Resilient Reachability for Linear Systems [⋆]

Jean-Baptiste Bouvier [*] **Melkior Ornik** [**]

[*] *Dept. of Aerospace Engineering (e-mail: bouvier3@illinois.edu)*
[**] *Dept. of Aerospace Engineering & Coordinated Science Laboratory,*
(e-mail: mornik@illinois.edu)
University of Illinois at Urbana-Champaign, Urbana, IL 61801 USA

Abstract: A fault-tolerant system is able to reach its goal even when some of its components are malfunctioning. This paper examines tolerance to a specific type of malfunction: the loss of control authority over actuators. Namely, we investigate whether the desired target set for a linear system remains reachable under any undesirable input. Contrary to robust control, we assume that the undesirable inputs can be observed in real time, and subsequently allow the control inputs to depend on these undesirable inputs. Building on previous work on reachability with undesirable inputs, this paper develops a reachability condition for linear systems, and obtains a formula that describes reachability of the goal set for driftless linear systems by computing the minimum of a concave-convex objective function. From this formulation we establish two novel sufficient conditions for resilient reachability.

Keywords: Linear systems, Fault-tolerant systems, Reachability, Zero drift, Non-convex optimization

1. INTRODUCTION

Fault-tolerant systems are required to be resilient to malfunctioning actuators. Among the possible malfunctions, the most widely studied type is actuator failure, which considers an actuator performing with a reduced amplitude or with a fixed unknown magnitude (Tang et al., 2007; Wang and Wen, 2010). Yet, the situation where an actuator becomes unmanageable and produces undesirable, uncontrolled outputs has been less investigated. Such a situation is referred to as *loss of control authority* over an actuator (Bucić et al., 2018). For instance, a damaged rudder flapping in the wind produces undesirable outputs, but cannot be turned off like a defective engine.

We are interested in the case of a system losing control authority over at least one of its actuators. The desire of this paper is to develop simple verification conditions determining whether the system is still able to reach its initial goal. While computation of a reachable set is a classical problem in control theory (Brockett, 1976; Isidori, 1985) and significant computational work has been performed in order to make finding a solution feasible (see, e.g., Kurzhanski and Varaiya (2000); Girard and Guernic (2008)), classical methods often rely on full knowledge of system state and inputs and cannot be directly applied to the case of loss of control authority.

To handle systems enduring undesirable inputs, the field of robust control aims at guaranteeing *strong reachability* i.e. finding a control working for any perturbation, and has been widely studied by, e.g., Bertsekas and Rhodes (1971), Bertsekas (1972) and Raković et al. (2006). However, our case of interest does not feature perturbations, but undesirable inputs from one of the very own actuators of the system. In that case, real-time input measurements are usually available, rendering robustness unnecessarily conservative, and calls for a different type of reachability. Namely, we say that a goal is *resiliently reachable* from an initial state if for any undesirable inputs, there exists a control law — possibly dependent on current undesirable inputs, but with no knowledge of future ones — able to drive the system to the target set. While not referring to it as resilient reachability, Marzollo and Pascoletti (1973) and Mitchell and Tomlin (2003) considered this setting but focused on algorithmic approaches instead of looking for an analytical solution. Delfour and Mitter (1969) transformed the problem of resilient reachability into a minimax formula assessing whether a target set is reachable. While our paper heavily draws from the latter work, their resulting reachability conditions are highly abstract, lack intuition, and are difficult to compute.

This paper aims at extending reachability analysis methods to linear systems with loss of control authority. The contributions of this paper are fourfold. First, we consider the reachability condition of Delfour and Mitter (1969) and develop it into a usable equation describing resilient reachability for linear systems. Second, we tackle the specific case of driftless systems, and derive a computable condition for resilient reachability. Third, we analyze the evolution with time of resilient reachability for driftless systems, and show that the resilient reachability problem can be formulated as a minimax optimization of a concave-convex objective function. Fourth, we establish several sufficient conditions that enable us to avoid solving the developed optimization problem.

The remainder of the paper is organized as follows. Section 2 defines the problem of interest and states the related

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

necessary definitions. Section 3 introduces preliminary results obtained by Delfour and Mitter (1969), upon which we build our theory. In Section 4 we develop a resilient reachability condition for linear systems. Section 5 applies this condition to driftless systems, while Section 6 explores how resilient reachability of a target set evolves with time and establishes a sufficient condition for resilient reachability. A scenario with an underwater robot illustrates our theory in Section 7.

Notation: We use $\|\cdot\|_X$ to denote the canonical norm on the space X. For $x = (x_1, ..., x_n) \in \mathbb{R}^n$, $\|x\|_{\mathbb{R}^n} = \sqrt{\sum x_i^2}$. The ball of center x and radius ε in the space X is $\mathbb{B}_X(x, \varepsilon)$. We use $\langle \cdot, \cdot \rangle_X$ to denote the inner product on X. The space of continuous linear maps from X into Y is denoted by $\mathcal{L}\big(X, Y\big)$, while $\mathcal{L}_2\big([0, T],\ \mathbb{R}^m\big)$ or simply $\mathcal{L}_2$ denotes the space of the square integrable functions. For a Banach space X, its topological dual space is $X^* = \mathcal{L}\big(X, \mathbb{R}\big)$. The dual vector of $x \in X$ is $x^* \in X^*$, and denotes the associated linear form from X to $\mathbb{R}$. For $S \in \mathcal{L}\big(X, Y\big)$, $S^* \in \mathcal{L}\big(Y^*, X^*\big)$ is the adjoint linear map.

2. PROBLEM STATEMENT

Consider a system's dynamics $\dot{x} = Ax + D\bar{u}$, where $A \in \mathbb{R}^{n \times n}$ and $D \in \mathbb{R}^{n \times (m+p)}$ are constant. Let $G \subset \mathbb{R}^n$ be the target set ("goal") to be reached by the system. Assume that, during its mission, the system loses authority over p of its $m + p$ actuators. We can then separate the controlled inputs $u \in \mathbb{R}^m$ from the undesirable inputs $w \in \mathbb{R}^p$ by writing $\bar{u} = [u^\top\ w^\top]^\top$ and $D = [B\ C]$, with $B \in \mathbb{R}^{n \times m}$ and $C \in \mathbb{R}^{n \times p}$. The system's dynamics can thus be rewritten as follows:

$$\dot{x}(t) = Ax(t) + Bu(t) + Cw(t), \qquad x(0) = x_0 \in \mathbb{R}^n. \quad (1)$$

The goal of this paper is to find a simple condition that characterizes whether a target set is reachable in a given time for a system undergoing a loss of control authority, *regardless* of the inputs imposed by the malfunctioning actuators, but with possible real-time knowledge of those inputs. We thus formulate the problems of *resilient reachability* of G within a time $T \geq 0$.

Problem 1. Determine if, for any undesirable inputs w, there exists a control law u_w driving the system from x_0 to G at time T.

Problem 2. Determine if, for any undesirable inputs w, there exists a control law u_w driving the system from x_0 to G before the time T.

We note the possible dependence of u_w on the undesirable input w. Unlike the concept of strong reachability in classical robust control (Bertsekas, 1972; Raković et al., 2006), the objective in Problems 1 and 2 is not to a priori design a control law driving the state to the target set for any undesirable inputs, but instead to guarantee that whatever the undesirable inputs are, one can determine a control law *dependent on the undesirable inputs* to drive the system to its goal. The intuition behind posing such problems is that the system inputs, even if not desirable, can often be measured. In turn, one can counteract undesirable inputs more efficiently when these inputs are known and a subsequent controller can thus handle perturbations of a larger magnitude than a standard robust controller.

The technical work of this paper follows the assumptions of Delfour and Mitter (1969) and considers square integrable inputs over their time domain $[0, T]$. Namely, if U is the set of admissible control laws and W is the set of undesirable signals, we consider

$$\begin{aligned} U &= \big\{u \in \mathcal{L}_2\big([0, T],\ \mathbb{R}^m\big) : \|u\|_{\mathcal{L}_2} \leq 1\big\} &&= \mathbb{B}_{\mathcal{L}_2}(0, 1), \\ W &= \big\{w \in \mathcal{L}_2\big([0, T],\ \mathbb{R}^p\big) : \|w\|_{\mathcal{L}_2} \leq 1\big\} &&= \mathbb{B}_{\mathcal{L}_2}(0, 1), \\ G &= \big\{x \in \mathbb{R}^n : \|x - x_{goal}\|_{\mathbb{R}^n} \leq \varepsilon\big\} &&= \mathbb{B}_{\mathbb{R}^n}(x_{goal}, \varepsilon), \end{aligned}$$

where $x_{goal} \in \mathbb{R}^n$ and $0 \leq \varepsilon < \infty$.

Let us formally define the sets of the initial states from which the system can be driven to G at or before time T:

$$\begin{aligned} X_0^T &= \big\{x_0 \in \mathbb{R}^n : \forall\ w \in W,\ \exists\ u \in U : x(T) \in G\big\}, \\ X_0^{\leq T} &= \big\{x_0 \in \mathbb{R}^n : \exists\ t \in [0, T] : x_0 \in X_0^T\big\}. \end{aligned} \quad (2)$$

We can now define the notion of resilient reachability associated with our problems:

Definition 1. The target set G is *resiliently reachable from x_0 in time t* if $x_0 \in X_0^T$.

Definition 2. The target set G is *resiliently reachable from x_0 by time T* if $x_0 \in X_0^{\leq T}$.

We emphasize that this paper is focused on solving Problems 1 and 2 as they are stated, i.e., on determining the existence of a control law and not on its calculation. The subsequent problem of determining the appropriate control law is naturally of future interest.

We now describe prior results enabling our work.

3. PRELIMINARIES

The main result of this section is a resilient reachability condition derived from Delfour and Mitter (1969), which will serve as foundation to build our theory.

Delfour and Mitter (1969) worked with the abstract system

$$x = s + S(u) + R(w), \quad (3)$$

where $x \in X_3$ is the state, $u \in X_1$ is the control and $w \in X_2$ is the disturbance. The system's initial state is $s \in X_3$, while maps $S \in \mathcal{L}\big(X_1, X_3\big)$ and $R \in \mathcal{L}\big(X_2, X_3\big)$ represent respectively the effects of controlled and undesirable inputs. We consider $X_1 = \mathcal{L}_2\big([0, T],\ \mathbb{R}^m\big)$, $X_2 = \mathcal{L}_2\big([0, T],\ \mathbb{R}^p\big)$, and $X_3 = \mathbb{R}^n$.

We first transform (1) into (3) by applying the process described in Section 7 of Delfour and Mitter (1969). We define the following continuous linear operators:

$$S(u) = \int_0^T e^{A(T-t)} Bu(t)dt, \qquad R(w) = \int_0^T e^{A(T-t)} Cw(t)dt.$$

By taking $s = e^{AT} x_0 \in \mathbb{R}^n$, the solution of (1) is then

$$x(T) = s + S(u) + R(w).$$

For a Banach space X and its adjoint X^*, the norm of $x^* \in X^*$ is defined (Conway, 1990) by

$$\|x^*\|_{X^*} = \sup_{\|x\|_X = 1} \big\{|x^*(x)|\big\} = \sup_{\|x\|_X \leq 1} \big\{|x^*(x)|\big\}. \quad (4)$$

Proposition 1. G is resiliently reachable from x_0 in time T if and only if

$$\sup_{\|x^*\|_{X_3^*} = 1} \Big\{x^*(s - x_{goal}) - \|S^* x^*\|_{X_1^*} + \|R^* x^*\|_{X_2^*} - \varepsilon\Big\} \leq 0.$$

Proof. Let us start from Corollary 5.8 of Delfour and Mitter (1969), which, while not using the same terminology, states that the goal G is resiliently reachable if and only if

$$\sup_{\|x^*\|_{X_3^*}=1} \Big\{ x^*(s) + \inf_{u\in U}\big(S^*x^*(u)\big) + \sup_{w\in W}\big(R^*x^*(w)\big) - \sup_{y\in G}\big(x^*(y)\big)\Big\} \le 0. \tag{5}$$

By the definition of U, for $u \in U$, $-u \in U$. Since S^*x^* is linear, $\inf\limits_{u\in U}\big(S^*x^*(u)\big) = -\sup\limits_{u\in U}\big(|S^*x^*(u)|\big) = -\|S^*x^*\|_{X_1^*}$. And similarly, $\sup\limits_{w\in W}\big(R^*x^*(w)\big) = \|R^*x^*\|_{X_2^*}$.

For $y \in G = \mathbb{B}_{\mathbb{R}^n}(x_{goal}, \varepsilon)$, we write $y = x_{goal} + \delta y$, since and x^* is linear, $x^*(y) = x^*(x_{goal}) + x^*(\delta y)$. Then,

$$\sup_{y\in G}\big(x^*(y)\big) = x^*(x_{goal}) + \sup_{\|\delta y\|\le\varepsilon}\big(x^*(\delta y)\big) = x^*(x_{goal}) + \varepsilon,$$

because $\sup\limits_{\|\delta y\|\le\varepsilon}\big(x^*(\delta y)\big) = \varepsilon \sup\limits_{\|z\|\le 1}\big(x^*(z)\big) = \varepsilon \underbrace{\|x^*\|_{X_3^*}}_{=\,1} = \varepsilon.$

We can then simplify the terms in (5) to obtain the desired formula. ■

The reachability condition derived in Proposition 1 is highly abstract due to the dual terms and is impractical to use. The following two sections aim to develop more workable conditions.

4. INTEGRAL RESILIENT REACHABILITY CONDITION

We will now work on the simplification of Proposition 1 into a more explicit condition. First, note that x^* is bounded as $\|x^*\|_{X_3^*} = 1$. We can thus use the Riesz representation theorem (Conway, 1990): there exists a unique $h \in \mathbb{R}^n$ such that

$$x^*(\cdot) = \langle h, \cdot\rangle \quad \text{and} \quad \|h\|_{\mathbb{R}^n} = \|x^*\|_{X_3^*} = 1.$$

Then, the supremum in Proposition 1 is over the unit sphere in $\mathbb{R}^n$, i.e. for $h \in \mathbb{U} = \big\{x \in \mathbb{R}^n : \|x\| = 1\big\}$. With $s = e^{AT}x_0$, the first term in Proposition 1 becomes

$$x^*(s - x_{goal}) = \langle h, e^{AT}x_0 - x_{goal}\rangle_{\mathbb{R}^n}. \tag{6}$$

We can now simplify the adjoint maps with the definition from Conway (1990). For any $u \in \mathcal{L}_2$ we have

$$\begin{aligned} S^*x^*(u) &= \big(x^* \circ S\big)(u) = x^*\big(S(u)\big) = \langle h, S(u)\rangle \\ &= \langle h, \int_0^T e^{A(T-\tau)}Bu(\tau)d\tau\rangle. \end{aligned} \tag{7}$$

Putting (4) and (7) together, we obtain

$$\|S^*x^*\|_{\mathcal{L}_2^*} = \sup_{\|u\|_{\mathcal{L}_2}=1}\left\{\left|\left\langle h, \int_0^T e^{A(T-\tau)}Bu(\tau)d\tau\right\rangle\right|\right\}. \tag{8}$$

We proceed similarly for $\|R^*x^*\|_{\mathcal{L}_2^*}$. We can then simplify Proposition 1.

Theorem 2. G is resiliently reachable from x_0 in time T if and only if

$$\max_{h\in\mathbb{U}}\Bigg\{\langle h, e^{AT}x_0 - x_{goal}\rangle - \sup_{\|u\|_{\mathcal{L}_2}=1}\left\{\left|\left\langle h, \int_0^T e^{A(T-\tau)}Bu(\tau)d\tau\right\rangle\right|\right\} + \sup_{\|w\|_{\mathcal{L}_2}=1}\left\{\left|\left\langle h, \int_0^T e^{A(T-\tau)}Cw(\tau)d\tau\right\rangle\right|\right\} - \varepsilon\Bigg\} \le 0. \tag{9}$$

Proof. After using (6) and (8) for S^* and R^* in Proposition 1, the only work left is to prove that the supremum from Proposition 1 turns into $\max_{h\in\mathbb{U}}$, which follows from the discussion preceding (6), $\mathbb{U}$ being closed, and the function to maximize being continuous in h. ■

Because Theorem 2 directly uses matrices A, B and C instead of adjoint maps, it is more direct than the equation (5) we started from. Yet, computing the two supremums on $\mathcal{L}_2$ is a difficult task because of its infinite dimension. We now focus on driftless systems where the integrals in (9) can be simplified.

5. DRIFTLESS SYSTEMS

Driftless systems are widely studied in robotics; examples are described in Siciliano and Khatlib (2016). For these systems matrix A equals 0, so that (1) becomes

$$\dot{x}(t) = Bu(t) + Cw(t). \tag{10}$$

We can then distill Theorem 2 into a simpler form.

Theorem 3. $G = \mathbb{B}_{\mathbb{R}^n}(x_{goal}, \varepsilon)$ is resiliently reachable at T from x_0 iff

$$\max_{h\in\mathbb{U}}\Big\{\langle h, x_0 - x_{goal}\rangle - \sqrt{T}\,\big\|B^\top h\big\|_{\mathbb{R}^m} + \sqrt{T}\,\big\|C^\top h\big\|_{\mathbb{R}^p}\Big\} \le \varepsilon.$$

Proof. When $A = 0$, the leftmost term in (9) clearly equals $\langle h, x_0 - x_{goal}\rangle$. We simplify the next term with the Cauchy-Schwarz inequality:

$$\left|\langle h, B\int_0^T u(\tau)d\tau\rangle_{\mathbb{R}^n}\right| \le \big\|B^\top h\big\|_{\mathbb{R}^m}\left\|\int_0^T u(\tau)d\tau\right\|_{\mathbb{R}^m} \tag{11}$$

The equality in (11) occurs when $B^\top h$ and $\int_0^T u(\tau)d\tau$ are positively collinear (Conway, 1990).

By decomposing u on the canonical basis of $\mathbb{R}^m$, we can bound the norm of the integral of u:

$$\begin{aligned} \left\|\int_0^T u(\tau)d\tau\right\|_{\mathbb{R}^m} &= \sqrt{\sum_{i=1}^m\left(\int_0^T 1 \times u_i(\tau)\ d\tau\right)^2} \\ &\le \sqrt{\sum_{i=1}^m\left(T\times\int_0^T u_i^2(\tau)d\tau\right)} = \sqrt{T}\|u\|_{\mathcal{L}_2}. \end{aligned} \tag{12}$$

In (12), we use again the Cauchy-Schwarz inequality. The equality occurs when each u_i is almost everywhere (in the measure-theoretical sense) collinear with the function $\tau \mapsto 1$, i.e., when u is almost everywhere constant. By combining (11) and (12), we proved that

$$\sup_{\|u\|_{\mathcal{L}_2}=1}\left\{\left|\left\langle h, \int_0^T Bu(\tau)d\tau\right\rangle\right|\right\} \le \|B^\top h\|_{\mathbb{R}^m}\sqrt{T}. \tag{13}$$

If we can find a function u_h of unit norm in $\mathcal{L}_2$ for which the inequality in (13) is an equality, then the supremum in

(13) would be a maximum. The function u_h must realize both equality cases of the Cauchy-Schwarz inequality used previously. Hence, for $h \in \mathbb{U}$ we define the following constant function: $u_h(t) := B^\top h/(\sqrt{T}\|B^\top h\|_{\mathbb{R}^m})$. We note that $\|u_h(t)\|_{\mathbb{R}^m} = 1/\sqrt{T}$ for all t. Thus,

$$\|u_h\|_{\mathcal{L}_2} = \sqrt{\int_0^T \|u_h(t)\|^2_{\mathbb{R}^m} dt} = \sqrt{\int_0^T \frac{1}{T} dt} = 1. \tag{14}$$

Moreover, as u_h is positively collinear with $B^\top h$ and is constant over time, it satisfies both of the Cauchy-Schwarz equality cases in (11) and (12), which leads to

$$\left|\left\langle h, \int_0^T Bu_h(\tau)d\tau\right\rangle\right| = \left\|B^\top h\right\|_{\mathbb{R}^m} \sqrt{T}\|u_h\|_{\mathcal{L}_2}. \tag{15}$$

From (13), (14) and (15), we clearly obtain

$$\max_{\|u\|_{\mathcal{L}_2}=1}\left\{\left|\left\langle h, \int_0^T Bu(\tau)d\tau\right\rangle\right|\right\} = \sqrt{T}\left\|B^\top h\right\|_{\mathbb{R}^m}.$$

The same process can be applied to the final term in (9), yielding the theorem claim. ■

To simplify the notation of Theorem 3, let us first write $d = x_0 - x_{goal}$ and define the functions:

$$J(h,\ t) := \langle h, d\rangle + \sqrt{t}\big(\left\|C^\top h\right\| - \left\|B^\top h\right\|\big) \tag{16}$$

and $f(t) := \max\limits_{h\in\mathbb{U}}\big\{J(h,t)\big\}$. Thus, the condition of Theorem 3 is equivalent to $f(T) \leq \varepsilon$.

The scalar product $\langle h, d\rangle$ gives the intuition that h represents a travel direction. Call h^* the argument of the maximum. Then, h^* is positively collinear with d, so it is driving the system away from x_{goal}. On the other hand, the terms $B^\top h$ and $C^\top h$ represent how the inputs drive the system when they are along the direction h. Hence, on an intuitive level, h^* is the direction giving the most strength to the undesirable inputs over the controlled inputs. Since $\mathbb{U}$ is the unit sphere in $\mathbb{R}^n$, $\max_{h\in\mathbb{U}}$ explores every direction. Therefore, h^* represents the "worst direction" for resilient reachability.

We can strengthen our faith in Theorem 3 by looking at a few special cases. Assuming $x_0 = x_{goal}$, G becomes reachable at time $T = 0$ since, for all $h \in \mathbb{U}$, $\langle h, d\rangle = 0$. Another simple case is when $B = C = 0$, so $\dot{x} = 0$, i.e. $x(t) = x_0$ for all t, and the reachability condition becomes as expected $\|d\| \leq \varepsilon$, which is equivalent to $x_0 \in G$.

Theorem 3 gives a condition on resilient reachability at time T. We now have all the tools to study how the resilient reachability of G evolves with time.

6. EVOLUTION OF REACHABILITY WITH TIME

Note first that for $t > 0$, $J(\cdot, t)$ is not a concave function, and thus its maximization over $\mathbb{U}$ may not be an easy task. Indeed, both functions $h \mapsto \|C^\top h\|$ and $h \mapsto \|B^\top h\|$ are convex, so $J(\cdot, t)$ is the difference between two convex functions. This type of maximization is referred to as a *difference of convex* (DC) problem, and analytical solutions are only available for a few special cases. Numerous algorithms have been developed by, e.g. Tuy (1987) and Tao and An (1997). In particular, the simple algorithm devised by Yuille and Rangarajan (2003) to minimize a function composed of a concave and a convex part has been of great interest and is called the *concave-convex procedure*. While these numerical results, combined with Theorem 3, enable us to determine whether set G is resiliently reachable *at* every given time, they do not enable us to directly gain insight regarding reachability *by* a certain time like an analytical solution would.

In order to discuss reachability by a certain time, we apply Theorem 3 to note that G is resiliently reachable from x_0 by time T if and only if

$$\min_{t\in[0,T]}\Big\{\max_{h\in\mathbb{U}}\big\{J(h,t)\big\}\Big\} \leq \varepsilon.$$

Hence the reachability by time T can be described as a minimax problem with a DC cost function. We will omit the discussion of possible numerical solutions to such a problem and instead focus on analytical results.

Let us define the function $g(h) := \|C^\top h\| - \|B^\top h\|$, so that $J(h,t) = h^\top d + g(h)\sqrt{t}$. For a given goal and initial state, $\|h^\top d\|$ is bounded. So, as time grows, $\sqrt{t}$ becomes the leading term in J, with its sign determined by $g(h)$. We therefore study the sign of $\max\big\{g(h)\big\}$. We will show the following:

- if $\max\limits_{h\in\mathbb{U}}\big\{g(h)\big\} > 0$, G is only resiliently reachable up to a certain time,
- if $\max\limits_{h\in\mathbb{U}}\big\{g(h)\big\} = 0$, the resilient reachability of G depends on the distance d,
- if $\max\limits_{h\in\mathbb{U}}\big\{g(h)\big\} < 0$, G is resiliently reachable from some time onwards.

We prove these claims in the following three subsections.

6.1 Maximum of g is positive

If $\max\big\{g(h)\big\} > 0$, then $\|C^\top h\| > \|B^\top h\|$ for some h. In other words, in line with our intuition, there is an input direction where the matrix C produces a stronger undesirable input than what the control matrix B is capable of counteracting. Since we want to guarantee reaching the goal for *any* undesirable input, the target is not resiliently reachable. We formalize this intuition as follows.

Theorem 4. Let $x_0 \in \mathbb{R}^n$. If $\max\limits_{h\in\mathbb{U}}\big\{g(h)\big\} > 0$, then there exists $t_{lim} > 0$ such that for all $t \geq t_{lim}$, $x_0 \notin X_0^T$.

Proof. We use the notation as given above. Because $\max\limits_{h\in\mathbb{U}}\big\{g(h)\big\} > 0$, there is a $h_+ \in \mathbb{U}$ such that $g(h_+) > 0$. $f(t) \geq \langle h_+, d\rangle + g(h_+)\sqrt{t} \xrightarrow[t\to\infty]{} +\infty$. So, $\lim\limits_{t\to\infty} f(t) = +\infty$. Then, there exists $t_{lim} > 0$ such that for $t \geq T$, $f(t) > \varepsilon$. In that case, Theorem 3 states that G is not reachable at time t from x_0, i.e. $x_0 \notin X_0^T$. ■

Theorem 4 states that, for a fixed initial state x_0 and a goal G, there exists a time T after which the target set is not resiliently reachable anymore. Thus, all resilient reachability can only happen in finite time.

6.2 Maximum of g equals zero

When $\max\big\{g(h)\big\} = 0$, there is at least one $h \in \mathbb{U}$ such that $g(h) = 0$. Intuitively, in this direction h the strength of the undesirable inputs matches the strength of the controlled ones. In directions where g is negative, the controlled inputs have a greater magnitude than the undesirable inputs. Thus, the resilient reachability of G depends on its location.

Let us define $H_0 = \{h \in \mathbb{U} : g(h) = 0\}$. The set H_0 is closed, bounded, and nonempty by the assumption of $\max\{g(h)\} = 0$. So with $d = x_0 - x_{goal}$, we can define $h_0 = \arg\max_{h \in H_0}\{h^\top d\}$. We note that vector h_0 need not be uniquely defined. The theorem below holds for every h_0.

Theorem 5. Assume $\max_{h\in\mathbb{U}}\{g(h)\} = 0$. If $\varepsilon \geq \|d\|$, then $x_0 \in X_0^T$ for all $t \geq 0$, and if $\varepsilon < h_0^\top d$, then $x_0 \notin X_0^T$ for all $t \geq 0$.

Proof. We note that $\max_{h\in\mathbb{U}}\{h^\top d\} = f(0) = \|d\|$. Thus,

$$f(t) \leq \max_{h\in\mathbb{U}}\{h^\top d\} + \max_{h\in\mathbb{U}}\{g(h)\sqrt{t}\} = \|d\| + 0 = \|d\|,$$

so $\max_{t\geq 0}\{f(t)\} = \|d\|$.

Additionally, $h_0 \in \mathbb{U}$, so $f(t) \geq h_0^\top d + g(h_0)\sqrt{t} = h_0^\top d$. Thus, $h_0^\top d \leq f(t) \leq \|d\|$ for all $t \geq 0$.

If $\varepsilon \geq \|d\|$, then for $t \geq 0$, $f(t) \leq \varepsilon$, i.e., by Theorem 3, $x_0 \in X_0^T$. On the other hand, if $\varepsilon < h_0^\top d$, then for $t \geq 0$, $f(t) > \varepsilon$, so by Theorem 3, $x_0 \notin X_0^T$. ■

So, if $\varepsilon \geq \|d\|$, G is resiliently reachable from the start and remains always resiliently reachable, while if $\varepsilon < h_0^\top d$, G is never resiliently reachable. There is obviously an intermediate case for $\varepsilon \in \left[h_0^\top d, \|d\|\right]$ where the resilient reachability of G depends on time.

6.3 Maximum of g is negative

We can now tackle the third case, where $\max\left\{g(h)\right\} < 0$. In this situation, our intuition indicates that controlled inputs are stronger than the undesirable inputs in every direction, so the reachable set grows unbounded with time. The theorem below confirms this intuition.

Theorem 6. If $\max_{h\in\mathbb{U}}\{g(h)\} < 0$, then there exists $t_{lim} \geq 0$ such that $x_0 \in X_0^T$ for all $t \geq t_{lim}$.

Proof. Let $\max_{h\in\mathbb{U}}\{g(h)\} = -\gamma < 0$. Then f can be bounded by above:

$$\begin{aligned} f(t) &= \max_{h\in\mathbb{U}}\{h^\top d + g(h)\sqrt{t}\} \\ &\leq \max_{h\in\mathbb{U}}\{h^\top d\} + \max_{h\in\mathbb{U}}\{g(h)\}\sqrt{t} = \|d\| - \gamma\sqrt{t}. \end{aligned}$$

We compare this upper bound with ε to obtain a reachability condition

$$\|d\| - \gamma\sqrt{t} \leq \varepsilon \iff t_{lim} := \left(\frac{\|d\| - \varepsilon}{\gamma}\right)^2 \leq t.$$

such that, for all $t \geq t_{lim}$, $f(t) \leq \varepsilon$, which is equivalent to $x_0 \in X_0^T$ according to Theorem 3. ■

The t_{lim} defined in the proof of Theorem 6 might not be the minimal time for resilient reachability. Nonetheless, Theorem 6 proves that, after some time, any target set becomes resiliently reachable.

Theorems 4, 5 and 6 show that the sign of the maximum of g leads to interesting conclusions. It is thus natural to attempt to analytically determine an upper bound for g.

6.4 Bounding g

Let $\sigma_{max}^{C^\top}$ be the maximal singular value of $C^\top$, and $\sigma_{min}^{B^\top}$ be the minimal singular value of $B^\top$. We claim that the relationship between these two values impacts the maximal value of g.

Theorem 7. If $\sigma_{max}^{C^\top} < \sigma_{min}^{B^\top}$, then $\max_{h\in\mathbb{U}}\{g(h)\} < 0$.

Proof. Let us define $M = CC^\top$. The matrix M is symmetric, so we can use the following classical inequality (Horn and Johnson, 2012):

$$\lambda_{min}^M \|x\|^2 \leq x^\top M x \leq \lambda_{max}^M \|x\|^2, \qquad \forall x \in \mathbb{R}^n,$$

with λ_{min}^M and λ_{max}^M respectively, the minimum and maximum eigenvalues of M. Since M is trivially positive semidefinite, $\lambda_{min}^M \geq 0$. Note that $\|C^\top h\| = \sqrt{h^\top CC^\top h} = \sqrt{h^\top M h}$. Thus we obtain

$$\sqrt{\lambda_{min}^M} \leq \|C^\top h\| \leq \sqrt{\lambda_{max}^M} = \sigma_{max}^{C^\top}, \qquad \forall h \in \mathbb{U}.$$

By doing the same for $B^\top$, g can be bounded as follows:

$$\sqrt{\lambda_{min}^{C^\top}} - \sqrt{\lambda_{max}^{B^\top}} \leq g(h) \leq \sigma_{max}^{C^\top} - \sigma_{min}^{B^\top}, \qquad \forall h \in \mathbb{U}.$$

So if $\sigma_{max}^{C^\top} < \sigma_{min}^{B^\top}$, then $\max_{h\in\mathbb{U}}\{g(h)\} < 0$. ■

Theorems 6 and 7 trivially imply the following corollary.

Corollary 8. If all singular values of $C^\top$ are strictly smaller than those of $B^\top$, then the target set is resiliently reachable in finite time.

The intuition behind Corollary 8 is that the singular values of $B^\top$ and $C^\top$ respectively quantify the strength of the controlled and undesirable inputs. We now proceed to computationally confirm the above theoretical results.

7. NUMERICAL EXAMPLE

We consider an underwater robot propelled by three engines, as shown in Fig. 7. The main engine u_1 has a small bias in the y direction.

$$\begin{bmatrix}\dot{x}\\ \dot{y}\end{bmatrix} = \begin{bmatrix}10 & 1 & 1\\ 0.2 & -1 & 1\end{bmatrix}\begin{bmatrix}u_1\\ u_2\\ u_3\end{bmatrix}$$

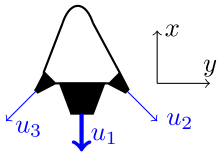

Fig. 1. A model of an underwater robot with three engines.

Our example is motivated by the work of Vela et al. (2002) and Yu et al. (2016), which have also considered driftless dynamics. The assumption of driftlessness can intuitively be justified by the viscosity of the water combined with a small speed of the robot.

During its mission the controller loses authority over the third actuator. The terms in (10) can thus be written as follows:

$$u = \begin{bmatrix}u_1\\ u_2\end{bmatrix}, \quad w = u_3, \quad B = \begin{bmatrix}10 & 1\\ 0.2 & -1\end{bmatrix}, \quad C = \begin{bmatrix}1\\ 1\end{bmatrix}.$$

Intuitively, the robot should still be able to reach any goal set, since the second actuator u_2 can counteract the undesirable inputs of u_3, and the small bias of u_1 on y provides a net motion on y, while the desired displacement along x is also realized by the main engine. Theorem 7 provides only a sufficient condition for reachability, so even if its conditions are not met ($\sigma_{max}^{C^\top} \approx 1,4 > \sigma_{min}^{B^\top} \approx 1,0$) it does not mean that the target is not resiliently reachable. Actually, we can compute $\max\limits_{h\in\mathbb{U}}\{g(h)\} = -0.02$, and use Theorem 6 to show that any target ball is eventually resiliently reachable, as suggested by our intuition.

In the situation where the controller loses authority over both the second and third actuators, our intuition suggests that a controlled motion along x is still possible, but the displacements along y cannot be controlled. Therefore, we cannot guarantee to reach any target position. We numerically compute g and obtain $\max\limits_{h\in\mathbb{U}}\{g(h)\} = 1.4 > 0$. The conclusion of Theorem 4 validates our intuition.

If the controller only loses authority over the first actuator, then $\max\limits_{h\in\mathbb{U}}\{g(h)\} = 8.6 > 0$. Of course none of the side engines can make up for the loss of the main one, as predicted by Theorem 4.

Another interesting case to note is when u_1 thrusts only along x without bias on y, i.e.,

$$\dot{X} = \begin{bmatrix} \dot{x} \\ \dot{y} \end{bmatrix} = \begin{bmatrix} 10 & 1 & 1 \\ 0 & -1 & 1 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix}.$$

Then, a loss of control authority over one of the side engines results in $\max\limits_{h\in\mathbb{U}}\{g(h)\} = 0.02 > 0$. Indeed, we cannot guarantee to reach a goal that is not on the x axis, because no net motion on y is guaranteed, since both side engines can cancel each other out.

8. CONCLUSION

This paper described the problem of resilient reachability: deciding whether a system can always be driven to a desired goal, given that some of its actuators act in an undesirable manner and without prior knowledge of these undesirable inputs. To solve this problem, we derived a resilient reachability condition for linear systems and a more specific condition for driftless systems. We investigated the evolution of resilient reachability with time and rewrote the problem as a minimax optimization with a concave-convex objective function. We then derived results that do not require directly solving the optimization problem, at the price of providing sufficient or necessary conditions.

This manuscript, however, presents only the first step in our long-term goal of *resilient system synthesis*, i.e., design of actuator functionality (in the context of this paper represented by system matrices) for which the system retains resilient reachability to loss of one or more actuators. Furthermore, since resilient reachability relates to the existence of a control law, our future work will naturally tackles the construction of such a control law.

REFERENCES

Bertsekas, D. (1972). Infinite-time reachability of state-space regions by using feedback control. *IEEE Transactions on Automatic Control*, 17(5), 604 – 612.

Bertsekas, D. and Rhodes, I. (1971). On the minimax reachability of target sets and target tubes. *Automatica*, 7, 233 – 247.

Brockett, R.W. (1976). Nonlinear systems and differential geometry. *Proceedings of the IEEE*, 64(1), 61–72.

Bucić, M., Ornik, M., and Topcu, U. (2018). Graph-based controller synthesis for safety-constrained, resilient systems. In *56th Annual Allerton Conference on Communication, Control, and Computing*, 297 – 304.

Conway, J.B. (1990). *A Course in Functional Analysis*. Springer.

Delfour, M.C. and Mitter, S.K. (1969). Reachability of perturbed systems and min sup problems. *SIAM Journal on Control and Optimization*, 7(4), 521 – 533.

Girard, A. and Guernic, C.L. (2008). Efficient reachability analysis for linear systems using support functions. In *17th IFAC World Congress*, 8966 – 8971.

Horn, R.A. and Johnson, C.R. (2012). *Matrix Analysis*. Cambridge University Press.

Isidori, A. (1985). *Nonlinear Control Systems*. Springer.

Kurzhanski, A.B. and Varaiya, P. (2000). Ellipsoidal techniques for reachability analysis. In *Hybrid Systems: Computation and Control*, 202 – 214.

Marzollo, A. and Pascoletti, A. (1973). On the reachability of a given set under disturbances. *Control and Cybernetics*, 2(3), 99 – 106.

Mitchell, I. and Tomlin, C. (2003). Overapproximating reachable sets by hamilton-jacobi projections. *Journal of Scientific Computing*, 19, 323 – 346.

Raković, S., Kerrigan, E., Mayne, D., and Lygeros, J. (2006). Reachability analysis of discrete-time systems with disturbances. *IEEE Transactions on Automatic Control*, 51(4), 546 – 561.

Siciliano, B. and Khatlib, O. (2016). *Springer Handbook of Robotics*. Springer.

Tang, X., Tao, G., and Joshi, S.M. (2007). Adaptive actuator failure compensation for nonlinear MIMO systems with an aircraft control application. *Automatica*, 43, 1869 – 1883.

Tao, P.D. and An, L.T.H. (1997). Convex analysis approach to d.c. programming: Theory, algorithms and applications. *Acta Mathematica Vietnamica*, 22(1), 289 – 355.

Tuy, H. (1987). Global minimization of a difference of two convex functions. *Mathematical Programming Study*, 30, 150 – 182.

Vela, P.A., Morgansent, K.A., and Burdick, J.W. (2002). Underwater locomotion from oscillatory shape deformations. In *41st IEEE Conference on Decision and Control*, volume 2, 2074 – 2080.

Wang, W. and Wen, C. (2010). Adaptive actuator failure compensation control of uncertain nonlinear systems with guaranteed transient performance. *Automatica*, 46, 2082 – 2091.

Yu, J., Wang, C., and Xie, G. (2016). Coordination of multiple robotic fish with applications to underwater robot competition. *IEEE Transactions on Industrial Electronics*, 63(2), 1280 – 1288.

Yuille, A.L. and Rangarajan, A. (2003). The concave-convex procedure. *Neural Computation*, 15(4), 915 – 936.