Safety Control Synthesis with Input Limits
A Hybrid Approach

Gray Thomas, Bingham He and Luis Sentis
American Control Conference
June 28, 2018
A system $\Sigma_0 : \dot{x} = f(x) + g(x)u$

- state constraint $x \in \mathcal{X}$
- input constraint $u \in \mathcal{U}$

We develop a controlled safe region $\mathcal{X}_0$ with a backup controller $k(x)$ which provides

- a safety guarantee for all initial states in a region $\mathcal{X}_0 \subseteq \mathcal{X}_s$,
- a close approximation of the exact safe region $\mathcal{X}_s$. 
Hybrid Safety Controller

A hybrid safety controller $K$ in feedback with the original system $\Sigma_0$ produces a safe system $\Sigma_s$.

$\dot{x} = f(x) + g(x)u$

**Hybrid Safety Controller $K$**

- chooses either to be completely transparent ($u = \hat{u}$) or apply the backup controller input $u = k(x)$.
Hybrid Safety Controller

A hybrid safety controller $K$ in feedback with the original system $\Sigma_0$ produces a safe system $\Sigma_s$.

Hybrid Safety Controller $K$

- chooses either to be completely transparent ($u = \hat{u}$) or apply the known-to-be-safe input $u = k(x)$.
- is tuned by two thresholds $\bar{\epsilon}$ and $\epsilon$. 
# Background

<table>
<thead>
<tr>
<th>Verification</th>
<th>Stability</th>
<th>State Limits</th>
<th>Input Limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lyapunov Function, Barrier Certificate</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Synthesis</td>
<td>Stability</td>
<td>State Limits</td>
<td>Input Limits</td>
</tr>
<tr>
<td>Barrier Lyapunov Function</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Control Lyapunov Function</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Control Barrier Function</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Barrier Pair</strong></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

---


Barrier Pair

<table>
<thead>
<tr>
<th>Verification</th>
<th>Stability</th>
<th>State Limits</th>
<th>Input Limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lyapunov Function</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Barrier Certificate</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Synthesis</th>
<th>Stability</th>
<th>State Limits</th>
<th>Input Limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barrier Lyapunov Function</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Control Lyapunov Function</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Control Barrier Function</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Barrier Pair</strong></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

A *Barrier Pair* is a pair of functions \((B, k)\) with two properties:

- \(-1 < B(x) \leq 0, u = k(x) \implies \dot{B}(x) < 0,\)
- \(B(x) \leq 0 \implies x \in \mathcal{X}, \; k(x) \in \mathcal{U}.\)
LMI Sub-problem

Consider a linear differential inclusion \(^5\) (LDI) model which approximates \(\Sigma_0\) near an equilibrium—a robust linearization.

**Constrained Polytopic LDIs**

**Linearized Dynamics**

\[
\dot{x} \in \text{Co}\{A_l(x - x_e) + B_l(u - u_e), \ l = 1, \ldots, L\}.
\]

**Region of Validity**

\[
\forall \ x \in \{x : |a_i^T(x - x_e)| \leq \alpha_i, \ i = 1, \ldots, n_a\} \subseteq \mathcal{X},
\]

\[
u \in \{u : |b_i^T(u - u_e)| \leq \beta_i, \ i = 1, \ldots, n_b\} \subseteq \mathcal{U}.
\]

LMI Sub-problem

A set of LMI constraints determine a positive definite matrix $Q$ and full state feedback matrix $K$ such that—defining

- $B(x) \triangleq V(x) - 1 = (x - x_e)^T Q^{-1} (x - x_e) - 1$
- $k(x) \triangleq u_e + K(x - x_e)$

LMIs:
- Lyapunov Stability
- State and Input Constraints

Cost Function:
- $\log(\det(Q))$
Composition of Barrier Pairs

**Proposition**

For any list of barrier pairs \((B_1, k_1), (B_2, k_2), \ldots, (B_N, k_N)\), the pair comprising the min-barrier function

\[
B(x) \triangleq \min_{n=1,\ldots,N} B_n(x)
\]

and (occasionally ambiguous) control input

\[
k(x) \triangleq k_n(x) \mid n \in \arg\min_{n=1,\ldots,N} B_n(x),
\]

\((B, k)\), is also a barrier pair.
Inverted Pendulum Example

An inverted pendulum \((m = 1 \text{ kg}, \ l = 1.213 \text{ m}, \ g = 9.8 \text{ m/s}^2)\)

Dynamics

\[ ml^2 \ddot{\theta} = \tau + mgl \cdot \sin(\theta) \]

Safe Region

\[ \begin{align*}
\mathcal{X} &= \left\{ \begin{bmatrix} \theta \\ \dot{\theta} \end{bmatrix} : |\theta| \leq \theta_c = 1 \text{ rad}, \ |\dot{\theta}| \leq 1 \text{ rad/s} \right\}, \\
\mathcal{U} &= \{ \tau : |\tau| \leq \bar{\tau} = 10 \text{ N} \cdot \text{m} \}. 
\end{align*} \]
Inverted Pendulum Example
Inverted Pendulum Example

The inverted pendulum system protected by the safety controller is placed in feedback.
**A dual spring-mass system ($M_1 = M_2 = 1$, $K = 1$)**

**Dynamics**

\[ M_1 \ddot{y}_1 = K(y_2 - y_1) + u, \quad M_2 \ddot{y}_2 = K(y_1 - y_2). \]

**Safe Region**

- $\mathcal{X} = \left\{ (y_1, \dot{y}_1, y_2, \dot{y}_2)^T : |y_1 - y_2| \leq 1, |y_i| \leq 1, |\dot{y}_i| \leq 1, \ i = 1, 2 \right\}$,
- $\mathcal{U} = \left\{ u : |u| \leq 10 \right\}$. 

Diagram:

- Masses $M_1$ and $M_2$ connected by a spring with stiffness $K$.
- Input $u$ applied to $M_1$.
Dual Spring-Mass Example

(a) $\dot{y}_1$ vs $y_1$
(b) $\dot{y}_2$ vs $y_2$
(c) $\dot{y}_2$ vs $y_1$
(d) $\dot{y}_1$ vs $y_2$
(e) $y_2$ vs $\dot{y}_1$
(f) $\dot{y}_1$ vs $\dot{y}_2$

- safety limits
- ellipsoid bounds
- trajectory
Thank you for listening!

This work was supported by NASA Space Technology Research Fellowship NNX15AQ33H (G.C.T), and a Longhorn Innovation Fund For Technology grant (B.H.).

Gray C. Thomas  
(512)-366-0230  
gray.c.thomas@utexas.edu

Binghan He  
(765)-404-5159  
bingham@utexas.edu

Luis Sentis  
(512)-471-5987  
lsentis@austin.utexas.edu
LMI Sub-problem

A set of LMI constraints determine a positive definite matrix $Q$ and full state feedback matrix $K = YQ^{-1}$ such that—defining

- $B(x) \triangleq (x - x_e)^T Q^{-1}(x - x_e) - 1$
- $k(x) \triangleq u_e + K(x - x_e)$

LMI Sub-problem

maximize $Q, Y$ \quad $\log(\det(Q))$

subject to

- $Q \succeq \varepsilon I$
- $a_i^T Q a_i \leq \alpha_i^2$, $\forall i = 1, \ldots, n_a$
- $\begin{pmatrix} Q & Y^T b_i \\ b_i^T Y & \beta_i^2 \end{pmatrix} \succeq 0$, $\forall i = 1, \ldots, n_b$
- $A_l Q + Q A_l^T + B_l Y + Y^T B_l^T + \varepsilon I + \lambda Q \preceq 0$, $\forall l = 1, \ldots, L$