# An Improved Algorithm for Robust Safety Analysis of Sampled Data Systems

## Now Robust to Sample Time Jitter!

Ian M. Mitchell[1] & Shahab Kaynama[1,2]

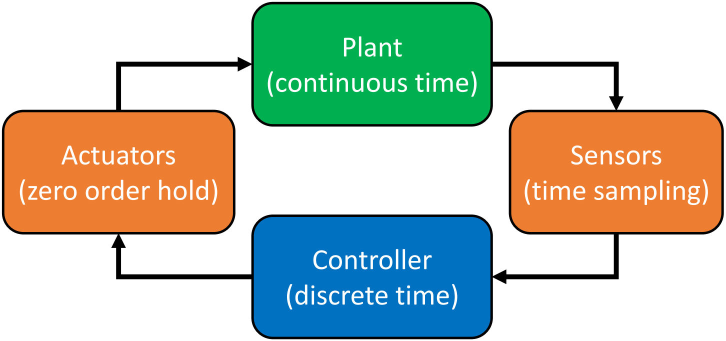
[1]Department of Computer Science, University of British Columbia
[2]Department of Electrical Engineering & Computer Science, University of California Berkeley

April 2015

mitchell@cs.ubc.ca
http://www.cs.ubc.ca/~mitchell

# A Common Design Pattern

*Sampled data* is a model of a common approach to designing cyber-physical systems:



- Unlike continuous time models, change to feedback control is only possible at sample times.
- Unlike discrete time models, state of plant between sample times is relevant.

# Outline

1. Background & Contributions
2. Model, Problem and Construct Definitions
3. Improved Algorithm
4. Analyzing the Improvement
5. Examples

# Outline

1. Background & Contributions

2. Model, Problem and Construct Definitions

3. Improved Algorithm

4. Analyzing the Improvement

5. Examples

# Prevous Work

Safety verification and safe controller synthesis for sampled data systems:

- In [Ding & Tomlin, CDC 2010]:
  - Reach-avoid tube.
  - Formulation based on Hamilton-Jacobi (HJ) partial differential equation (PDE)
- In [Mitchell, Chen & Oishi, ADHS 2012]:
  - Minimal reach tubes (no disturbance input).
  - State space partition into free and constrained control sets.
  - Permissive set-valued control policy.
  - Formulation based on HJ PDE.
- In [Mitchell, Kaynama, Chen & Oishi, NAHS 2013]:
  - Discriminating kernels.
  - State space partition into free and constrained control sets.
  - Permissive set-valued control policy.
  - Formulation based on abstract viability / reachability operators.
  - Ellipsoidal and HJ PDE implementations.

All versions assumed fixed sample period.

# Other Related Work

- Much work on traditional control objectives for sampled data systems; for example [Goodwin et al, IEEE Control Systems Magazine 2013], [Monaco & Normand-Cyrot, Euro. J. Control 2007], [Nešić & Teel, IEEE TAC 2004].
- In [Tsuchie & Ushio, ADHS 2006]: Controller determines switches, more restrictive (but more realistic?) class of jitter, require trajectory solutions.
- In [Karafylllis & Kravaris, Int. J. Control 2009]: Define $r$-robust reachability, but requires Lyapunov-like function.
- In [Simko & Jackson, HSCC 2014]: Taylor models and SMT solver, but only initial state is nondeterministic.
- In [Gillula, Kaynama & Tomlin, HSCC 2014]: Sampled data viability kernel (no disturbance input) with polytopic set representation.
- In [Aréchiga & Krogh, ACC 2014]: theorem prover to verify (and synthesize?) invariants and control envelopes robust to parameter variations including sample time uncertainty.
- In [Dabadie, Kaynama & Tomlin, IROS 2014]: robust reach set is complement of (jitter-free) discriminating kernel.

# Goal and Contributions

For a sampled data model, construct a permissive, set-valued control policy such that system trajectories remain within a constraint set over bounded time horizon despite disturbance input and sample time jitter.

Contributions

- Modification of algorithm from [Mitchell et al, 2013].
- Proof that algorithm is tight for systems with no jitter.
- Proof that algorithm is robust to jitter.
- Example application of algorithm to nonlinear model of quadrotor height maintenance.
- Experimental evidence that algorithm is more accurate and faster.

Results can be extended to hybrid systems with mode switches at sample times. Other types of mode switching are challenging.

# Outline

1. Background & Contributions

2. Model, Problem and Construct Definitions

3. Improved Algorithm

4. Analyzing the Improvement

5. Examples

# Sampled Data Systems

Consider a nondeterministic nonlinear system

$$\dot{x} = f(x, u, v) \text{ with } x(0) = x_0$$

We make typical assumptions:

- State $x \in \Omega \subset \mathbb{R}^{d_x}$.
- Control input $u \in \mathcal{U}$.
- Disturbance input $v \in \mathcal{V}$.
- Input sets $\mathcal{U} \subset \mathbb{R}^{d_u}$ and $\mathcal{V} \subset \mathbb{R}^{d_v}$ compact and convex.
- $f$ is Lipschitz continuous in $x$ and continuous in $u$ and $v$.
- Disturbance signal $v(\cdot)$ must be measurable and will use non-anticipative strategies (includes open loop and state feedback).

Consequently, trajectories $x(\cdot)$ exist and are unique.

# Jittery Sample Times

State is sampled and control input is chosen at times $t_k$ in sample time sequence $\mathcal{T} = \{t_k\}_{k=0}^{N}$

- Sample period divided into fixed and jitter components:

$$t_{k+1} - t_k = \delta^{\mathsf{F}} + \delta^{\mathsf{J}}_k$$

where $\delta^{\mathsf{F}} \geq 0$ and $\delta^{\mathsf{J}}_k \in [0, \delta^{\mathsf{J}}]$ for some fixed $\delta^{\mathsf{J}} \geq 0$.

Control is piecewise constant in time

$$u_{\mathsf{pw}}(t) = u_{\mathsf{fb}}(x(t_k)) \text{ for } t_k \leq t < t_{k+1}$$

where $u_{\mathsf{fb}} : \Omega \rightarrow \mathcal{U}$ is a feedback control policy

- Feedback policy does not know $\mathcal{T}$.
- Resulting dynamics $\dot{x}(t) = f(x(t), u_{\mathsf{pw}}(t), v(t))$ are time-dependent for a given state $x$ (eg: they cannot be written $\dot{x} = \hat{f}(x, v)$).

# Problem Definition and Basic Approach

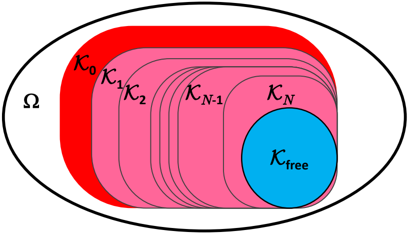
Given constraint set $\mathcal{K}_0 \subset \Omega$, times $\delta^{\mathsf{F}}$, $\delta^{\mathsf{J}}$ and horizon $T$.

- Find subset of $\Omega$ and (set-valued) control policy such that $x(t) \in \mathcal{K}_0$ for all $t \in [0, T]$.
- Solution must be robust to disturbance input $v(\cdot)$ and sample time jitter $\delta^{\mathsf{J}}_k$.

Divide $\Omega$ into nested sets:

- Constraint $\mathcal{K}_0$.
- Finite horizon safe sets $\mathcal{K}_k$.
- Free control set $\mathcal{K}_{\text{free}}$.

Control is constrained within $\mathcal{K}_k$. Safety can be ensured for $k$ sample periods.



More details on $\mathcal{K}_{\text{free}}$ in [Mitchell et al, 2013].

# Construct: Augmented State Space

We will often work in an augmented state space

$$\tilde{x} \triangleq \begin{bmatrix} x \\ u \end{bmatrix} \in \tilde{\Omega} \triangleq \Omega \times \mathbb{R}^{d_u}$$

with dynamics

$$\frac{d}{dt}\tilde{x} = \frac{d}{dt}\begin{bmatrix} x \\ u \end{bmatrix} = \begin{bmatrix} f(x,u,v) \\ 0 \end{bmatrix} \triangleq \tilde{f}(\tilde{x}, v).$$

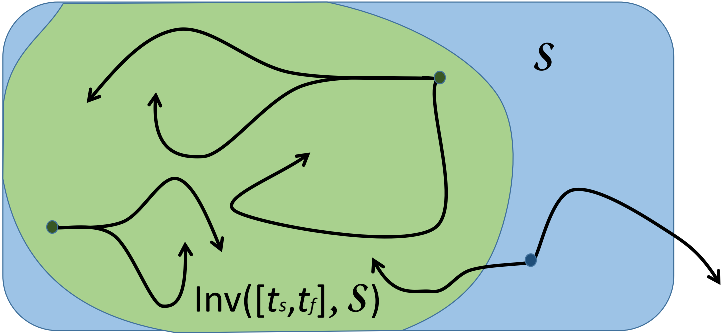
Define two projection operators for $\tilde{\mathcal{X}} \subseteq \tilde{\Omega}$ and $x \in \Omega$:

$$\begin{aligned} \mathsf{Proj}_x\left(\tilde{\mathcal{X}}\right) &\triangleq \left\{ x \in \Omega \,\middle|\, \exists u, \begin{bmatrix} x \\ u \end{bmatrix} \in \tilde{\mathcal{X}} \right\}, \\ \mathsf{Proj}_u\left(\tilde{\mathcal{X}}, x\right) &\triangleq \left\{ u \in \mathcal{U} \,\middle|\, \begin{bmatrix} x \\ u \end{bmatrix} \in \tilde{\mathcal{X}} \right\}, \end{aligned}$$

Both projections can easily be applied to implicit surface function (HJ PDE formulation) and ellipsoid set representations.

# Construct: Invariance Kernel

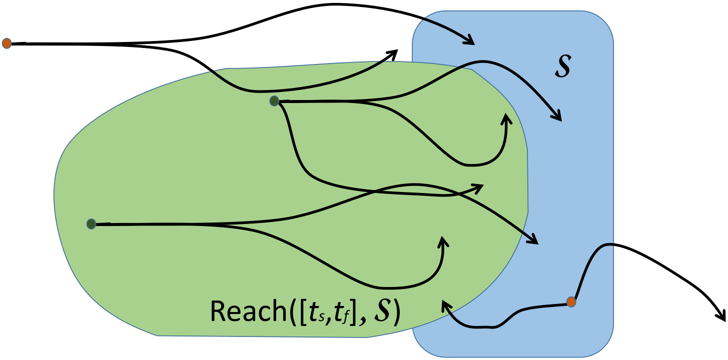
$$\mathsf{Inv}\left([t_s, t_f], \mathcal{S}\right) \triangleq \{\tilde{x}(t_s) \in \mathcal{S} \mid \forall v(\cdot), \forall t \in [t_s, t_f], x(t) \in \mathcal{S}\},$$



- Straightforward HJ PDE approximation.
- Ellipsoidal approximation based on recursive reach sets followed by intersections [Kaynama et al, HSCC 2012].

# Construct: Robust Reach Set

$$\text{Reach}\left([t_s, t_f], \mathcal{S}\right) \triangleq \{\tilde{x}(t_s) \in \tilde{\Omega} \mid \forall v(\cdot), \tilde{x}(t_f) \in \mathcal{S}\}$$



- Straightforward HJ PDE approximation.
- Straightforward ellipsoidal approximation.

# Goal: Jitter Robust Sampled Data Discriminating Kernel

$$\mathsf{Disc}_{\mathsf{sd}}\left([0,T],\mathcal{S}\right) \triangleq \left\{ x_0 \in \mathcal{S} \;\middle|\; \begin{array}{c} \exists u_{\mathsf{pw}}(\cdot), \forall \mathcal{T}, \forall v(\cdot), \\ \forall t \in [0,T], x(t) \in \mathcal{S} \end{array} \right\},$$

*That is hard to draw. . .*

Define the maximum number of sample periods in the chosen horizon:

$$\bar{N} \triangleq \left\lceil \frac{T}{\delta^{\mathsf{F}}} \right\rceil$$

# Outline

1. Background & Contributions
2. Model, Problem and Construct Definitions
3. Improved Algorithm
4. Analyzing the Improvement
5. Examples

# Working Sets

Sets of states and constant control values such that (no matter what the disturbance $v(\cdot)$) the trajectories will:

- Stay within $\mathcal{S}$ for $\delta^{\mathsf{F}} + \delta^{\mathsf{J}}$ time:

$$\mathcal{I}_1 \triangleq \mathsf{Inv}\left([0, \delta^{\mathsf{F}} + \delta^{\mathsf{J}}], \mathcal{S} \times \mathcal{U}\right).$$

- Be in $\mathsf{Disc}_{j-1}(\mathcal{S})$ in exactly $\delta^{\mathsf{F}}$ time:

$$\mathcal{R}_j \triangleq \mathsf{Reach}\left([0, \delta^{\mathsf{F}}], \mathsf{Disc}_{j-1}(\mathcal{S}) \times \mathcal{U}\right), \qquad \text{for } j = 2, 3, \ldots, \bar{N}.$$

- Be in $\mathsf{Disc}_{j-1}(\mathcal{S})$ during the time interval $[\delta^{\mathsf{F}}, \delta^{\mathsf{F}} + \delta^{\mathsf{J}}]$:

$$\mathcal{I}_j \triangleq \mathsf{Inv}\left([0, \delta^{\mathsf{J}}], \mathcal{R}_j\right) \qquad \text{for } j = 2, 3, \ldots, \bar{N}.$$

Also define

$$\widehat{\mathcal{I}}_j \triangleq \mathcal{I}_j \cap \mathcal{I}_1; \qquad \mathsf{Disc}_j(\mathcal{S}) \triangleq \mathsf{Proj}_x\left(\widehat{\mathcal{I}}_j\right)$$

for $j = 1, 2, \ldots, \bar{N}$.

# Problem Solution

Approximation of the finite horizon safe sets:

$$\mathcal{K}_j = \mathsf{Disc}_j\left(\mathcal{K}_0\right).$$

Using these sets, we can define a set-valued control signal:

- For $x \in \mathcal{K}_0$, define the safety horizon of $x$ as

$$n(x) \triangleq \begin{cases} \bar{N}, & \text{if } x \in \mathcal{K}_{\bar{N}}; \\ j, & \text{if } x \in \mathcal{K}_j \setminus \mathcal{K}_{j+1}; \end{cases}$$

  for $j = \bar{N} - 1, \bar{N} - 2, \ldots, 0$.

- Control policy:

$$\mathcal{U}_{\mathsf{ctrl}}(x) \triangleq \mathsf{Proj}_u\left(\widehat{\mathcal{I}}_{n(x)}, x\right)$$

- By construction, applying $u \in \mathcal{U}_{\mathsf{ctrl}}(x(t_k))$ ensures that $x(t_{k+1}) \in \mathcal{K}_{n(x(t_k))-1}$.

# Outline

1. Background & Contributions
2. Model, Problem and Construct Definitions
3. Improved Algorithm
4. Analyzing the Improvement
5. Examples

# Old Algorithm was Jitter Robust!

- Original algorithm [Mitchell et al, 2013] was designed for fixed sample periods: $\delta^{\mathsf{F}} = \delta$ and $\delta^{\mathsf{J}} = 0$.
- Translated into this notation, it used

$$\mathcal{I}_j \triangleq \mathsf{Inv}\left([0, \delta], \mathsf{Disc}_{j-1}\left(\mathcal{S}\right) \times \mathcal{U}\right)$$

  (there was no $\mathcal{R}_j$).
- In other words, it was robust to the case $\delta^{\mathsf{F}} = 0$ and $\delta^{\mathsf{J}} = \delta$.

Not surprising that the results were conservative.

# The Theory

- Proposition: Algorithm is conservative for systems with sample time jitter ($\delta^{\mathsf{J}} \geq 0$):

$$\mathsf{Disc}_{\bar{N}}\left(\mathcal{S}\right) \subseteq \mathsf{Disc}_{\mathsf{sd}}\left([0,T],\mathcal{S}\right).$$

- Proposition: Algorithm is tight for fixed sample times ($\delta^{\mathsf{J}} = 0$):

$$\mathsf{Disc}_{N}\left(\mathcal{S}\right) = \mathsf{Disc}_{\mathsf{sd}}\left([0,T],\mathcal{S}\right),$$

  where $N = T/\delta^{\mathsf{F}}$.

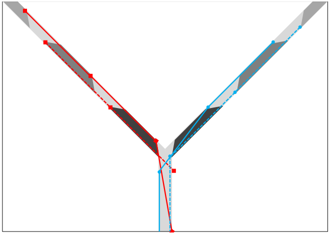
- Theorem: Control policy guarantees safety of $x(\cdot)$ for all $t \in [0, n(x(t))\delta^{\mathsf{F}}]$ despite sample time jitter and action of disturbance input $v(\cdot)$.

# Demonstration of Tightness

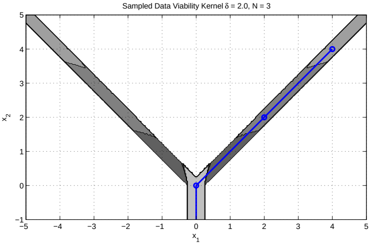
Consider example system from [Mitchell et al, 2013]:

$$f(x,u,v) = \begin{bmatrix} u \\ -1 \end{bmatrix},$$

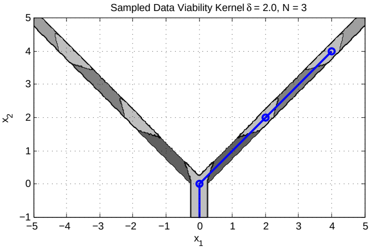
$\mathcal{U} = [-1,+1]$, $\delta^{\mathsf{F}} = 2$, $\delta^{\mathsf{J}} = 0$ and $\mathcal{K}_0$ the Y-shaped shaded region.



True sampled data viability kernel.



Conservative algorithm.



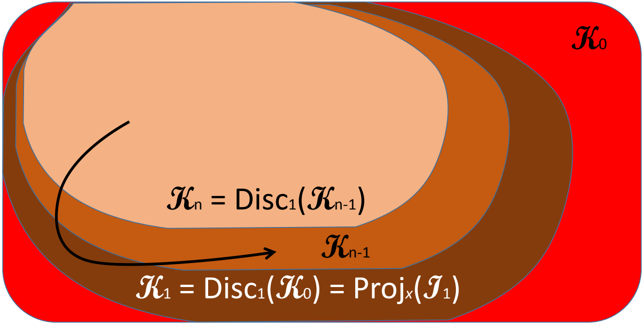
Improved algorithm.

# The Intuition

Difference between old and new algorithms:

- Old algorithm's invariance kernel required $x(t) \in \mathcal{K}_{n(x(t_k))-1}$ for all $t \in [t_k, t_{k+1}]$.
- New algorithm's reach set followed by invariance kernel permits $x(t) \notin \mathcal{K}_{n(x(t_k))-1}$ for $t \in [t_k, t_k + \delta^{\mathsf{F}}]$.
- However, $x(t) \in \mathcal{K}_0$ for all $t \in [t_k, t_{k+1}]$ because

$$\mathcal{K}_{n(x(t_k))} \subseteq \mathsf{Proj}_x\left(\mathcal{I}_1\right) = \mathsf{Proj}_x\left(\mathsf{Inv}\left([0, \delta^{\mathsf{F}} + \delta^{\mathsf{J}}], \mathcal{S} \times \mathcal{U}\right)\right).$$



$\mathscr{K}_0$
$\mathscr{K}_n$ = Disc$_1$($\mathscr{K}_{n-1}$)
$\mathscr{K}_{n-1}$
$\mathscr{K}_1$ = Disc$_1$($\mathscr{K}_0$) = Proj$_x$($\mathscr{I}_1$)

# Outline

1. Background & Contributions
2. Model, Problem and Construct Definitions
3. Improved Algorithm
4. Analyzing the Improvement
5. Examples

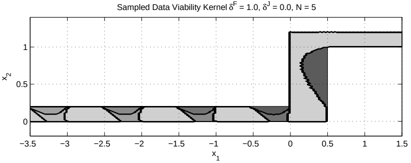
# Toy Example with Time Jitter

Let $f(x,u,v) = u$ with

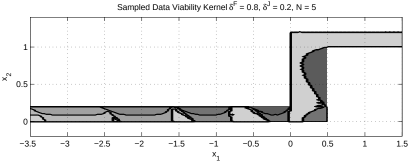
$$u_{\mathsf{up}} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \qquad u_{\mathsf{right}} = \begin{bmatrix} 1 \\ 0 \end{bmatrix};$$

$$\mathcal{U} = \{u \mid u = \lambda u_{\mathsf{up}} + (1-\lambda) u_{\mathsf{right}}\};$$

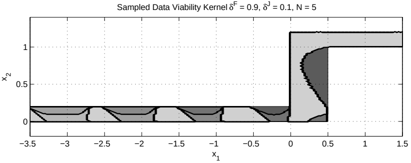
where $0 \leq \lambda \leq 1$.



$\delta^{\mathsf{F}} = 1.0$ and $\delta^{\mathsf{J}} = 0.0$



$\delta^{\mathsf{F}} = 0.8$ and $\delta^{\mathsf{J}} = 0.2$



$\delta^{\mathsf{F}} = 0.9$ and $\delta^{\mathsf{J}} = 0.1$

- Each plot shows $\mathrm{Disc}_j(\mathcal{S})$ for $j = 0, 1, \ldots, 5$ (darkest to lightest).
- Computed using HJ PDE formulation on $\Omega \times \mathcal{U}$ grid $201 \times 161 \times 25$.

# Quadrotor Altitude Maintenance

Nonlinear model from [Akametalu et al, CDC 2014]:

$$\begin{aligned}
\dot{x}_1 &= x_2, && \text{(vertical position)},\\
\dot{x}_2 &= k_T x_3^2 - g, && \text{(vertical velocity)},\\
\dot{x}_3 &= k_p(u - x_3) && \text{(related to thrust)}.
\end{aligned}$$

- Constants $k_p = 6.6667$ and $k_T = 0.1222$ empirically determined.
- State constraints

$$\mathcal{K}_0 = \left\{ x \;\middle|\; \begin{array}{l} x_1 \in [0.5, 2.8], \\ x_2 \in [-1.5, +1.5], \\ x_3 \in [8, 10] \end{array} \right\}$$

- Input constraint $u \in \mathcal{U} = [0, 10]$.
- Fixed sample period $\delta^{\mathsf{F}} = \delta = 0.1$ and $\delta^{\mathsf{J}} = 0$.
- Horizon $T = 1$.

# Linearization with Safety Guarantee

Linearize about hover condition $x_{\mathsf{eq}} = \begin{bmatrix} 2 & 0 & 8.96 \end{bmatrix}^T$ and $u_{\mathsf{eq}} = 8.96$:

$$\dot{x} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 2(8.96)k_T \\ 0 & 0 & -k_p \end{bmatrix} \bar{x} + \begin{bmatrix} 0 \\ 0 \\ k_p \end{bmatrix} \bar{u} + \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} v,$$

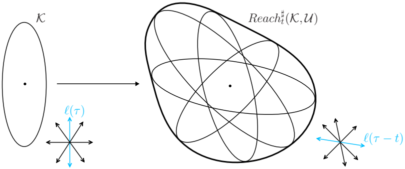
where $\bar{x} = x - x_{\mathsf{eq}}$ and $\bar{u} = u - u_{\mathsf{eq}}$.

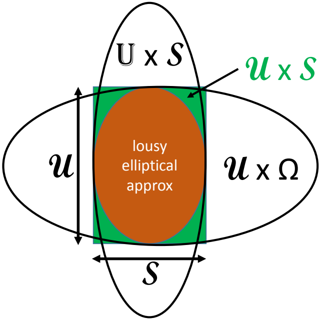
- Choose $\mathcal{V} = [0, 0.1]$ to bound linearization error.
- Constraint on $x_3$ could be loosened at cost of larger $\mathcal{V}$.

# Working with Ellipsoids

Ellipsoids can be efficiently represented, but the class of ellipsoidal sets is:

- Invariant under projection.
- Not invariant under invariance kernels, reach sets, intersection or tensor products.



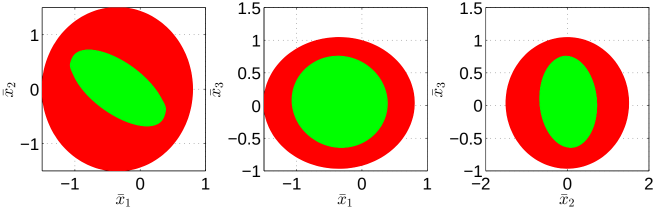


Ellipsoidal underapproximations of the latter operations can be efficiently computed (mostly in Ellipsoidal Toolbox).

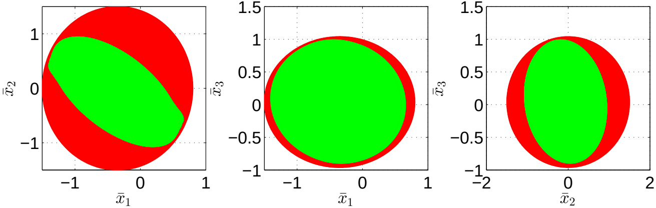
- Tensor product underapproximation is very poor.
- Instead, separately evolve two large ellipsoids and then take the intersection.

# Comparison between Algorithms

Start with ellipsoidal approximations in 20 terminal directions.



Old algorithm (173 min, 13 nonempty terminal directions)

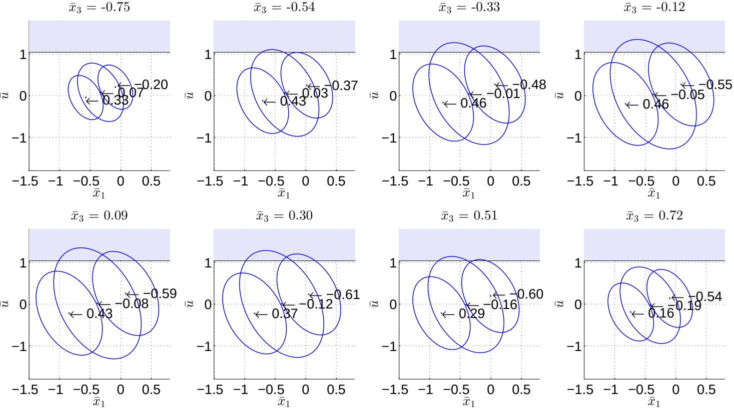


Improved algorithm (5 min, 15 nonempty terminal directions)

Projections of one second finite horizon safe set $\mathcal{K}_1 0$ (green) and state constraint $\mathcal{K}_0$ (red).

# Synthesized Safety Preserving Control Set

Slices of (underapproximation of) safe range of $\bar{u}$ for various $\bar{x}$ using a single terminal direction.



Ellipsoids in each subplot show three slices for $\bar{x}_2$ fixed at the values shown. Values of $\bar{u}$ in the grey region are infeasible.

# Conclusions and Future Work

What we did:

- Described a modified algorithm for approximating the sampled data discriminating kernel.
- Proved result is conservative for systems with sample time jitter.
- Proved result is tight for systems with fixed sample times.
- Demonstrated on a nonlinear quadrotor example that algorithm produces better underapproximations in less time that are usable despite inherent accuracy limits of ellipsoidal representations.

What we plan to do:

- Account for state discretization and uncertainty.
- Allow for separate (jittery) sensing and actuation delays.
- Improved treatment of ellipsoids.
- Hybrid models.
- More examples in higher dimensions.

Research funded by NSERC Discover Grant #298211 (IMM & SK) and NSERC Collaborative Health Research Project #CPG-127770 (SK).