Safety-Preserving Control of High-Dimensional Continuous-Time Uncertain Linear Systems

Shahab Kaynama
Electrical Engineering & Computer Sciences, UC Berkeley
Jointly with Ian M. Mitchell (UBC), Meeko Oishi (UNM), Guy A. Dumont (UBC)

Motivation
- Presence of hard input and state constraints
- Particularly important with unknown (but bounded) disturbances/uncertainties
- Goal: Design a scalable permissive feedback controller that maintains feasibility/safety

Background
- \( x = (x, u, v), u(t) \in U, v(t) \in V, x(t) \in X, T \in T \subseteq [0, 1] \)
- Discriminating kernel
  \[ \text{Discr}(K(t, t'), V, X) = \{ s \in X \ | \ y(t) \in Y \} \]
  \[ \text{Reach}(K(t, t'), V, X) = \left\{ s \in X \ | \ y(t) \in Y \right\} \]
- Feedback strategy for control: \( u(t) = \bar{u}(x, t) \in U \)
- When \( K \) is deemed safe, \( u(t) \) is safety-preserving

Conventional Approaches
- Synthesize safety-preserving controllers based on the shape of the kernel
  - Contingent cones and proximal normals (per Naugman's theorem)
  - Terminal constraint set for Receding Horizon Control
- Numerical solutions to compute the kernel
  - Eulerian methods, e.g. level-set techniques, Saint-Pierre's algorithm: grid-based
  - Recursive methods for DT LTI systems with polytopic constraints, e.g. Blanchard's algorithm: explosion of vertices
- A control Lyapunov function sublevel-set for CT systems: possibly too conservative

Discriminating Kernel Approximation (Offline)
Approximate \( \text{Discr}(K(t, t'), V, X) \) via a nested sequence of sets robustly reachable in small sub-intervals of \( T \): \( \text{Reach}(K(t, t'), V, X) = \{ s \in X \ | \ y(t) \in Y \} \)

Piecewise Ellipsoidal Algorithm (Offline)
- Based on the ellipsoidal techniques for maximal reachability (LTL) [Shahab and Vidyasagar 10]
- For fixed terminal direction \( \ell_k \) and partition \( P \) with \( K_{\ell_k}(P, V) = K_{\ell_k}(P) \), do
  \[ K_{\ell_k}(P) = \text{maxvol} \left\{ K_{\ell_k}(P) \cap \text{Reach}(K(t, t'), \{K_{\ell_k}(P), U, Y\}) \right\} \]
- Generates an ellipsoidal set \( K_{\ell_k}(P) \) such that \( \cup_{k \in M} K_{\ell_k}(P) \subseteq \text{Discr}(K(t, t'), V, X) \)
- Allows partitioning with higher accuracy loss (empirically)
- Computational complexity \( \approx O(n^3) \) (ellipsoidal reach & SDP)

Smoothing Modification
- Safety and performance control laws may be conflicting: pathological behavior
- One solution: with \( \phi^{\beta} \) a measure of how deep inside ellipsoid \( y \),
  \[ u(t)^* = \left\{ 1 - \beta(\phi^{\beta}(x(t), y(t))) \right\} u_{mp}(t)^* + \beta(\phi^{\beta}(x(t), y(t)))u_{saf}(t)^* \]
- Benefit: If (t) is continuous across the automaton's transitions
  -When disturbance plays optimally (with inexact arithmetic)
    - Unmodified policy: Chattering in HA and \( u \) chatters
    - Modified policy: HA is likely to chatter, \( u \) does not chatter
  - When disturbance allowed to play non-optimally
    - Unmodified policy: Chattering in HA and \( u \) chatters
    - Modified policy: Neither HA nor \( u \) chatters

Application: 12D Quadrotor
- 12D model [Cao et al. 12]: Linearized about hover
  \[ x = [x, y, z, \dot{x}, \dot{y}, \dot{z}, \phi, \theta, \psi, \dot{\phi}, \dot{\theta}, \dot{\psi}]^T \]
- Control \( u = [u_1, u_2, u_3]^T \in [0.5, 5.4] \)
- Disturbance is wind: unknown but bounded (\( v \sim \text{uniform}(0, 0.1) \) in simulations)
- Physical constraints: Also, keep 1–2 m above ground for at least 2 s
- Performance: LQR (saturated) to move to \( x_{des} = [0 0 5 0 0 0 0 0 0 0 0 0] \)

Case 1: No safety controls; (Saturated) LQR, Failed at 1.8 s

Case 2: Safety control with (saturated) LQR in \( u^* \); Can extent up to 4.5 s

Further Readings