Resilient Reachability for Linear Systems

Jean-Baptiste Bouvier, Melkior Ornik

Department of Aerospace Engineering and Coordinated Science Laboratory,
University of Illinois at Urbana-Champaign, USA
Email: bouvier3@illinois.edu & mornik@illinois.edu

21st IFAC World Congress, July 2020

This work was supported by an Early Stage Innovations grant from NASA's Space Technology Research Grants Program, grant no. 80NSSC19K0209.

Motivating example: story

Figure 1: SuBlue WhiteShark Max underwater robot[1]

Imagine if the circled thruster got damaged and produces undesirable uncontrolled inputs.

Can the robot still reach its target ?

[1] https://www.roboticgizmos.com/whiteshark-max-underwater-robot/

Motivating example: model

Underwater robot

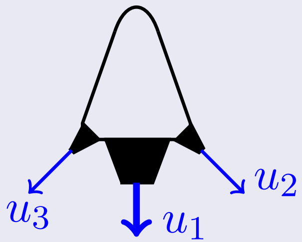


Figure 2: Underwater robot model

$$\dot{x} = Ax + \bar{B}\bar{u} \qquad x(0) = x_0,$$

$$\text{with} \qquad \bar{u} = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix}.$$

Scenario: After an accident the robot loses control authority over u_3, now producing undesirable inputs renamed $w = u_3$. The remaining controlled inputs are $u = \begin{bmatrix} u_1 & u_2 \end{bmatrix}^\top$ and we split $\bar{B} = \begin{bmatrix} B & C \end{bmatrix}$, so that

$$\dot{x} = Ax + Bu + Cw \qquad x(0) = x_0.$$

Problem statement

Assumption: The undesirable input w is measured in real-time.

Definition 1

The target G is *resiliently reachable at time T from x_0* if for all undesirable input $w \in W$, there exists a control law $u_w \in U$ such that $x(T) \in G$.

Problem: Is the target G resiliently reachable at time T from x_0?

Remark: Since w is measured, the control law can depend on the current and past undesirable input w, but not on the future values of w.

Limitations of current approaches

- *Actuator failure* considers actuator performing with a reduced magnitude or with a fixed unknown amplitude, e.g. Tang et al.[2], Wang and Wen[3].
- *Robust control* aims at strong reachability: a control law working for all undesirable inputs, e.g. Bertsekas and Rhodes[4], Rakovic et al.[5].
- *Reachability* studies of Marzollo and Pascoletti[6] and Mitchell and Tomlin[7] focused on numerical approaches.

---

[2] Tang, Tao, and Joshi, "Adaptive actuator failure compensation for nonlinear MIMO systems with an aircraft control application".

[3] Wang and Wen, "Adaptive actuator failure compensation control of uncertain nonlinear systems with guaranteed transient performance".

[4] Bertsekas and Rhodes, "On the Minimax Reachability of Target Sets and Target Tubes".

[5] Raković et al., "Reachability Analysis of Discrete-Time Systems With Disturbances".

[6] Marzollo and Pascoletti, "On the reachability of a given set under disturbances".

[7] Mitchell and Tomlin, "Overapproximating Reachable Sets by Hamilton-Jacobi Projections".

Framework

The controls and the undesirable inputs are square-integrable:

$$U = \big\{u \in \mathcal{L}_2\big([0,T],\mathbb{R}^2\big) : \|u\|_{\mathcal{L}_2} \leq 1\big\}$$
$$W = \big\{w \in \mathcal{L}_2\big([0,T],\mathbb{R}\big) : \|w\|_{\mathcal{L}_2} \leq 1\big\}.$$

The $\mathcal{L}_2$-norm is

$$\|u\|_{\mathcal{L}_2}^2 = \int_0^T \|u(t)\|^2 dt.$$

The target is a ball of radius $\varepsilon > 0$ centered around x_{goal}:

$$G = \big\{x \in \mathbb{R}^2 : \|x - x_{goal}\| \leq \varepsilon\big\}.$$

The unit circle in $\mathbb{R}^2$ is denoted by $\mathbb{U} = \big\{x \in \mathbb{R}^2 : \|x\| = 1\big\}$.

Preliminaries

The work of Delfour and Mitter[8] derived an analytical reachability condition for the dynamics $x(T) = s + S(u) + R(w)$.

Proposition 1 (Delfour and Mitter)

G is resiliently reachable at time T from x_0 if and only if

$$\sup_{\|x^*\|_{(\mathbb{R}^2)^*}=1} \Big\{ x^*(s - x_{goal}) - \|S^* x^*\|_{U^*} + \|R^* x^*\|_{W^*} - \varepsilon \Big\} \leq 0.$$

Highly abstract condition, due to dual terms denoted with a star.

[8] Delfour and Mitter, "Reachability of Perturbed Systems and Min Sup Problems".

Integral condition for resilient reachability

The Riesz-Fréchet representation theorem and the definition of adjoint maps simplify the previous Proposition and remove all dual terms.

Theorem 1 (Integral condition)

G is resiliently reachable at time T from x_0 if and only if

$$\max_{h\,\in\,\mathbb{U}} \left\{ \langle h, e^{AT}x_0 - x_{goal}\rangle - \sup_{\|u\|_{\mathcal{L}_2}=1} \left\{ \left| \left\langle h, \int_0^T e^{A(T-\tau)}Bu(\tau)d\tau \right\rangle \right| \right\} + \sup_{\|w\|_{\mathcal{L}_2}=1} \left\{ \left| \left\langle h, \int_0^T e^{A(T-\tau)}Cw(\tau)d\tau \right\rangle \right| \right\} - \varepsilon \right\} \leq 0.$$

Condition less abstract than the result of Delfour and Mitter, but still not easily computable.

A driftless submarine

Many systems, including the underwater robot are driftless, e.g. Vela et al.[9] or Siciliano and Khatlib[10]. With $A = 0$, the dynamics become

$$\dot{x} = Bu + Cw \qquad x(0) = x_0,$$

and from the Integral condition we derive

Theorem 2 (Driftless condition)

G is resiliently reachable at time T from x_0 if and only if

$$\max_{h \,\in\, \mathbb{U}} \Big\{ \langle h, d \rangle + g(h)\sqrt{T} \Big\} \leq \varepsilon,$$

with $\quad d = x_0 - x_{goal} \quad$ *and* $\quad g(h) := \big\| C^\top h \big\| - \big\| B^\top h \big\|.$

[9] Vela, Morgansent, and Burdick, "Underwater locomotion from oscillatory shape deformations".

[10] Siciliano and Khatlib, *Springer Handbook of Robotics*.

Intuition

The resilient reachability condition is $\max_{h\,\in\,\mathbb{U}} \Big\{ \langle h, d \rangle + g(h)\sqrt{T} \Big\} \leq \varepsilon$, with $d = x_0 - x_{goal}$, $g(h) := \big\| C^\top h \big\| - \big\| B^\top h \big\|$, and h^* the argument of the maximum.

- h^* maximizes $\langle h, d \rangle$, so it drives the system away from x_{goal}.
- Along direction h, $g(h)$ quantifies the difference of strength between undesirable inputs and controls.
- $\text{sign}\big(\max g(h) \big)$ tells which input is the strongest.
- h^* is the travel direction giving the most strength to the undesirable inputs over the controls.
- So h^* is the worst direction for resilient reachability.

Evolution of reachability with time

In the Driftless condition $\langle h, d\rangle$ is bounded, while $g(h)\sqrt{T}$ grows unbounded with time, so the sign of the maximum of $g(h)$ dictates the evolution of reachability with time.

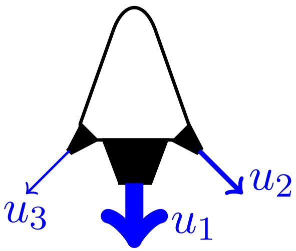
Theorem 3 (Time evolution)

- *If* $\max\{g(h)\} > 0$, *there exists a time* $\tau(d, \varepsilon)$ *after which* G *is not resiliently reachable from* x_0.
- *If* $\max\{g(h)\} = 0$, *the resilient reachability of* G *from* x_0 *depends on the distance* $d = x_0 - x_{goal}$.
- *If* $\max\{g(h)\} < 0$, *there exists a time* $\tau(d, \varepsilon)$ *after which* G *is resiliently reachable from* x_0.

Application to the underwater robot

The nominal dynamics of the underwater robot before the accident are

$$\dot{x} = \bar{B}\bar{u} = \begin{bmatrix} 10 & 1 & 0.5 \\ 0 & -1 & 0.5 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix}.$$



When losing control of u_3, $B = \begin{bmatrix} 10 & 1 \\ 0 & -1 \end{bmatrix}$, and $C = \begin{bmatrix} 0.5 \\ 0.5 \end{bmatrix}$, then $\max\big\{g(h)\big\} < 0$, so any target ball becomes resiliently reachable after some time.

However $\max\big\{g(h)\big\} > 0$ when losing control of u_1 or u_2.

Therefore, the robot is only resilient to the loss of u_3.

A sufficient reachability condition

The maximum of $g(h) = \|C^\top h\| - \|B^\top h\|$ can be difficult to compute, so we calculated an upper bound of $g(h)$ using $\sigma_{max}^{C^\top}$, the maximal singular value of $C^\top$ and $\sigma_{min}^{B^\top}$ the minimal singular value of $B^\top$.

Theorem 4 (Sufficient condition for reachability)

If $\sigma_{max}^{C^\top} < \sigma_{min}^{B^\top}$, *then* $\max\limits_{h \,\in\, \mathbb{U}} \big\{ g(h) \big\} < 0$.

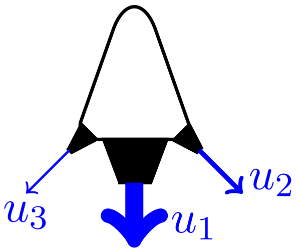
This result derives from

$$\begin{cases} \|C^\top h\|^2 = h^\top C C^\top h \leq \|h\|^2 \big(\sigma_{max}^{C^\top}\big)^2 \\ \|B^\top h\|^2 = h^\top B B^\top h \geq \|h\|^2 \big(\sigma_{min}^{B^\top}\big)^2 \end{cases}.$$

Application to the underwater robot

Recall the dynamics of the underwater robot before the accident:

$$\dot{x} = \bar{B}\bar{u} = \begin{bmatrix} 10 & 1 & 0.5 \\ 0 & -1 & 0.5 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix}.$$



When losing control of u_3 the singular values are: $\sigma_{max}^{C^\top} \approx 0.7 < \sigma_{min}^{B^\top} \approx 1$, the sufficient condition is verified, so the robot is resilient to the loss of u_3.

However, for the loss of u_1 or u_2 the inequality is not verified, so the sufficient condition is inconclusive about the resiliency of the robot.

Conclusion

We derived an analytical condition for resilient reachability in linear systems and two simple conditions for driftless systems.

Future work:

- Non-driftless systems.
- Inputs with other types of bounds.
- Resilient systems.
- Control synthesis.