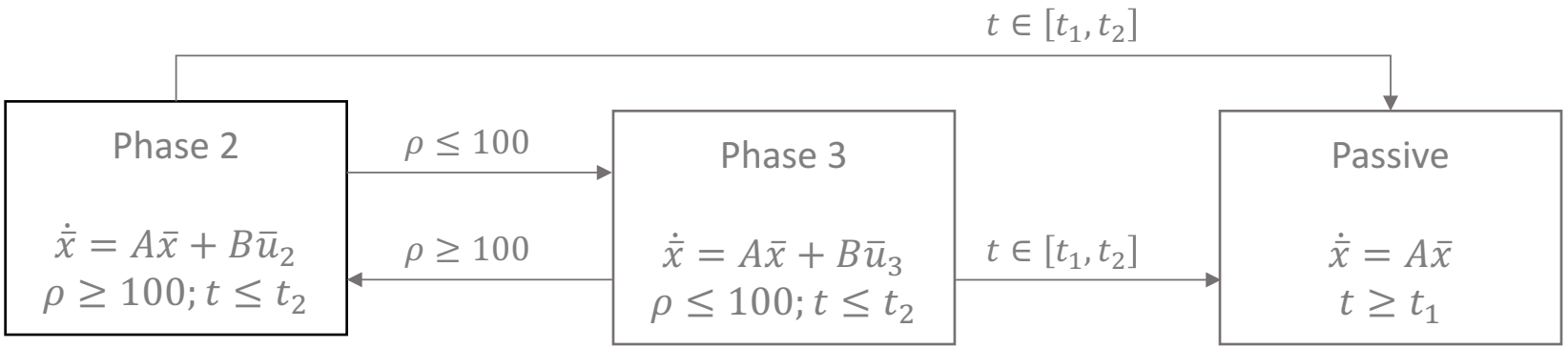
Phase 2: Chaser rendezvous with target without constraint.

Phase 3: Chaser continues rendezvous with constraints on its path and velocity, target location.

Phase 4: Plant mass changes and the terminal constraint is a new location. (not in this paper)

Abort/passive: Chaser shuts off its thrusters if a failure is detected





Safety constraints

Max thrust

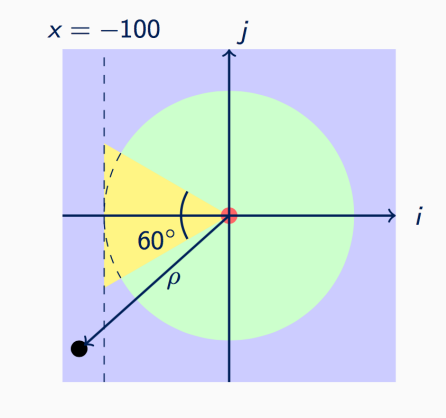
$$|F_x|, |F_y| \leq 10N$$

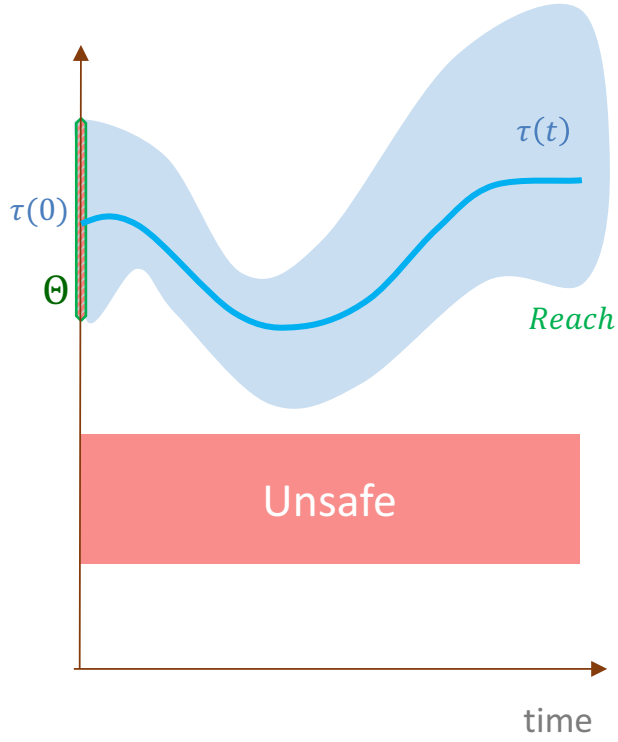
Closing velocity

$$\sqrt{\dot{x}^2 + \dot{y}^2} \leq 5cm/sec$$

Line of sight

$$\theta \in [-\frac{7\pi}{6}, -\frac{5\pi}{6}]$$





Problem: Design a controller for ARPOD and verify that all reachable states (from a set of initial states (Θ) and given set of disturbance inputs) meet these constraints.

Control and verification strategies

MPC-based controller using ellipsoidal constraints

[Jewison, Erwin, and Saenz-Otero 2015]

Optimal control using Reach-Avoid set computation

[Oishi et al. CDC 2016]

Hybrid supervisory control

[Malladi, Sanfelice, Butcher, and Wang, 2016-2017]

Trajectory planning using MPC (Phase 2) and differential flatness (Phase 1) [Farahani, Papusha, McGhan, and Murray]

Optimal control policy via stochastic reachability analysis

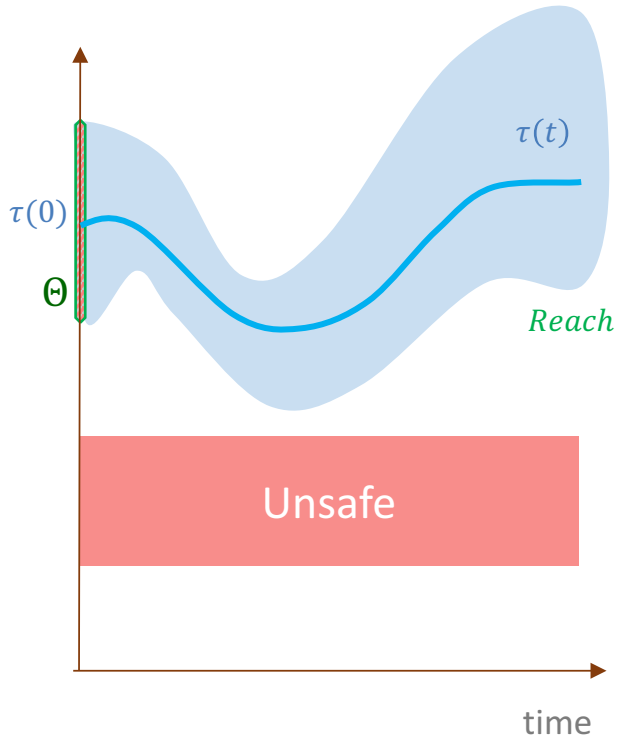
[Poonawala and Topcu, CDC 2016]

State-dependent LQ (SDLQ) and verification

[Chan and Mitra, 2016-17]

Simulation-driven bounded verification

Safety problem: given initial set Θ and unsafe set U, decide $Reach \cap U = \emptyset$?



Controller Design: SDLQ

$$\dot{\bar{x}} = A\bar{x} + B\bar{u} \; = (A - \; BK_i)\bar{x}$$

- Extend LQR to multiple stages; gives flexibility to handle local constraints

- Weights Q(·), R(·) of the quadratic cost are functions of the sampled state $\bar{x}(t)$; at ith period K_i is computed as:

$$\min_{\bar{u}} \int_0^{\infty} \bar{x}^T Q\big(\bar{x}(t_i)\big)\bar{x} + \bar{u}^T R\big(\bar{x}(t_i)\big)\bar{u}]dt$$

- Solution $K_i \; = \; R^{-1}B^T P_i$, where P_i is solution to algebraic Riccati equation

- **Challenge:** Simulations behave correctly, but analytical solution not available (needed for previous verification approaches)

Simulation-driven bounded verification

Simulation-driven verification for a single mode v

1. simulate → 2. check safety → 3. refine

Discrepancy β bounds distance between neighboring trajectories $\|\tau_1(t) - \tau_2(t)\| \leq \beta(\tau_1(0), \tau_2(0), t)$,

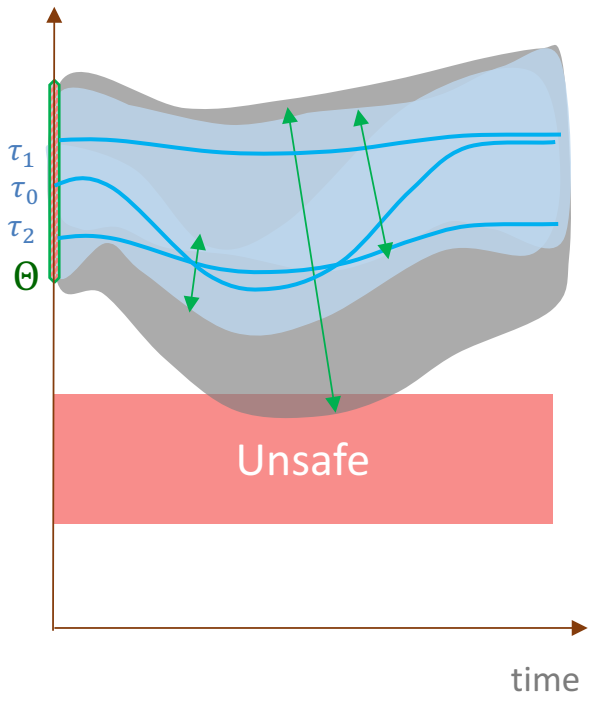
From a single simulation $\tau_1(t)$ + β over-approximate reach set from neighborhood of $\tau_1(0)$

Earlier approaches use $f(x), \frac{\partial f(x)}{\partial x}$

[C2E2: Duggirala et al. TACAS 15, Fan et al. CAV 15-16]

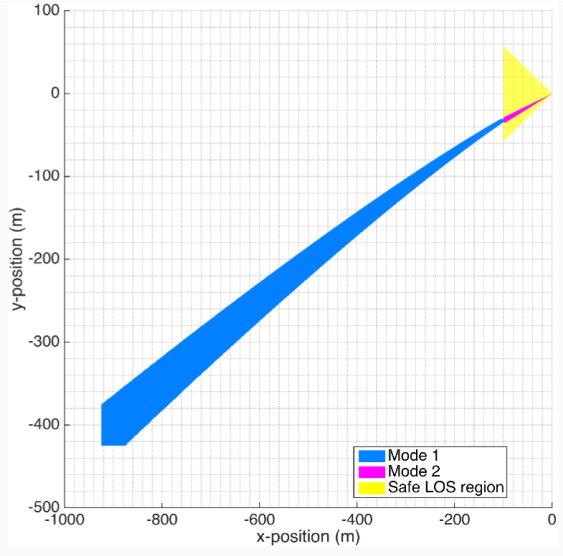
For LQR, closed-loop system admits analytical solution, sensitivity analysis, and verification with existing algorithms (tools like SpaceEx and C2E2)

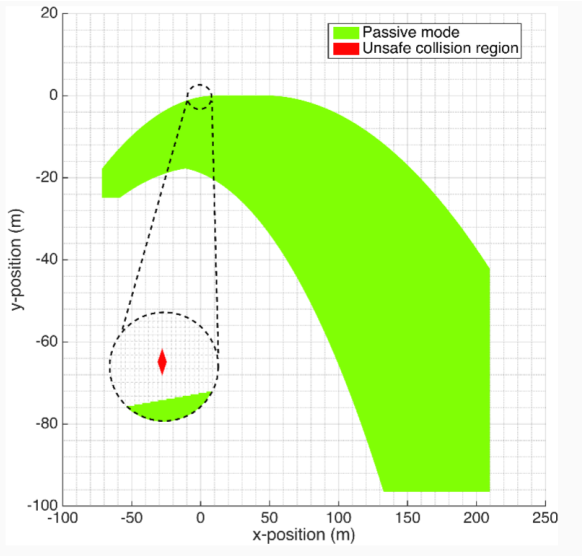
[Chan and Mitra, ARCH 2017]



Reachability analysis for LQ controller

Algorithm	Linear with passive	Linear w/o passive	Nonlinear w/o passive
SDVTool [1]	Safe	Safe	n/v
SpaceEx [2]	Safe	Safe	n/v
C2E2 [3]	n/v	Safe	Safe



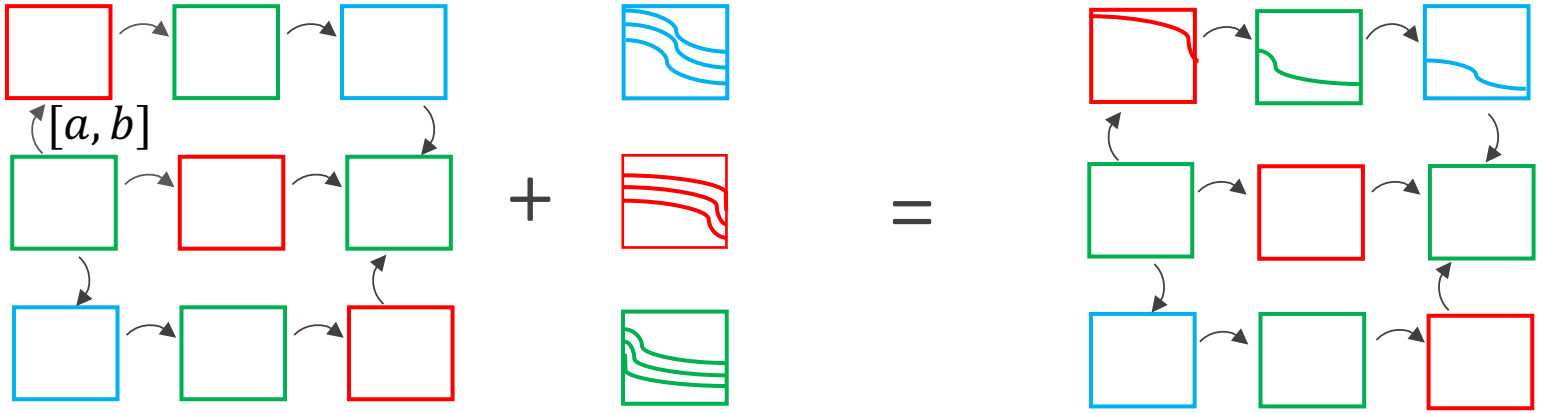


[2] *Frehse, et al.* http://spaceex.imag.fr/

[3] *Duggirala, et al.* http://publish.illinois.edu/c2e2-tool/

[1] *Chan and Mitra*, MATLAB implementation of C2E2 algorithm

DryVR: A new view of hybrid verification



Transition graph

Trace: $l_1, t_1, l_2, t_2, \ldots, l_k$

Black-box simulator

Trajectory: $\tau(t)$

Labeled trajectory set: $\langle \tau, l \rangle \in \mathcal{TL}$

Hybrid system $\mathcal{H} = \langle \mathcal{L}, \Theta, G, \mathcal{TL} \rangle$

State: a point in $\mathbb{R}^n \times \mathcal{L}$

$Reach = \{\langle x, l \rangle |$ for some $v, t, \langle x, l \rangle$ is reachable from $\Theta\}$

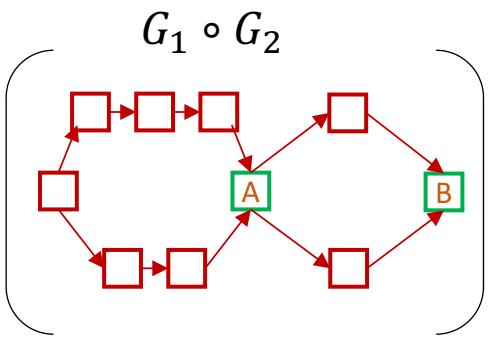
$Reach|v$: all states reachable in vertex v

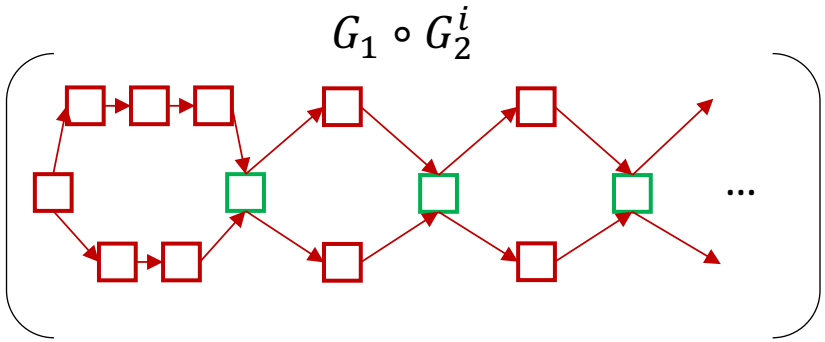
[Fan, Qi, Mitra, and Viswanathan, CAV 2017]

[DryVR: http://dryvr.readthedocs.io/en/latest/index.html#]

Composition for unbounded time analysis

If $Reach|B \subseteq Reach|A$ then

$Reach$ 

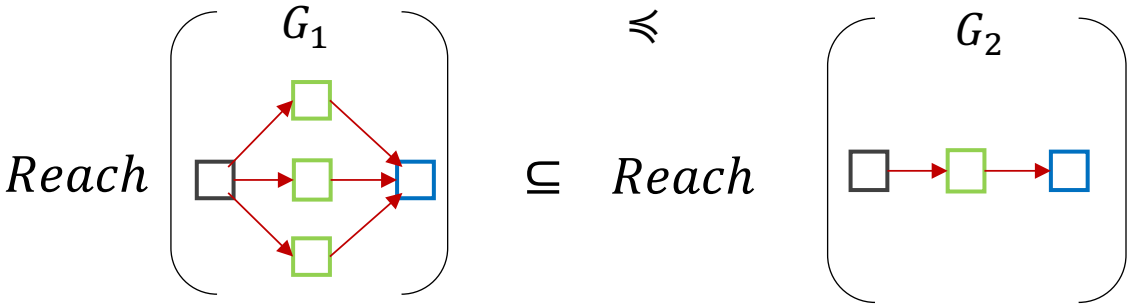
$\supseteq Reach$ 

Reasoning about behavior containment

Trace containment $G_1 \preccurlyeq G_2$

Trajectory containment $\mathcal{TL}_1 \preccurlyeq \mathcal{TL}_2$

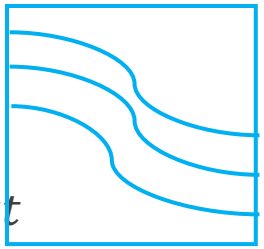
If $\Theta_1 \subseteq \Theta_2, G_1 \preccurlyeq G_2, \mathcal{TL}_1 \preccurlyeq \mathcal{TL}_2$, then



Learning discrepancy from data

Global exponential discrepancy function

$$\beta(x_1, x_2, t) = |x_1 - x_2| K e^{\gamma t}$$



For any pair of trajectories τ_1 and τ_2 in mode $\square$

$$\forall t \in [0, T], |\tau_1(t) - \tau_2(t)| \leq |\tau_1(0) - \tau_2(0)| K e^{\gamma t}$$

Taking logarithm and rearrange:

$$\forall t, \ln \frac{|\tau_1(t) - \tau_2(t)|}{|\tau_1(0) - \tau_2(0)|} \leq \gamma t + \ln K$$

Learning linear separators

For S $\subseteq \mathbb{R}\times\mathbb{R}$, a linear separator is a pair $(a, b) \in \mathbb{R}^2$ s.t. $\forall (x, y) \in S, x \leq ay + b$

Algorithm:

1. Draw k pairs $(x_1, y_1), \ldots, (x_k, y_k)$ from S according to $\mathcal{D}$.

2. Find $(a, b) \in \mathbb{R}^2$ such that $x_i \leq ay_i + b$ for all $i \in \{1, \ldots, k\}$.

Proposition [Valiant 84]: Let $\epsilon, \delta \in \mathbb{R}^+$. If $k \geq \frac{1}{\epsilon} \ln \frac{1}{\delta}$ then with probability $1 - \delta$, the above algorithm finds (a, b) such that $err_{\mathcal{D}}(a, b) < \epsilon$;

$$err_{\mathcal{D}}(a, b) = \mathcal{D}(\{(x, y) \in S \mid x > ay + b\})$$

Solve LP: $\min\ 2c \ln K + c(c+1)\gamma T$

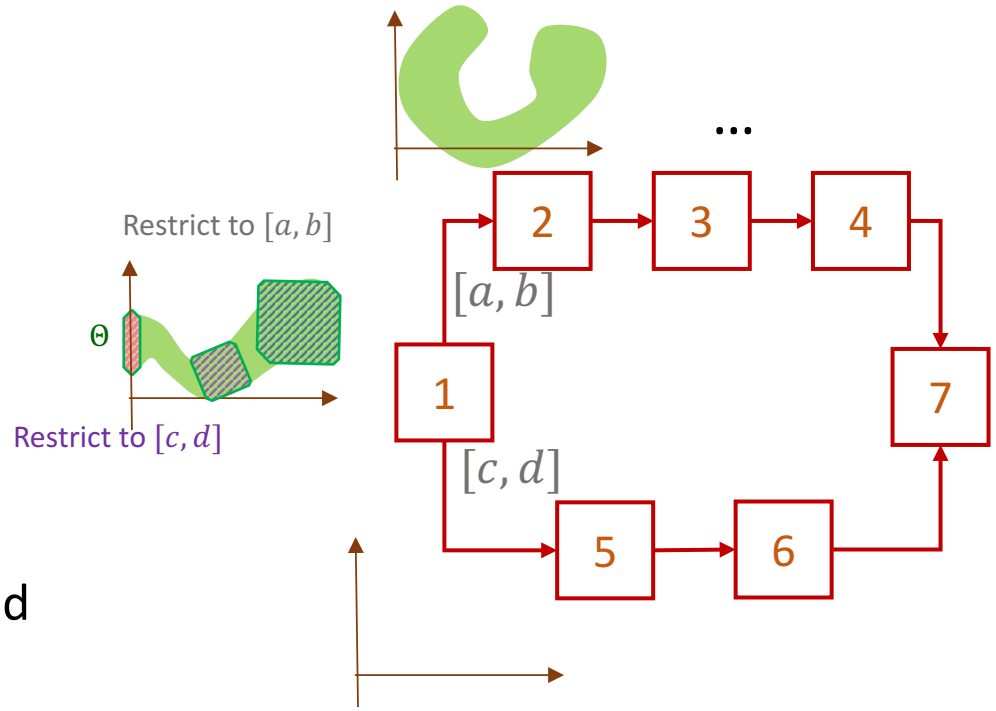
s.t. $\forall i, j, s, \ln \frac{|\tau_i(t_s) - \tau_j(t_s)|}{|\tau_i(0) - \tau_j(0)|} \leq \gamma t_s + \ln K$

Bounded safety algorithm

Compute reach set from Θ: proceeds on G in a topologically sorted order

Refinement

- Split Θ to smaller sets
- Split transition time intervals



Guarantee: Assuming that the learned discrepancy function is correct:

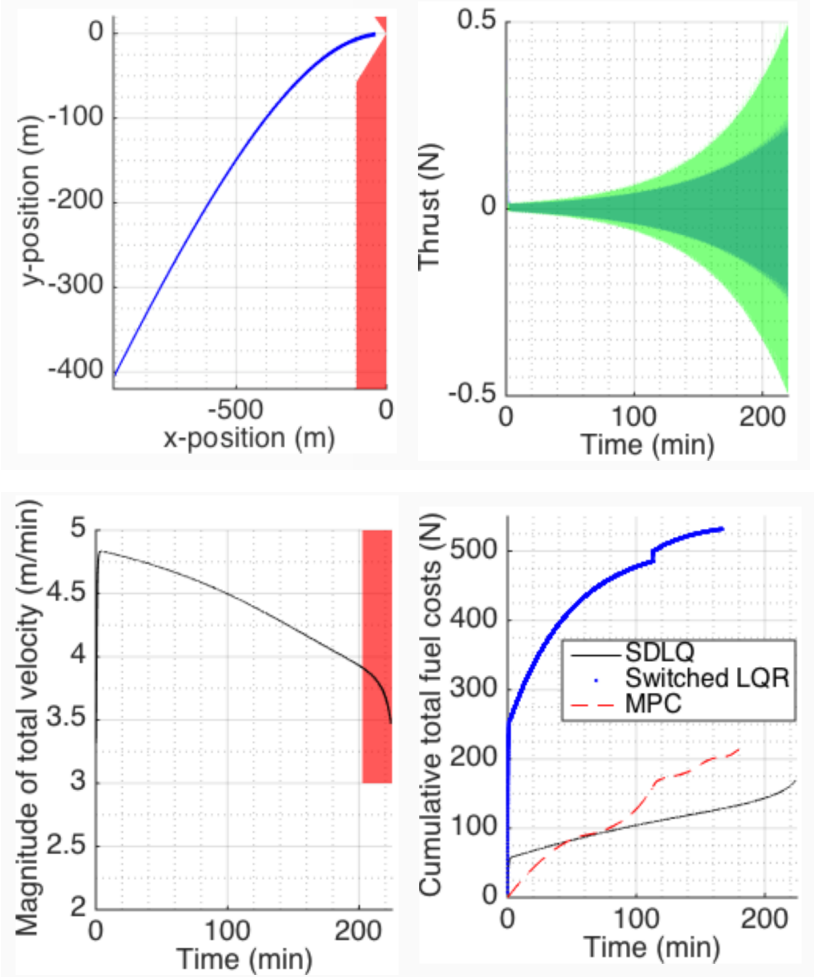
- Soundness
- Relative completeness

Conclusions

DryVR proves safety for Thrust and LOS constraints and a counterexample (unsafe) for Total Velocity constraint.

Simulation-driven verification, promising approach for grey-box models (try it)

Design and verification for complete ARPOD (with disturbance inputs)



Reachable positions (blue) and unsafe positions (red). (b) Reachable thrusts: Fx (blue) and Fy (green).

Composition for unbounded time analysis

If $Reach|B \subseteq Reach|A$ then