Designing Resilient Linear Driftless Systems

Jean-Baptiste Bouvier and Melkior Ornik *

June 25, 2020

Abstract

Critical systems must be designed resilient to the loss of control authority over some of their actuators. This paper investigates the design of resilient linear systems capable of reaching their target even after one or multiple actuators started to produce uncontrolled and undesirable inputs. In contrast with the setting considered by robust control, where perturbations are unknown, we consider undesirable inputs produced by a faulty actuator belonging to the system and thus observed in real time. The control inputs can then depend on these undesirable inputs. Building on our previous work, we establish two novel sufficient conditions for resilient reachability. We then focus on designing resilient systems able to withstand the loss of one or multiple actuators. Since resiliency refers to the existence of a control law driving the state to the target, we naturally continue with the synthesis of such a control law. We conclude with a numerical application of our theory on the ADMIRE fighter jet model.

Index terms— Linear systems, Reachability analysis, Control design, Reliability, Redundancy.

I Introduction

Loss of control is the major factor behind fatal aircraft accidents [1]. That is why such critical systems must be able to operate safely even after sustaining actuator failures. This paper is a continuation of our initial work in [2] and discusses design of resilient systems able to withstand the loss of control authority over any actuator, and still be able to reach their initial target. Redundancy is the key to guarantee the resiliency of a system, as proven by NASA during the space race [3]. However, redundancy of subsystems does not always guarantee safety [4] as it increases the complexity of the overall system. Resiliency has also become a key issue in other fields like manufacturing [5] or integrated circuits [6]. In comparison with the bulk of such work specific to certain systems, our approach focuses on general linear systems.

*Jean-Baptiste Bouvier and Melkior Ornik are with the Department of Aerospace Engineering and the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA.
e-mail: bouvier3@illinois.edu & mornik@illinois.edu
This work was supported by an Early Stage Innovations grant from NASA's Space Technology Research Grants Program, grant no. 80NSSC19K0209.

Among the types of system malfunction, we specifically consider the *loss of control authority* over actuators. This setting has been introduced in [7] and refers to actuators becoming unmanageable and producing undesirable, uncontrolled outputs. For instance, a damaged rudder flapping in the wind produces undesirable outputs and it cannot be turned off like a defective engine. Such an actuator malfunction is not covered by the definition of actuator failure, which considers actuators performing with a reduced amplitude or with a fixed unknown magnitude and has been widely studied, e.g., [8, 9].

To handle systems enduring undesirable inputs, the field of robust control aims at guaranteeing *strong reachability*, i.e., finding a control driving the system state to the desired target for any perturbation, and has been widely studied by, e.g., [10, 11, 12, 13]. However, our setting of interest does not feature unknown generic 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 calling for a different type of reachability.

Namely, we say that a target 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. While not referring to it as resilient reachability, [14] and [15] considered this setting but developed complex algorithms stating whether a target is resiliently reachable or not. To design resilient systems, we need a deep understanding and intuition about resilient reachability that only an analytical theory can provide. The work of [16] transformed the problem of resilient reachability into a minimax optimization problem assessing whether a target set is reachable. Based on the latter work, [2] established simple reachability conditions for linear and mostly driftless systems. However, [2] did not investigate the resiliency of systems to the loss of control of any actuator.

As a first step towards a more general theory of resilient systems, the bulk of the results of this paper focuses on the case of driftless systems. Our objective is to design linear driftless systems resilient to the loss of control authority over some of their actuators. The contributions of this paper are fourfold. First, based on [2] we introduce the notion of resilient control matrices, and we derive straightforward verification criteria. Second, we investigate the minimal degree of overactuation necessary to design a resilient system. Third, we establish several methods to design resilient systems. Fourth, we synthesize a control law driving a resilient system's state to its target despite actuator failure.

The remainder of the paper is organized as follows. Section II defines the problems of interest and states the related definitions. In Section III we introduce the necessary preliminary results previously obtained in [2]. In Section IV we develop the notion of resilient control matrices and describe how to generate them. Section V focuses on the synthesis of a control law for resilient systems. We illustrate our theory in Section VI with three scenarios featuring a model of a fighter jet undergoing loss of control authority. In Appendix A we provide examples of resilient matrices with a low degree of overactuation. Appendix B gathers the technical details of the comparison between our approach and a robust control method.

Notation: The identity matrix of size n is denoted I_n. The transpose of a matrix M is $M^\top$, a positive semidefinite matrix is denoted by $M \succeq 0$ and a positive definite matrix by $M \succ 0$.

The eigenvalues of a square matrix M are gathered in $\lambda(M) := \{z : \det(zI - M) = 0\}$. The singular values of a matrix M are the $\sigma^M \geq 0$ such that $\det\left((\sigma^M)^2 I - M^\top M\right) = 0$, and $\sigma^M_{max} = \max\sqrt{\lambda(M^\top M)}$.

The vector e_i is composed of zeros except its i^{th} element is one. The column vector $z = (z_1, \ldots, z_n) \in \mathbb{R}^n$ has a norm $\|z\| = \sqrt{\sum z_i^2}$. We use $\langle \cdot, \cdot \rangle$ to denote the inner product between vectors.

The set of integers from 1 to n is denoted by $[n]$. The unit sphere in $\mathbb{R}^n$ is denoted by $\mathbb{U} = \left\{x \in \mathbb{R}^n : \|x\| = 1\right\}$, while $\mathbb{B}_X(c, \varepsilon) = \left\{x \in X : \|x - c\| \leq \varepsilon\right\}$ is the ball of center c and radius ε in the space X. The ellipsoid of center c and shape matrix $P \succ 0$ is $\mathcal{E}(c, P) = \left\{x : (x - c)^\top P(x - c) \leq 1\right\}$.

The space of square integrable functions $u : [0, T] \to \mathbb{R}^m$ is denoted by $\mathcal{L}_2\big([0, T],\ \mathbb{R}^m\big)$ or simply $\mathcal{L}_2$, and contains all functions with a finite $\mathcal{L}_2$-norm: $\|u\|^2 = \int_0^T \|u(t)\|^2 dt$.

Operators Tr and det respectively denote the trace and the determinant of a matrix. To obtain the real part of a complex number we use the operator $Re : \mathbb{C} \to \mathbb{R}$. The quantifiers $\exists$ and $\forall$ denote "there exists" and "for all", respectively. For $K \leq m \in \mathbb{N}$, we denote the number of K-combinations among m elements with the binomial coefficient $\binom{m}{K}$.

II Problem Statement

Consider a system governed by the differential equation

$$\dot{x} = Ax + \bar{B}\bar{u}, \qquad x(0) = x_0 \in \mathbb{R}^n, \tag{1}$$

where $A \in \mathbb{R}^{n\times n}$ and $\bar{B} \in \mathbb{R}^{n\times m}$ are constant matrices with n and $m \in \mathbb{N}$. Assume that the control specification is one of reachability. In other words, let $G \subset \mathbb{R}^n$ be the *target ball* of radius $\varepsilon \geq 0$ around $x_{goal} \in \mathbb{R}^n$ to be reached by the system. Assume that during its mission the system loses control authority over p of its m actuators, with $p \in [m]$. These p actuators are then producing uncontrolled and undesirable inputs. We can separate the controlled inputs $u \in \mathbb{R}^{m-p}$ from the undesirable inputs $w \in \mathbb{R}^p$ by writing $\bar{u} = (u^\top,\ w^\top)$ and $\bar{B} = [B\ C]$, with $B \in \mathbb{R}^{n\times(m-p)}$ and $C \in \mathbb{R}^{n\times p}$. The system's dynamics can thus be rewritten as follows:

$$\dot{x}(t) = Ax(t) + Bu(t) + Cw(t), \qquad x(0) = x_0 \in \mathbb{R}^n. \tag{2}$$

The technical work of this paper follows the assumptions of [2, 16] by considering square integrable inputs. Namely, if U is the set of admissible control laws and W is the set of undesirable inputs, we consider

$$\begin{aligned} U &= \left\{u \in \mathcal{L}_2\big([0, T],\ \mathbb{R}^{m-p}\big) : \|u\| \leq 1\right\} = \mathbb{B}_{\mathcal{L}_2}(0, 1), \\ W &= \left\{w \in \mathcal{L}_2\big([0, T],\ \mathbb{R}^p\big) : \|w\| \leq 1\right\} = \mathbb{B}_{\mathcal{L}_2}(0, 1), \\ G &= \left\{x \in \mathbb{R}^n : \|x - x_{goal}\| \leq \varepsilon\right\} = \mathbb{B}_{\mathbb{R}^n}(x_{goal}, \varepsilon). \end{aligned} \tag{3}$$

We want to determine what kind of system is still able to reach its target after a loss of control over some actuators. We can now define a *resilient system* as follows

Definition 1: The system $(A, \bar{B})$ following the dynamics (1) is *resilient* to the loss of control authority over the p actuators represented by C if for any target ball G and any undesirable input w, there exists a control law u_w that drives the system following (2) from x_0 to G.

We note that, as in [2], the control law u_w can depend on the undesirable input w. Unlike the concept of strong reachability in classical robust control [10, 11, 12, 13], the objective is not to a priori design a control law working for any perturbation, but instead to have a control law for each undesirable input. Since the undesirable inputs are generated by an actuator belonging to the system, we assume their real-time measurement is available to the controller. Therefore, resilient reachability guarantees that whatever the undesirable inputs are, there is a control law *dependent on the undesirable inputs* driving the system to its target. The intuitive expectation behind this dependency is that such a controller can handle undesirable inputs of a larger magnitude than a standard robust controller. We now formulate our three main objectives.

Problem 1: Establish necessary and sufficient conditions for a driftless system $\bar{B}$ to be resilient to the loss of any single or multiple actuators.

The work in [2] does not tackle resilient systems and thus is not completely addressing Problem 1. Since a resilient system can operate with fewer actuators than in its nominal configuration, we have the intuition that such a system must be initially *overactuated*.

Definition 2: A system is *overactuated* if the control matrix $\bar{B}$ has strictly more columns than rows.

Problem 2: Determine the minimal degree of overactuation required to build a resilient driftless system.

Since the definition of a resilient system calls for the existence of a control law, we are naturally led to our third objective.

Problem 3: For a resilient system sustaining an undesirable input w, synthesize a control law u_w that drives the system's state $x(t)$ to the target G.

We now introduce results previously proved in [2] that will be required to pursue the investigation of resilient reachability.

III Preliminaries

The first results obtained in [2] concern *resilient reachability at a certain time*.

Definition 3: The target G is *resiliently reachable at time* T from x_0 if for any undesirable inputs $w \in W$, there exists a control law $u_w \in U$ that drives the system following (2) to $x(T) \in G$.

In the case where the matrix B is invertible the problem of resilient reachability becomes trivial. Indeed, the control law $u_w = -B^{-1}Cw$ would completely counteract the undesirable

inputs. However, we are interested in general matrices B. We focus at first on *driftless* systems, i.e., where the state equation (2) becomes

$$\dot{x}(t) = Bu(t) + Cw(t), \qquad x(0) = x_0 \in \mathbb{R}^n. \tag{4}$$

For those systems, the work in [2] offers a straightforward expression to evaluate reachability at a certain time.

Theorem 1: G is resiliently reachable at time T from x_0 if and only if

$$\max_{h \in \mathbb{U}} \Big\{ \langle h, x_0 - x_{goal} \rangle - \sqrt{T} \left\| B^\top h \right\| + \sqrt{T} \left\| C^\top h \right\| \Big\} \leq \varepsilon.$$

The condition in Theorem 1 is simplified in [2] with the definitions of $d = x_0 - x_{goal}$ and of the function

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

Theorem 1 only states whether G is reached exactly at T. The situations where the target must instead be reached before a time limit, call for *resilient reachability by time T*.

Definition 4: The target G is *resiliently reachable by time T* if there exists a time $t \leq T$ at which G is resiliently reachable.

Then, [2] described reachability by time T as a minimax problem. The target G is resiliently reachable from x_0 by time T if and only if $\min\limits_{t \in [0,T]} \Big\{ \max\limits_{h \in \mathbb{U}} \big\{ J(h,t) \big\} \Big\} \leq \varepsilon$.
The function

$$g(h) := \|C^\top h\| - \|B^\top h\| \qquad \text{for } h \in \mathbb{U}, \tag{5}$$

leads to $J(h,t) = h^\top d + g(h)\sqrt{t}$. 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 $g(h)$.

Theorem 2: The following statements hold:

(a) If $\max\limits_{h \in \mathbb{U}} \big\{ g(h) \big\} < 0$, there exists a time t_{lim} such that G is resiliently reachable at time t for all $t \geq t_{lim}$.

(b) If $\max\limits_{h \in \mathbb{U}} \big\{ g(h) \big\} > 0$, there exists a time t_{lim} such that G is not resiliently reachable at time t for all $t > t_{lim}$.

(c) If $\max\limits_{h \in \mathbb{U}} \big\{ g(h) \big\} = 0$, the resilient reachability of G depends on the distance d.

The function g can be upper bounded with the maximal singular value of $C^\top$, denoted by $\sigma_{max}^{C^\top}$ and with the minimal singular value of $B^\top$, denoted by $\sigma_{min}^{B^\top}$.

Proposition 1: $\max\limits_{h \in \mathbb{U}} \big\{ g(h) \big\} \leq \sigma_{max}^{C^\top} - \sigma_{min}^{B^\top}$.

We have now summarized the results derived in [2] required to pursue our investigation. Before addressing Problem 1, we need to introduce two new results, a necessary and a sufficient condition for resilient reachability.

Theorem 3: For $F := BB^\top - CC^\top$, the following statements hold:

(a) If $F \succ 0$, there exists a time t_{lim} such that G is resiliently reachable at time t for all $t \geq t_{lim}$.

(b) If $F \not\succeq 0$, there exists a time t_{lim} such that G is not resiliently reachable at time t for all $t > t_{lim}$.

Proof: The statement (a) is equivalent to Theorem 2 (a):

$$\begin{aligned}
\max_{h \in \mathbb{U}} g(h) < 0 &\iff \forall\, h \in \mathbb{U}, \quad \|C^\top h\| - \|B^\top h\| < 0 \\
&\iff \forall\, h \in \mathbb{U}, \quad h^\top CC^\top h < h^\top BB^\top h \\
&\iff \forall\, h \in \mathbb{U}, \quad 0 < h^\top F h \\
&\iff \forall x \in \mathbb{R}^n \backslash \{0\}, \quad 0 < \frac{x^\top F x}{\|x\|^2} \\
&\iff \quad F \succ 0.
\end{aligned}$$

And similarly, statement (b) is equivalent to Theorem 2 (b):

$$\begin{aligned}
\max_{h \in \mathbb{U}} g(h) > 0 &\iff \exists\, h \in \mathbb{U} : \|C^\top h\| - \|B^\top h\| > 0 \\
&\iff \exists\, h \in \mathbb{U} : h^\top CC^\top h > h^\top BB^\top h \\
&\iff \exists\, h \in \mathbb{U} : h^\top F h < 0 \\
&\iff \quad F \not\succeq 0. \quad \blacksquare
\end{aligned}$$

The conditions of Theorem 3 are easier to verify than those of Theorem 2. We have thus obtained simple analytical conditions concerning the resilient reachability of a target. We are now able to tackle Problem 1.

IV Resilient Control Matrices

A driftless system is entirely described by its control matrix $\bar{B}$. Thus, our overarching idea is to link the resiliency of a driftless system to the properties of its control matrix.

When losing control authority over K of the m actuators of the system, we remove the corresponding columns $j_1, \ldots, j_K$ from $\bar{B}$ to form the matrix C and we name B the remaining control matrix. We can now define a *K-resilient control matrix*.

Definition 5: The control matrix $\bar{B} \in \mathbb{R}^{n \times m}$ is *K-resilient* if for all pairwise distinct $j_1, \ldots, j_K \in [m]$ the system following the driftless dynamics (4) can resiliently reach any target ball.

The *degree of resiliency* of the matrix $\bar{B}$ is the highest K for which $\bar{B}$ is K-resilient. Definition 5 implies that if a control matrix is K-resilient, then it is also (K-1)-resilient. On the other hand, if a control matrix is not K-resilient, then it is not (K+1)-resilient either.

IV.1 Necessary and sufficient conditions for K-resiliency

Based on our previous work, we derive two necessary and sufficient criteria to verify if a control matrix is resilient.

Proposition 2: The control matrix $\bar{B} \in \mathbb{R}^{n\times m}$ is K-resilient if and only if $\max\limits_{h \in \mathbb{U}} g(h) < 0$ for all pairwise distinct $j_1, \dots, j_K \in [m]$, with $g(h) = \|C^\top h\| - \|B^\top h\|$.

Proof: If $\max\limits_{h \in \mathbb{U}} g(h) < 0$ for all pairwise distinct indices $j_1, \dots, j_K \in [m]$, then from Theorem 2, any target ball is resiliently reachable by the system of dynamics (4), so $\bar{B}$ is K-resilient.

On the other hand, assume that $\bar{B}$ is K-resilient. For all pairwise distinct $j_1, \dots, j_K \in [m]$, the continuous function g reaches a maximum g_{max} over the compact set $\mathbb{U}$. If $g_{max} > 0$, then from Theorem 2 (b) after some time, any target ball becomes not resiliently reachable, which contradicts the resiliency of $\bar{B}$. If $g_{max} = 0$, then from Theorem 2 (c) there are some balls that are not resiliently reachable. It also contradicts the resiliency of $\bar{B}$. Therefore, $g_{max} < 0$. ■

Computing the maximum of each function g can be difficult. Thus, we employ Theorem 3 to simplify the result of Proposition 2. As previously, we create C by removing K columns from $\bar{B}$, indexed by $j_1, \dots, j_K$ and call B the remaining control matrix.

Proposition 3: The matrix $\bar{B}$ is K-resilient if and only if $F = BB^\top - CC^\top \succ 0$ for all pairwise distinct $j_1, \dots, j_K \in [m]$.

Proof: The result follows directly from Proposition 2 and the proof of Theorem 3. ■

Proposition 3 enables us to determine K-resiliency of a system with m actuators by verifying the positive definiteness of $\binom{m}{K}$ matrices. Before proceeding further, we need to establish a less obvious necessary condition for 1-resiliency.

Proposition 4: If $\bar{B}$ is 1-resilient, then $\bar{B}\bar{B}^\top \succ 0$.

Proof: Assume that $\bar{B}\bar{B}^\top$ is not positive definite. Then, there exists $x \neq 0$ such that $x\bar{B}\bar{B}^\top x \leq 0$. Without loss of generality, assume we remove the last column C from $\bar{B}$:

$$\bar{B}\bar{B}^\top = \begin{bmatrix} B & C \end{bmatrix} \begin{bmatrix} B^\top \\ C^\top \end{bmatrix} = BB^\top + CC^\top.$$

So $F = BB^\top - CC^\top = \bar{B}\bar{B}^\top - 2CC^\top$.
Then $x^\top F x = x^\top \bar{B}\bar{B}^\top x - 2x^\top CC^\top x \leq 0 - 2\|C^\top x\|^2 \leq 0$, so F is not positive semidefinite. By Proposition 3, $\bar{B}$ is not 1-resilient. ■

We have now addressed Problem 1, so we can start to think about Problem 2 and formalize our initial intuition about overactuation.

Proposition 5: If $\bar{B}$ is 1-resilient, then the system is overactuated.

Proof: Assume $\bar{B} \in \mathbb{R}^{n\times m}$ is not overactuated, then $m \leq n$. After losing control of one actuator, the remaining control matrix B has n rows and at most $n-1$ columns. From [17], the rank of a matrix is smaller than its smallest dimension, so $rank(B) \leq n-1$. The rank of a product of matrices is smaller than the rank of each of the matrices [17], so $rank(BB^\top) \leq rank(B)$. Thus, $rank(BB^\top) \leq n-1$.

Since $BB^\top$ is a square matrix of size n, it is not invertible. Then, $BB^\top$ is not positive definite, so $F = BB^\top - CC^\top$ is not positive definite either. According to Proposition 3, $\bar{B}$ is not 1-resilient. ■

It is intuitive that a system without redundancy among actuators cannot be resilient, because a malfunctioning actuator cannot be counteracted. On the other hand, if there are many copies of each actuator, then the system can lose control of one and still be functioning. In between these extremes there is a minimum degree of overactuation required for resiliency. Since adding actuators in practice comes with a cost, determining the minimal size of a resilient matrix can help reducing that cost.

IV.2 Resiliency invariant and SVD

The degree of resiliency of a matrix is left unchanged when applying some basic transformations. Determining those will help our study of the minimal size of a resilient matrix.

Proposition 6: The degree of resiliency is not affected by left multiplication by an invertible matrix.

Proof: Let $\bar{B}$ be a K-resilient control matrix, and P an invertible matrix of adequate size. The modified control matrix is $\bar{B}^P = P\bar{B}$. We extract K columns of $\bar{B}^P$ to create $B^P = PB$ and $C^P = PC$. Then,

$$\begin{aligned} F^P &= B^P\big(B^P\big)^\top - C^P\big(C^P\big)^\top \\ &= \big(PB\big)\big(PB\big)^\top - \big(PC\big)\big(PC\big)^\top \\ &= PBB^\top P^\top - PCC^\top P^\top = PFP^\top, \end{aligned}$$

with $F = BB^\top - CC^\top$. Because P is invertible, we know from [18] that $F \succ 0$ if and only if $F^P \succ 0$. Using Proposition 3, we conclude that $\bar{B}^P$ is also K-resilient. ■

We note that rotations, permutations of columns and non-zero scaling are all invertible operations, and thus do not change the degree of resiliency of a matrix. We can now simplify the resiliency investigation with the Singular Value Decomposition (SVD).

Let $\bar{B} \in \mathbb{R}^{n\times m}$. The compact SVD [19] of $\bar{B}$ is UDV, with U orthogonal of size $n \times n$, D a diagonal matrix gathering the n singular values of $\bar{B}$, and V of size $n \times m$ with orthonormal rows: $VV^\top = I$.

Proposition 7: The following statements hold for $K \geq 1$:

(a) If $\bar{B}$ is K-resilient, then V is also K-resilient.

(b) If V is K-resilient and $\bar{B}\bar{B}^\top \succ 0$, then $\bar{B}$ is K-resilient.

Proof: For statement (a), assume that $\bar{B}$ is K-resilient with $K \geq 1$. Then, Proposition 4 states that $\bar{B}\bar{B}^\top \succ 0$. Thus, the singular values of $\bar{B}$ are non-zero [19]. Then, the diagonal matrix D is invertible. The matrix U is orthogonal so it is also invertible. Therefore, $\bar{B} = UDV$ and V have the same degree of resiliency according to Proposition 6.

For statement (b), since $\bar{B}\bar{B}^\top \succ 0$, the matrix D is invertible. Then, by Proposition 6 the matrix $\bar{B}$ has the same degree of resiliency as V. ■

Since V has orthonormal rows, we proceed to study the K-resiliency of V instead of $\bar{B}$. Let C_V be any matrix formed with K columns taken from V, and B_V the associated remaining control matrix.

Proposition 8: The matrix $V \in \mathbb{R}^{n\times m}$ with orthonormal rows is K-resilient if and only if $\sigma_{max}^{C_V^\top} < \frac{1}{\sqrt{2}}$ for all $\binom{m}{K}$ possible C_V matrices.

Proof: We extract K columns from V to create B_V and C_V and we investigate whether $F_V := B_V B_V^\top - C_V C_V^\top$ is positive definite. Without loss of generality, $V = [B_V \ C_V]$, so that $VV^\top = B_V B_V^\top + C_V C_V^\top$. The matrix V has orthonormal rows: $VV^\top = I_n$. Then, $F_V = VV^\top - 2C_V C_V^\top = I_n - 2C_V C_V^\top$. Let λ be an eigenvalue of F_V. Then,

$$\begin{aligned} 0 &= \det\left(\lambda I_n - F_V\right) = \det\left(\lambda I_n - I_n + 2C_V C_V^\top\right) \\ &= \det\left((\lambda - 1)I_n + 2C_V C_V^\top\right) \\ &= \left(-2\right)^n \det\left(\left(\frac{1-\lambda}{2}\right) I_n - C_V C_V^\top\right). \end{aligned}$$

Let us define $s := \frac{1-\lambda}{2}$, so that s is an eigenvalue of $C_V C_V^\top$. Let $x \neq 0$ be an eigenvector such that $C_V C_V^\top x = sx$. A left multiplication by $x^\top$ lead to $\|C_V^\top x\|^2 = s\|x\|^2$, so $s \geq 0$.

Then, $\sqrt{s}$ is a singular value of $C_V^\top$. We note that $\lambda > 0$ if and only if $\sqrt{s} < \frac{1}{\sqrt{2}}$. Since $\sigma_{max}^{C_V^\top}$ is the maximal singular value of $C_V^\top$, $F_V \succ 0$ if and only if $\sigma_{max}^{C_V^\top} < \frac{1}{\sqrt{2}}$. ■

Propositions 7 and 8 greatly simplify the investigation of the minimal size of resilient matrices.

IV.3 1-resilient matrices

We will now establish a necessary condition determining the minimal size of a 1-resilient control matrix.

Theorem 4: If $\bar{B} \in \mathbb{R}^{n\times m}$ is 1-resilient, then $m \geq 2n + 1$.

Proof 1: Let $\bar{B} \in \mathbb{R}^{n\times m}$ be 1-resilient. We extract the column $i \in [m]$ from $\bar{B}$ to form C_i, while the remaining control matrix is called B_i.
We showed that $F_i = B_i B_i^\top - C_i C_i^\top = \bar{B}\bar{B}^\top - 2C_i C_i^\top$ in the proof of Proposition 4. Therefore,

$$\det(F_i) = \det\left(\bar{B}\bar{B}^\top - 2C_i C_i^\top\right).$$

We now employ the matrix determinant lemma [17]:

$$\det\left(\bar{B}\bar{B}^\top - 2C_i C_i^\top\right) = \left(1 - 2C_i^\top \left(\bar{B}\bar{B}^\top\right)^{-1} C_i\right) \det\left(\bar{B}\bar{B}^\top\right).$$

We sum the previous equations over $i \in [m]$ to obtain

$$\sum_{i=1}^{m} \det(F_i) = \det\left(\bar{B}\bar{B}^\top\right)\left(m - 2\sum_{i=1}^{m} C_i^\top \left(\bar{B}\bar{B}^\top\right)^{-1} C_i\right).$$

Now, note that

$$\begin{aligned}\sum_{i=1}^{m} C_i^\top \left(\bar{B}\bar{B}^\top\right)^{-1} C_i &= \sum_{i=1}^{m} (\bar{B}e_i)^\top \left(\bar{B}\bar{B}^\top\right)^{-1} \bar{B}e_i = \sum_{i=1}^{m} e_i^\top \bar{B}^\top \left(\bar{B}\bar{B}^\top\right)^{-1} \bar{B}e_i \\ &= Tr\left(\bar{B}^\top \left(\bar{B}\bar{B}^\top\right)^{-1} \bar{B}\right) = Tr\left(\bar{B}\bar{B}^\top \left(\bar{B}\bar{B}^\top\right)^{-1}\right) = Tr(I_n) = n.\end{aligned}$$

Therefore,

$$\sum_{i=1}^{m} \det(F_i) = \det\left(\bar{B}\bar{B}^\top\right)(m - 2n). \tag{6}$$

Following Proposition 4, we know that $\bar{B}\bar{B}^\top \succ 0$, so its determinant is positive. According to Proposition 3, we also have that for all $i \in [m]$, $\det(F_i) > 0$. Thus $m - 2n > 0$, i.e., $m \geq 2n + 1$. ■

We also present an alternate proof of this theorem making use of Propositions 7 and 8.

Proof 2: Similarly as in Proposition 7, we employ the compact SVD on $\bar{B} = UDV$. From the part (a) of Propositon 7 the matrix $V \in \mathbb{R}^{n \times m}$ is 1-resilient. The columns of V are denoted C_j and its orthonormal rows r_i. Then,

$$\sum_{j=1}^{m} \|C_j\|^2 = \sum_{j=1}^{m}\sum_{i=1}^{n} V_{ij}^2 = \sum_{i=1}^{n}\sum_{j=1}^{m} V_{ij}^2 = \sum_{i=1}^{n} \underbrace{\|r_i\|^2}_{=\,1} = n. \tag{7}$$

If $\max_j \|C_j\|^2 < \frac{n}{m}$, then it contradicts (7). From [18] we also know that the maximum singular value of a column vector is its norm. We combine these results with the condition of Proposition 8:

$$\frac{n}{m} \leq \max_j \|C_j\|^2 = \left(\sigma_{max}^{C^\top}\right)^2 < \frac{1}{2},$$

so $m \geq 2n + 1$ is a necessary condition for 1-resiliency. ■

Theorem 4 shows that at least $2n + 1$ actuators are required to have a 1-resilient control system in n dimensions. We will now prove that $n \times (2n + 1)$ is in fact the minimal size of 1-resilient matrices by producing such a matrix for all $n \in \mathbb{N}$.

Proposition 9: For any $n \in \mathbb{N}$, the matrix $\bar{B} = [I_n\ I_n\ D]$ with the column $D = \frac{1}{\sqrt{n}}[1 \ldots 1]^\top$ is 1-resilient.

Proof: We will use Theorem 2 and calculate $\max_{h\,\in\,\mathbb{U}} g(h)$ for the loss of any one actuator. First, assume we lose control of one of the first $2n$ columns. Without loss of generality, we assume

losing the column j of the first identity matrix, so $C = e_j$. Then for $h = (h_1, \ldots, h_n) \in \mathbb{U}$, we have

$$B^\top h = \left(h_1, \ldots, h_{j-1},\ h_{j+1}, \ldots, h_n,\ h^\top,\ \sum_{i=1}^{n} \frac{h_i}{\sqrt{n}} \right)^\top,$$

$$\text{so} \qquad \|B^\top h\|^2 = \sum_{i=1, \neq j}^{n} h_i^2 + \sum_{i=1}^{n} h_i^2 + \left(\sum_{i=1}^{n} \frac{h_i}{\sqrt{n}} \right)^2 = 2 \underbrace{\|h\|^2}_{=\,1} - h_j^2 + \frac{1}{n} \left(\sum_{i=1}^{n} h_i \right)^2.$$

$$\text{Then,} \qquad g(h) < 0 \iff \|C^\top h\|^2 < \|B^\top h\|^2 \iff h_j^2 < 2 - h_j^2 + \frac{1}{n} \left(\sum_{i=1}^{n} h_i \right)^2$$

$$\iff h_j^2 < 1 + \frac{1}{2n} \left(\sum_{i=1}^{n} h_i \right)^2. \tag{8}$$

If $h_j^2 = 1$, then $h_i = 0$ for all $i \neq j$ because $\|h\| = 1$. Thus $\sum h_i = 1$, so (8) is true. Otherwise, $h_j^2 < 1$ and (8) is also true. Thus, for any $h \in \mathbb{U}$, $g(h) < 0$.

The remaining case is when the system loses control of the last actuator. Then $B = [I_n\ I_n]$ and $C = D$. For any $h \in \mathbb{U}$,

$$g(h) = \left| \sum_{i=1}^{n} \frac{h_i}{\sqrt{n}} \right| - \sqrt{2}\|h\| \leq \frac{\sum |h_i|}{\sqrt{n}} - \sqrt{2}.$$

Using the Cauchy-Schwarz inequality [20], we obtain

$$\sum_{i=1}^{n} |h_i| \leq \sqrt{\sum_{i=1}^{n} |h_i|^2} \sqrt{\sum_{i=1}^{n} 1^2} = \|h\| \sqrt{n} = \sqrt{n}.$$

Then $g(h) \leq 1 - \sqrt{2} < 0$. Therefore, in both cases $\max\limits_{h\ \in\ \mathbb{U}} g(h) < 0$. From Proposition 2, the control matrix $\bar{B}$ is 1-resilient. ■

To sum up, we showed that the minimal size of a 1-resilient control matrix is $n \times (2n+1)$. We will now investigate sufficient conditions allowing to generate 1-resilient control matrices by making use of Proposition 8.

Proposition 10: Any matrix $V \in \mathbb{R}^{n \times m}$ where $m \geq 2n + 1$ which has orthonormal rows and whose columns have all the same norm, is 1-resilient.

Proof: Since the columns C of matrix V have the same norm, equation (7) implies $\|C\|^2 = \frac{n}{m}$. The maximal singular value of a column vector is its norm [18], so $\sigma_{max}^{C^\top} = \|C\| = \sqrt{\frac{n}{m}}$. Since $m \geq 2n + 1$, we obtain

$$\frac{n}{m} \leq \frac{1}{2} - \frac{1}{2m} < \frac{1}{2}, \quad \text{i.e.,} \quad \sigma_{max}^{C^\top} < \frac{1}{\sqrt{2}}.$$

Then, Proposition 8 states that V is 1-resilient. ■

Intuitively, the columns of V having the same norm means that the actuators are equally powerful, whereas the rows having the same norm means that all the states are equally actuated. Furthermore, the orthogonality of rows enforces the necessary condition for 1-resiliency of Proposition 4 by making $VV^\top$ positive definite.

With Proposition 10 we can now easily generate 1-resilient matrices for any size n. For instance,

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \end{bmatrix} \quad \text{are 1-resilient.}$$

We now wish to expand our minimal size investigation to higher degrees of resiliency.

IV.4 Higher degree of resiliency

We first generalize Proposition 9 to K-resiliency. Let us define the matrices $\bar{B}_p = [I_n \dots I_n \; D]$ composed of p identity matrices and a column vector $D = \frac{1}{\sqrt{n}}[1 \dots 1]^\top$.

Proposition 11: The matrix $\bar{B}_{2K}$ is K-resilient.

Proof: We calculate $\max\limits_{h \,\in\, \mathbb{U}} g(h)$ for all possible losses of K actuators.

First, assume the system loses control of K columns belonging all to the identity matrices. Without loss of generality we assume losing one column per matrix. The index of the column lost in the i^{th} identity matrix is $j_i \in [n]$. These columns form the matrix $C = \big[e_{j_1} \dots e_{j_K}\big]$, while B is the remaining control matrix. Then, for $h = \big(h_1, \dots, h_n\big) \in \mathbb{U}$, we have

$$C^\top h = \big(h_{j_1}, \dots, h_{j_K}\big) \quad \text{so} \quad \|C^\top h\|^2 = \sum_{i=1}^{K} h_{j_i}^2,$$

$$\|B^\top h\|^2 = 2K \sum_{i=1}^{n} h_i^2 - \sum_{i=1}^{K} h_{j_i}^2 + \left(\sum_{i=1}^{n} \frac{h_i}{\sqrt{n}} \right)^2 = 2K - \sum_{i=1}^{K} h_{j_i}^2 + \frac{1}{n} \left(\sum_{i=1}^{n} h_i \right)^2.$$

From (5) we have $g(h) = \|C^\top h\| - \|B^\top h\|$. Then,

$$\begin{aligned} g(h) < 0 &\iff \sum_{i=1}^{K} h_{j_i}^2 < 2K - \sum_{i=1}^{K} h_{j_i}^2 + \frac{1}{n} \left(\sum_{i=1}^{n} h_i \right)^2 \\ &\iff \sum_{i=1}^{K} h_{j_i}^2 < K + \frac{1}{2n} \left(\sum_{i=1}^{n} h_i \right)^2. \end{aligned} \tag{9}$$

If $j_1 = \dots = j_K$, and $h = e_{j_1}$, then (9) simplifies into $K < K + \frac{1}{2n}$, which is true. In all other cases, the left hand side of (9) is strictly smaller than K, so the inequality also holds true. Overall $g(h) < 0$ for all $h \in \mathbb{U}$ and all choice of columns $j_1, \dots, j_K \in [n]$.

The other possible case is when $\bar{B}_{2K}$ loses $K-1$ columns among the identity matrices and the last column D. Then,

$$g(h) = \sqrt{\sum_{i=1}^{K-1} h_{j_i}^2 + \frac{1}{n}\left(\sum_{i=1}^{n} h_i\right)^2} - \sqrt{2K - \sum_{i=1}^{K-1} h_{j_i}^2}\ .$$

Since $\|h\| = 1$, $h_{j_i}^2 \leq 1$ for all $i \in [K\text{-}1]$. We use the Cauchy-Schwarz inequality [20]

$$\left(\sum_{i=1}^{n} h_i\right)^2 \leq \left(\sum_{i=1}^{n} h_i^2\right)\left(\sum_{i=1}^{n} 1^2\right) = \|h\|^2\ n = n.$$

Then,

$$g(h) \leq \sqrt{K - 1 + \frac{1}{n}n} - \sqrt{2K - (K-1)} \leq \sqrt{K} - \sqrt{K+1} < 0.$$

Therefore, in both cases $\max\limits_{h\ \in\ \mathbb{U}} g(h) < 0$. Proposition 2 then states that $\bar{B}_{2K}$ is K-resilient. ■

We can also extend Proposition 10 to 2-resilient matrices with a consequential increase in the calculations required.

Proposition 12: Any matrix $V \in \mathbb{R}^{n\times m}$ where $m \geq 4n+1$ which has orthonormal rows and whose columns have all the same norm, with at least two columns being collinear, is 2-resilient.

Proof: Similarly as in the proof of Proposition 10 the columns have a squared norm of $\|C\|^2 = \frac{n}{m}$. We extract any two columns C_1 and C_2 from V to form C, the remaining part of V is named B. Since $C = \begin{bmatrix} C_1\ C_2 \end{bmatrix}$, we have $CC^\top = C_1C_1^\top + C_2C_2^\top$.

The singular values $\sigma^{C^\top}$ of $C^\top$ are defined as the square roots of the eigenvalues s of $CC^\top$. Therefore we calculate $s = \left(\sigma^{C^\top}\right)^2$ to use Proposition 8. From the matrix determinant lemma [17],

$$\begin{aligned} 0 &= \det\left(sI_n - CC^\top\right) = \det\left(sI_n - C_1C_1^\top - C_2C_2^\top\right) \\ &= \left(1 - C_2^\top\left(sI_n - C_1C_1^\top\right)^{-1}C_2\right)\det\left(sI_n - C_1C_1^\top\right). \end{aligned}$$

If $\det\left(sI_n - C_1C_1^\top\right) = 0$, then the resulting eigenvalue is either 0 or $\|C_1\|^2 = \frac{n}{m}$ by [18]. To investigate when the other term goes to zero, we develop the inverse into a Neumann series [18] for s such that $\left\|\frac{C_1C_1^\top}{s}\right\| < 1$:

$$\begin{aligned} s\left(sI_n - C_1C_1^\top\right)^{-1} &= \left(I_n - \frac{C_1C_1^\top}{s}\right)^{-1} = \sum_{p=0}^{\infty}\left(\frac{C_1C_1^\top}{s}\right)^p \qquad (10) \\ &= I + \sum_{p=1}^{\infty}\frac{1}{s^p}C_1\left(C_1^\top C_1\right)^{p-1}C_1^\top = I + \frac{C_1C_1^\top}{s}\sum_{p=1}^{\infty}\left(\frac{\|C_1\|^2}{s}\right)^{p-1} \\ &= I + \frac{C_1C_1^\top}{s}\frac{1}{1 - \frac{\|C_1\|^2}{s}} = I + \frac{C_1C_1^\top}{s - \|C_1\|^2}. \end{aligned}$$

$$\text{Then,} \quad \left(1 - C_2^\top \left(sI_n - C_1C_1^\top\right)^{-1} C_2\right) = 0 \iff s = C_2^\top s\left(sI_n - C_1C_1^\top\right)^{-1} C_2$$
$$\iff C_2^\top \left(I + \frac{C_1C_1^\top}{s - \|C_1\|^2}\right) C_2 = s = \|C_2\|^2 + \frac{\left(C_1^\top C_2\right)^2}{s - \|C_1\|^2}$$
$$\iff s^2 - \left(\|C_1\|^2 + \|C_2\|^2\right)s + \|C_1\|^2\|C_2\|^2 - \left(C_1^\top C_2\right)^2 = 0.$$

Recall that $\|C_1\|^2 = \|C_2\|^2 = \frac{n}{m}$. Then the previous equation becomes

$$s^2 - \frac{2n}{m}s + \frac{n^2}{m^2} - \left(C_1^\top C_2\right)^2 = 0.$$

The maximal root of this quadratic equation is

$$s_{max} = \frac{n}{m} + \left|C_1^\top C_2\right|. \tag{11}$$

This expansion is only valid for the case where s satisfies $\left\|\frac{C_1C_1^\top}{s}\right\| < 1$. We note that $\|C_1C_1^\top\| = \lambda_{max}(C_1C_1^\top) = \|C_1\|^2 = \frac{n}{m}$, from [18]. Therefore, in the other case $s \leq \frac{n}{m}$. From (11) we deduce that s_{max} is the maximal eigenvalue of $CC^\top$.

The matrix C maximizing s_{max} is the one composed of two collinear columns of V. Indeed, by the Cauchy-Schwarz inequality $\left|C_1^\top C_2\right| \leq \|C_1\|\,\|C_2\|$, and the equality only happens when C_1 and C_2 are collinear. In that case, $s_{max} = \frac{2n}{m}$.

Then, the resiliency condition of Proposition 8 is equivalent to $2s_{max} < 1$, i.e., $m \geq 4n+1$. Thus, V is 2-resilient. ■

Note that two collinear columns of same norm are either the same or opposites. Proposition 12 thus deals with the case where at least one actuator of the system is doubled.

With the guidelines provided by Proposition 12 we produce an example of a 2-resilient matrix V of size 2×10:

$$V = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \end{bmatrix}.$$

With Proposition 11 we can generate K-resilient matrices of size $n \times (2Kn + 1)$. For $K = 1$ it corresponds to $n \times (2n + 1)$, which is the minimal size for 1-resilient matrices. For $K = 2$, we obtain a matrix with $4n + 1$ columns, which is consistent with the minimal size detailed in Proposition 12.

In order to determine the minimal size of a K-resilient matrix, with $K \geq 2$, the only missing result is an equivalent of Theorem 4 for higher degrees of resiliency.

However, the process employed in the first proof of Theorem 4 does not scale well with the degree of resiliency. Indeed, the fact that $\sum \det(F_i) = 0$, when $m = 2n$ cannot be generalized to $K \geq 2$.

As for the second proof, the calculations are already significantly more complex for $K = 2$ as can be seen in the proof of Proposition 12. Without the assumption of same column norm for the case $K = 2$ the calculations do not even reach a conclusion. For $K \geq 3$, the calculations become even more cumbersome. The Neumann series (10) becomes

$$s\left(sI_n - \sum_{j=1}^{K-1} C_jC_j^\top\right)^{-1} = \sum_{p=0}^{\infty}\left(\sum_{j=1}^{K-1} \frac{C_jC_j^\top}{s}\right)^p.$$

We would then need the multinomial formula to calculate each term of the series:

$$\left(\sum_{j=1}^{K-1} C_j C_j^\top\right)^p = \sum_{i_1+\ldots+i_{K-1}=p} \binom{p}{i_1, \ldots, i_{K-1}} \prod_{j=1}^{K-1} \left(C_j C_j^\top\right)^{i_j}.$$

Proceeding to the separation of $\left(C_j C_j^\top\right)^{i_j}$ into a scalar part with the power $i_j - 1$ and a matrix part like we did for $K = 2$ is still possible but brings numerous cross-terms that did not appear for $K = 2$. Because of the complexity of the calculations for $K \geq 2$, we were unable to obtain a simple necessary condition on the minimal size of such K-resilient matrices.

Remark: If we based our intuition about the minimal size of K-resilient matrices on Theorem 4 and on Proposition 11, then we might conjecture a minimal size of $n \times (2Kn + 1)$ for K-resilient matrices $\bar{B}$.

Such a conjecture holds for 2-resilient matrices with a state dimension $n = 1$. Indeed, let us consider $\bar{B} = \begin{bmatrix} b_1 & b_2 & b_3 & b_4 \end{bmatrix}$. Without loss of generality, assume that b_3 and b_4 have a greater absolute value than b_1 and b_2. When losing control of the last two columns we form $B = \begin{bmatrix} b_1 & b_2 \end{bmatrix}$ and $C = \begin{bmatrix} b_3 & b_4 \end{bmatrix}$. Then, $F = BB^\top - CC^\top = b_1^2 + b_2^2 - b_3^2 - b_4^2 \leq 0$. Therefore, there are no 2-resilient matrices of size 1×4. The minimal size of a 2-resilient matrix for $n = 1$ is then 1×5, since $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \end{bmatrix}$ is 2-resilient.

However, we are able to generate 2-resilient matrices of size $n \times 4n$ for $n = 6$ and $n = 8$, and even of size $n \times (4n - 2)$ for $n = 12$. Since these matrices are of consequent size, they can be found in the Appendix A. We will now provide the intuition that led us to these counterexamples.

We consider a matrix $V \in \mathbb{R}^{n \times m}$ with orthogonal rows whose only elements are ± 1. Obviously, all columns have the same norm: $\|C\|^2 = n$, and the maximal singular value of $CC^\top$ defined in (11) becomes $s_{max} = \left|C_1^\top C_2\right| + n$, with the notations from the proof of Proposition 12. To build a 2-resilient matrix of minimal size, we need to minimize s_{max}. Indeed, for these matrices the resiliency condition of Proposition 8 becomes $2s_{max} < m$. For a small s_{max}, we should then be able to have a small number m of columns. To minimize s_{max}, V should not have any collinear columns, because they would maximize the scalar product $\left|C_1^\top C_2\right|$, as seen in the proof of Proposition 12.

There are 2^n different vectors composed of n elements ± 1. These vectors are only collinear with the vector of opposite sign. Thus, there are 2^{n-1} of such non-collinear vectors. To build a matrix with $4n$ columns, we then require $2^{n-1} \geq 4n$. The minimal dimension realizing that condition is $n = 6$. We believe that it is impossible to build a 2-resilient matrix of $4n$ columns for $n \leq 5$.

We propose two ways of generating a 2-resilient matrix with $4n$ columns for $n \geq 6$. The first approach consists in producing all the non-collinear vectors and then selecting $4n$ of them to create a matrix with orthogonal rows. With this approach, we were able to produce a 2-resilient matrix of size 6×24, as can be seen in Appendix A.

The other approach uses the Hadamard matrices [21]. They are square and orthogonal matrices composed of only ± 1. By carefully selecting n rows of a $4n \times 4n$ Hadamard matrix, it is possible to have $4n$ non-collinear columns. We extracted 8 chosen rows of a 32×32 Hadamard matrix and we built a 2-resilient matrix of minimal size 8×32 in Appendix A.

In order to generate a 2-resilient matrix with an even lower degree of overactuation, the maximal scalar product in (11) must be made even smaller. We succeeded by taking $n = 12$ and selecting n partial rows from a $4n \times 4n$ Hadamard matrix in order to obtain a 2-resilient matrix of size $n \times (4n - 2)$ presented in the Appendix A.

Therefore the above conjecture is wrong. Its demise also explains why the proof of Theorem 4 cannot be extended to higher degrees of resiliency.

It is now time to tackle Problem 3, the generation of a control law for resilient systems.

V Control synthesis

The definition of resilient reachability asks for the existence of a control law. A natural follow-up question is thus one of designing such a control law. For a driftless resilient system following the state equation $\dot{x}(t) = Bu(t) + Cw(t)$, we want u to drive the state to the target in spite of the undesirable input w. As noted at the beginning of the paper, if matrix B was invertible, the control law $u = -B^{-1}Cw$ would cancel w. However, B might not even be a square matrix. Instead, we design the control law using the Moore-Penrose pseudo-inverse of B [18]. An additional challenge in generating the adequate control law is to ensure that for all $w \in W$, the control u stays in its set U. To do so, we make use of the resilient reachability conditions previously established and require the positive definiteness of $F = BB^\top - CC^\top$.

Theorem 5: If $F \succ 0$, then there exists $\alpha > 0$ such that

$$u(t) := B^\top \big(BB^\top\big)^{-1}\Big(- Cw(t) + \alpha\big(x_{goal} - x(t)\big)\Big) \tag{12}$$

drives the resilient system (4) to its target ball G, and $u \in U$ for any $w \in W$.

Proof: We need to prove that u is well-defined, stays in U at all time and drives the system to the target. We assumed that measurements of the undesirable inputs are available in real-time and the state is completely observable, so the controller has access to $w(t)$ and $x(t)$. Since $F = BB^\top - CC^\top \succ 0$, obviously $BB^\top \succ 0$, so $BB^\top$ is invertible, and the control law is well-defined.

If we plug the control law (12) into the state equation (4) we obtain

$$\begin{aligned}\dot{x} &= BB^\top \big(BB^\top\big)^{-1}\Big(- Cw + \alpha\big(x_{goal} - x\big)\Big) + Cw \\ &= \alpha\big(x_{goal} - x\big).\end{aligned}$$

The solution is $x(t) = x_{goal} + e^{-\alpha t}d$, with $d = x(0) - x_{goal}$. Since $\alpha > 0$, the state x converges globally exponentially to the target. Therefore, the control law is successful.

We need to prove that for all $w \in W$, we have $u \in U$, i.e., that $\|u\|_{\mathcal{L}_2} \leq 1$. Note that $x_{goal} - x(t) = -e^{-\alpha t}d$, and define $v(t) := Cw(t) + \alpha e^{-\alpha t}d$, so that $u(t) = -B^\top \big(BB^\top\big)^{-1} v(t)$.

Then,

$$\begin{aligned}\|u\|_{\mathcal{L}_2}^2 &= \int_0^T \|u(t)\|_{\mathbb{R}^m}^2 dt = \int_0^T u(t)^\top u(t)\ dt \\ &= \int_0^T v(t)^\top \big(BB^\top\big)^{-\top} B\ B^\top \big(BB^\top\big)^{-1} v(t)\ dt \\ &= \int_0^T v(t)^\top \big(BB^\top\big)^{-1} v(t)\ dt.\end{aligned}$$

To simplify, let $P := \big(BB^\top\big)^{-1} \succ 0$, and expand $v(t)$ as

$$\begin{aligned}v(t)^\top P v(t) &= \underbrace{w(t)^\top C^\top P C w(t)}_{=\ T_1} + \underbrace{w(t)^\top C^\top P \alpha e^{-\alpha t} d}_{=\ T_2} + \underbrace{\alpha e^{-\alpha t} d^\top P C w(t)}_{=\ T_3} + \underbrace{\alpha^2 d^\top e^{-\alpha t} P e^{-\alpha t} d}_{=\ T_4} \\ &= T_1 + T_2 + T_3 + T_4. \end{aligned} \tag{13}$$

The first term T_1 is the most complicated to bound. From the Woodbury formula [18], we learn that $\big(I + C^\top F^{-1} C\big)$ is invertible, and we simplify the inverse of $BB^\top = F + CC^\top$. Since F is invertible,

$$P = \big(F + CC^\top\big)^{-1} = F^{-1} - F^{-1} C \big(I + C^\top F^{-1} C\big)^{-1} C^\top F^{-1}.$$

Now we define $D := C^\top F^{-1} C$. Then, $C^\top P C = D - D\big(I + D\big)^{-1} D$.
By expanding $\big(I + D\big)^{-1}\big(I + D\big) = I$, we easily obtain $\big(I + D\big)^{-1} D = I - \big(I + D\big)^{-1}$, so that

$$C^\top P C = D - D + D\big(I + D\big)^{-1}.$$

Similarly, from $\big(I + D\big)\big(I + D\big)^{-1} = I$, we finally obtain $C^\top \big(BB^\top\big)^{-1} C = I - \big(I + D\big)^{-1}$.
Let λ be an eigenvalue of $C^\top \big(BB^\top\big)^{-1} C$. Then

$$\begin{aligned}0 &= \det\big(\lambda I - C^\top \big(BB^\top\big)^{-1} C\big) = \det\big(\lambda I - I + \big(I + D\big)^{-1}\big) \\ &= \det\big((\lambda - 1)(I + D)(I + D)^{-1} + I(I + D)^{-1}\big) \\ &= \det\big((\lambda - 1)(I + D) + I\big) \det(I + D)^{-1}.\end{aligned}$$

From the Woodbury formula we know that $(I + D)$ is invertible, so $\det(I + D))^{-1} \neq 0$. If $\lambda = 1$, then $\det(I) = 0$, which is absurd. Thus $\lambda \neq 1$, so we can divide by $(\lambda - 1)$:

$$0 = \det\Big(I + D + \frac{1}{\lambda - 1} I\Big) = \det\Big(\frac{\lambda}{\lambda - 1} I + D\Big) = (-1)^m \det\Big(\frac{-\lambda}{\lambda - 1} I - D\Big).$$

Since D is symmetric, its eigenvalues are nonnegative, so $\frac{-\lambda}{\lambda - 1} \geq 0$. Since $C^\top \big(BB^\top\big)^{-1} C$ is also symmetric, $\lambda \geq 0$. Therefore $\lambda - 1 < 0$, i.e. $\lambda < 1$. Define $\lambda_M < 1$ as the maximal eigenvalue of $C^\top \big(BB^\top\big)^{-1} C$. Then,

$$\int_0^T T_1 dt = \int_0^T w(t)^\top C^\top \big(BB^\top\big)^{-1} C w(t)\ dt \leq \int_0^T w(t)^\top \lambda_M w(t)\ dt = \lambda_M \|w\|_{\mathcal{L}_2}^2 \leq \lambda_M. \tag{14}$$

We can now tackle the integral of the second term of (13):

$$\int_0^T T_2 \, dt = \int_0^T \alpha w(t)^\top C^\top P e^{-\alpha t} d \, dt = \alpha \int_0^T w(t)^\top e^{-\alpha t} \, dt \; C^\top P d. \tag{15}$$

Then, we calculate the norm of the integral term in (15) and use the Cauchy-Schwarz inequality to bound it:

$$\begin{aligned}\left|\left|\int_0^T w(t)^\top e^{-\alpha t} dt\right|\right|_{\mathbb{R}^m} &= \sqrt{\sum_{i=1}^m \left(\int_0^T w_i(t) e^{-\alpha t} dt\right)^2} \leq \sqrt{\sum_{i=1}^m \left(\int_0^T w_i^2(t) dt\right)\left(\int_0^T e^{-2\alpha t} dt\right)} \\ &\leq \sqrt{\left[\frac{e^{-2\alpha t}}{-2\alpha}\right]_0^T \int_0^T \sum_{i=1}^m w_i^2(t) dt} \;=\; \sqrt{\frac{1-e^{-2\alpha T}}{2\alpha}} \, \|w\|_{\mathcal{L}_2}.\end{aligned}$$

Thus,

$$\int_0^T T_2 \, dt \leq \sqrt{\frac{\alpha}{2}} \|C^\top P d\| \, \|w\|_{\mathcal{L}_2}. \tag{16}$$

The same process is applied to T_3, and results in the same upper bound:

$$\int_0^T T_3 \, dt \leq \sqrt{\frac{\alpha}{2}} \|d^\top P C\| \, \|w\|_{\mathcal{L}_2}. \tag{17}$$

We also simplify the integral of the fourth term of (13):

$$\begin{aligned}\int_0^T T_4 &= \int_0^T \alpha^2 d^\top e^{-\alpha t} P e^{-\alpha t} d \, dt = \alpha^2 d^\top P d \int_0^T e^{-2\alpha t} \, dt = \alpha^2 d^\top P d \left[\frac{e^{-2\alpha t}}{-2\alpha}\right]_0^T \\ &= \frac{\alpha}{2} d^\top P d\big(1 - e^{-2\alpha T}\big) \leq \frac{\alpha}{2} \, d^\top P d.\end{aligned} \tag{18}$$

Then, we combine (14), (16), (17) and (18):

$$\|u\|_{\mathcal{L}_2}^2 \;\leq\; \frac{\alpha}{2} \, d^\top P d + 2\sqrt{\frac{\alpha}{2}} \|C^\top P d\| + \lambda_M. \tag{19}$$

Since $\lambda_M < 1$, and d, P and C are constant, we can choose α small enough so that the right hand side of (19) is smaller than 1, which finally leads to $\|u\|_{\mathcal{L}_2}^2 \leq 1$, i.e. $u \in U$. ■

The proof of Theorem 5 provides a constructive method of finding α satisfying the claim of the theorem. For instance, an appropriate α is given by

$$\alpha = 2 \, \frac{\left(\sqrt{b^2 + (1-\lambda_M)a} - b\right)^2}{a^2}, \qquad \text{with} \quad a = d^\top P d \quad \text{and} \quad b = \|C^\top P d\|. \tag{20}$$

Theorem 5 gives an intuitive validation of the work developed in the previous sections. Indeed, we established that resilient reachability implies $F \succ 0$. From Theorem 5, we see that such a condition is indeed sufficient to build a control law of the form (12).

The positive definiteness of F brings two results. The part $BB^\top \succ 0$ guarantees the existence of u. But $BB^\top$ is more than just positive definite, in fact $BB^\top \succ CC^\top$ with a slight abuse of notation. This relation ensures that u of the form (12) remains within the bounds of U even when w is maximal.

We finally briefly return to a general system (2) with possible drift. We will show that the same control law as in the driftless case can be used if the natural dynamics $\dot{x} = Ax$ are not overly unstable. The intuition is that the magnitude of u exceeds w, and that excess of magnitude can be used to counteract instability to a certain extent. We formalize our intuition in Theorem 6.

First, let us introduce the set

$$\mathcal{A} := \Big\{\alpha > 0 : \ \frac{\alpha}{2} d^\top P d + \sqrt{2\alpha}\|C^\top P d\| \leq 1 - \lambda_M\Big\}, \tag{21}$$

with $\lambda_M = \max\big(\lambda(C^\top \big(BB^\top\big)^{-1} C)\big) < 1$. Set $\mathcal{A}$ is non-empty, as explained at the end of the proof of Theorem 5. Since $d = x(0) - x_{goal}$, the case $d = 0$ implies that the system starts at the target and no control law is needed. Otherwise, $d \neq 0$ and $P = \big(BB^\top\big)^{-1} \succ 0$ whenever $F \succ 0$. Therefore, $d^\top P d > 0$, so the set $\mathcal{A}$ is bounded from above if $F \succ 0$. We can now define $\alpha^* := \max \mathcal{A}$, and easily compute it from (20).

Theorem 6: If $F \succ 0$ and if $\max(Re(\lambda(A))) < \alpha^*$, then the control law

$$u(t) := B^\top \big(BB^\top\big)^{-1}\Big(- Cw(t) + \alpha^*\big(x_{goal} - x(t)\big)\Big)$$

drives the resilient system (2) to its target ball G, and $u \in U$ for any $w \in W$.

Proof: For the same reasons as in the proof of Theorem 5, u is well-defined, and $u \in U$ because $\alpha^* \in \mathcal{A}$. The only difference concerns the effect of the control law on the trajectory. Indeed, when plugging (12) into (2), we obtain:

$$\dot{x} = Ax + \alpha(x_{goal} - x) = (A - \alpha I)x + \alpha x_{goal}.$$

Thus, $x(t) = x_{goal} + e^{(A-\alpha I)t}$. Then, the state converges towards x_{goal} if and only if $\max(Re(\lambda(A - \alpha I))) < 0$, i.e., if $\alpha > \max(Re(\lambda(A)))$. And $u \in U$ if and only if $\alpha \leq \alpha^*$. ■

Note that the value of α^* depends on d, the distance between the initial state and the target. Therefore, the further away the target is, the less instability can be counteracted by the control law. If the system is overly unstable, i.e., $\alpha^* < \max(Re(\lambda(A)))$, then the proposed control law cannot drive the state to the target.

From Theorem 6 we can easily derive a sufficient condition for resiliency and confirm our intuition about stable systems.

Corollary: If A is Hurwitz and $\bar{B}$ is K-resilient, then the system $\dot{x} = Ax + \bar{B}u$ is also K-resilient.

Proof: Since $\bar{B}$ is K-resilient, we can remove any K columns of $\bar{B}$ and have $F \succ 0$. We choose a target ball G. As in the proof of Theorem 6, the set (21) has a maximal bound $\alpha^* > 0$. Since A is Hurwitz, its eigenvalues have a negative real part, so $\alpha^* > \max(Re(\lambda(A)))$. Thus, the control law (12) drives the state to the target ball. Therefore, the system is also K-resilient. ■

We have here obtained a simple resiliency condition for non-driftless systems. We now proceed to computationally confirm the above theoretical results.

VI Numerical example

To validate our theory, we consider the ADMIRE fighter jet model developed by the Swedish Defense Research Agency [22]. The ADMIRE model has already served as an application case in several control frameworks [23], [24].

We explore three different scenarios featuring the fighter jet. First, we investigate the resiliency of the simplified model used in [23]. We also use this model as a benchmark to compare our approach with a robust control method. We finally study the resiliency of a more advanced driftless dynamics model of the aircraft.

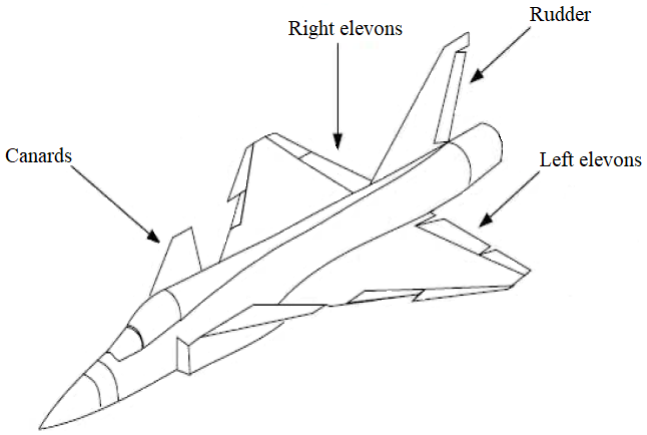

Figure 1: The ADMIRE fighter jet model. Image modified from [24].

VI.1 Resiliency of a fighter jet

We consider only four of the actuators of the jet: the canard, the left and right elevons and the rudder, as depicted on Figure 1. With these control surfaces, the pilot can directly affect the angular acceleration in roll, pitch and yaw.

The nominal linearized dynamics of the jet established in [23] are $\dot{x} = Ax + \bar{B}u$, with the state vector x gathering the angular velocities in roll, pitch and yaw (rad/s):

$$x = \begin{bmatrix} p \\ q \\ r \end{bmatrix} \qquad A = \begin{bmatrix} -0.9967 & 0 & 0.6176 \\ 0 & -0.5057 & 0 \\ -0.0939 & 0 & -0.2127 \end{bmatrix}$$

$$\bar{B} = \begin{bmatrix} 0 & -4.2423 & 4.2423 & 1.4871 \\ 1.6532 & -1.2735 & -1.2735 & 0.0024 \\ 0 & -0.2805 & 0.2805 & -0.8823 \end{bmatrix}.$$

Note that the system is naturally stable: the eigenvalues of A have negative real parts. The inputs of the system are the deflections of the control surfaces: u_c for the canard wings, u_{re} and u_{le} for the right and left elevons, and u_r for the rudder. They are mechanically

constrained:

$$u = \begin{bmatrix} u_c \\ u_{re} \\ u_{le} \\ u_r \end{bmatrix} \quad \text{with} \quad \begin{array}{c} u_c \in [-25, 55]\frac{\pi}{180}, \\ u_{re}, u_{le}, u_r \in [-30, 30]\frac{\pi}{180}. \end{array} \tag{22}$$

Consider the scenario in which, after sustaining damage (e.g., during air combat), one of the control surfaces of the fighter jet stops responding to the commands. This surface is now producing undesirable inputs. The pilot wants to minimize the aircraft roll, pitch and yaw rates, so the target is a ball of radius 0.1 centered around the origin, $x = 0$.

By looking at the matrix $\bar{B}$ we can build our intuition on the resiliency of the system. The first column represents the effect of the canard and only modifies the pitch rate of the aircraft. This actuator can be counteracted by the combined actions of both elevons, because $1.2735 + 1.2735 > 1.6532$. The elevons can counteract each other in terms of roll but doing so would induce a high pitching moment that cannot be counteracted. The yawing moment produced by the rudder cannot be counteracted by the other actuators: $0.8823 > 0.2805 + 0.2805$. Therefore, our intuition states that the fighter jet is only resilient to the loss of control authority over the canard.

We check whether the matrix $F = BB^\top - CC^\top$ is positive definite for each of the four possible actuator losses. Table 1 gathers the minimal eigenvalues of F for the four cases. As predicted by our intuition, the jet is only resilient to the loss of control authority over the canard.

Table 1: Minimal eigenvalue of F for each actuator losses

Loss of control of:	$\min \lambda(F)$
Canards	0.51
Right elevon	-8.5
Left elevon	-8.5
Rudder	-1.0

We study more in-depth the loss of control over the canard with Theorem 6. We reuse the notations employed in the proof and after some calculations we obtain: $\lambda_M = 0.8426 < 1$, $\alpha^* = 0.0343 > 0$, $\max(Re(\lambda(A))) = -0.259 < \alpha^*$, so the control law (12) should work.

We simulate our system on MATLAB with *ode*45. The undesirable input follows a uniform distribution between the bounds of u_c defined in (22). As predicted, the state converges exponentially from $x_0 = (1,\ 1,\ 1)\ rad/s$ to the origin, as shown by the blue curve in Figure 2. Without a control input, the state does not converge to the origin, as shown in red.

If the pilot loses control authority over any one of the elevons, then F is not positive definite, but $BB^\top$ is invertible. The control law (12) is still well-defined, so it can be implemented, but for some $w \in W$ the control is not admissible: $u_w \notin U$.

If the pilot loses control of the rudder, $BB^\top$ is not invertible, so the control law (12) is not well-defined. The jet cannot be guaranteed to be able to reach the desired target.

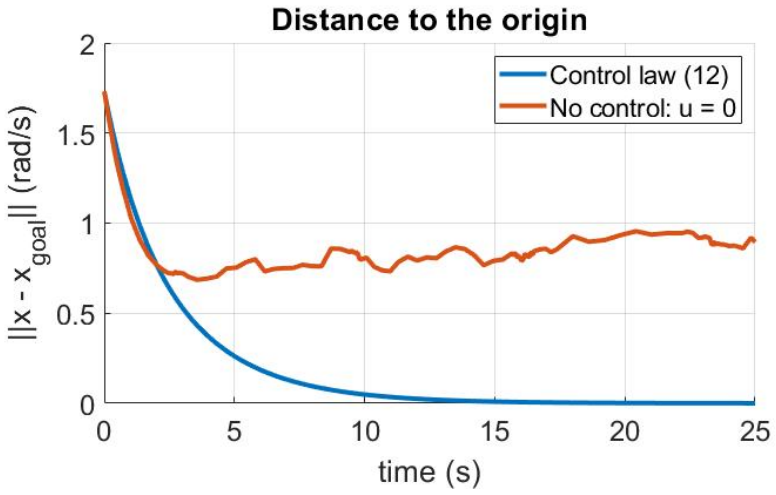

Figure 2: Distance of the state from the origin.

VI.2 Comparison with robust control

To illustrate the strength of our approach in the considered scenario, we compare our results with those of classical robust control.

Let us first recall the differences in assumptions between robust control and resilient reachability. A control law is said to be robust if it drives the state to the target *whatever the disturbance is*, i.e., there exists a control law u such that for all undesirable input w, we have $x(T) \in G$. On the other hand, resilient reachability considers a controller *aware of the undesirable input*, i.e., for all w, there exists a control law u_w such that $x(T) \in G$.

In our setting, the undesirable input is produced by an actuator belonging to the system. It is thus reasonable to assume that the actuator input can be measured. The resilient controller has access to more information than a robust controller. We thus expect the resilient controller to perform better than the robust controller.

We choose the robust control approach developed in [12]. Its objective is to approximate the closed-loop reach set $\mathcal{X}[T]$ with internal and external ellipsoids. The reach set gathers the states $x_{goal} \in \mathbb{R}^n$ for each of which there exists a control law such that, whatever the undesirable input is, $x(T) \in \mathcal{B}(x_{goal}, \mu)$ for a certain radius $\mu \geq 0$.

We compare the precision of our approach with [12] based on the size of the smallest target ball guaranteed to be reached. The application case is the ADMIRE model with drift studied in the previous subsection VI.1. We assume that the pilot loses control authority over the canards.

The resilient inputs have $\mathcal{L}_2$ bounds. However, the robust control inputs u must be bounded by an ellipsoid. To make the comparison as fair as possible, we choose the maximal ellipsoid within the actuators range (22). For the details of its construction we refer the reader to Appendix B.

We now need to calculate the radius μ of the smallest robustly reachable target. We compute only the tight ellipsoidal internal approximation of the closed-loop reach set: $\mathcal{E}\big(x_-(T), X_-(T)\big) \subseteq \mathcal{X}[T]$. We numerically obtained $\mu = 5.9$. Thus, the robust control law (with standard ellipsoidal approximations of the reachable set) can only guarantee to reach

a target state within a radius of 5.9. The initial state $x_0 = (1,\ 1,\ 1)$ was already inside that ball. Thus, the robust control cannot even guarantee that the state will get closer to the target than its initial state.

On the other hand, we know that the jet is resilient to the loss of control over the canards. Therefore, a target ball of any size is resiliently reachable. By having access to the undesirable input, a controller ensuring resilient reachability is then more effective than a robust controller.

In the major part of this work, we have considered driftless systems. We will now proceed to illustrate the developed theory for these systems.

VI.3 A driftless model

The aircraft model used as previous example is very convenient for our study because of the linearization and the overactuation. However, to render the dynamics driftless, we needed a more in-depth analysis of the model. We obtained the original simulation code of the ADMIRE model from [25].

For our purposes, we removed the states representing the sensor dynamics and those not directly affected by the controls from the initial 28-states model [22]. We also removed four of the sixteen inputs as they are negligible compared to the other inputs.

The simulation generates a pair of matrices A and $\bar{B}$ following the nominal dynamics (1). The effect of the matrix A is negligible compared to $\bar{B}$, when considering the states $x = (V_t,\ q,\ r)$, i.e., the jet speed, pitch and yaw rates. Thus, we approximate their dynamics by a driftless system, setting $A = 0$.

Since the jet has a single engine, it is not resilient to its loss. For our study, we assume a guaranteed authority over the thrust command, except for the afterburners. In the model the thrust command actuator also encompasses the afterburners. Since they account for only 20% of the thrust, the corresponding column in $\bar{B}$ is scaled by 20%.

At Mach 0.75 and altitude 3000 m, the control matrix is

$$\bar{B}^\top = \begin{bmatrix} -2.7 & 7.1 & -1.9 \\ -2.7 & 7.1 & 1.9 \\ -1.0 & -7.7 & -1.1 \\ -1.8 & -13 & -3.0 \\ -1.8 & -13 & 3.0 \\ -1.0 & -7.7 & 1.1 \\ -1.9 & 0.0 & -11 \\ -0.8 & -0.5 & 0 \\ -4.3 & -0.7 & 0 \\ 1.2 & 0 & 0 \\ -71 & 1.2 & -710 \\ -113 & -882 & 0 \end{bmatrix} \begin{matrix} \text{right canard,} \\ \text{left canard,} \\ \text{right outboard elevon,} \\ \text{right inboard elevon,} \\ \text{left inboard elevon,} \\ \text{left outboard elevon,} \\ \text{rudder,} \\ \text{leading edge flaps,} \\ \text{landing gear,} \\ \text{afterburner,} \\ \text{yaw thrust vectoring,} \\ \text{pitch thrust vectoring.} \end{matrix}$$

Each row of $\bar{B}^\top$ represents the effect of the actuator written on the right. All the values of the inputs are in radians except for the landing gear and the afterburner which are between 0 and 1. This control matrix is not 1-resilient, because the thrust vectoring inputs are several

orders of magnitude greater than any of the other inputs. For the same reason, the system is resilient to the loss of any one of the other ten actuators.

Simply removing thrust vectoring capabilities does not render the system 1-resilient; the control of the yaw rate would then primarily depend on the rudder, hence rendering the aircraft not resilient to the loss of the rudder.

Instead of removing the thrust vectoring actuators, if their range of motion is restricted to 1.4% of their current range, then $\bar{B}$ becomes resilient. Indeed, the thrust vectoring actuators can now be counteracted by the rudder and the elevons. Since we reduced the magnitude of two columns of $\bar{B}$, we also had to verify that the driftless hypothesis was still valid by comparing the effects of A and $\bar{B}$.

We showed how to make the fighter jet resilient in terms of speed, pitch and yaw rates, by scaling down thrust vectoring and having a guaranteed thrust. The resiliency improvement by reducing the thrust vectoring might seem counterintuitive. Yet, it is explained by the fact that these actuators were too powerful to be balanced if they became uncontrolled. While the new system is resilient, its capabilities have been reduced. For instance, reaching a target (while undamaged) would take significantly more time for the new resilient system than for the old one.

The resiliency analysis developed for this fighter jet is affected by several limitations of the current state of our theory. The first and obvious limitation comes from the driftless hypothesis but is justified here by the difference of magnitude between the drift and controlled dynamics. The most limiting hypothesis is that the controls are bounded by a $\mathcal{L}_2$ norm. Indeed, each actuator is independent of the others so a joint bound may not be appropriate. The structure of U from (3) also assumes that each actuator has a symmetric range of functioning, which makes sense for the rudder, for instance, but not for the landing gear which can only be stored or deployed. These two main limitations lead our future work directions.

VII Conclusions and Future Work

This paper introduced the notion of resilient systems that can withstand the loss of control over any single or multiple actuators and still guarantee to drive the state to its target. We established necessary and sufficient conditions to verify the resiliency of a system. We determined the minimal number of actuators required for 1- and 2-resilient systems. Further developing the theory, we established several methods to design resilient systems of any dimension and of any degree of resiliency. We then focused on control law synthesis for driftless and non-driftless systems. We proceeded to illustrate our results on a model of a fighter jet.

There are four promising avenues of future work. Most of our work so far has concerned driftless systems. We aim to extend the theory to a broader class of dynamics. Another direction of work concerns the type of bounds on the inputs. In this work we considered a bound on the total actuation effort of all the actuators over time. Instead, we want each actuator to have its own bound enforced at every instant. Another useful future step is to establish a metric quantifying the resiliency of a given system, for example, comparing the time required to reach a target with and without loss of control over actuators. Our

fourth direction of future work is to investigate more complex control specifications, e.g., reach-avoid, where the system seeks to avoid parts of the state space while reaching a target.

Appendices

A Examples of 2-resilient matrices

The following matrix $\bar{B}$ of size 6×24 is 2-resilient:

$$\bar{B} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 \end{bmatrix}.$$

The matrix $\bar{B}$ of size 8×32 is 2-resilient:

$$\bar{B}^\top = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \end{bmatrix}.$$

The following matrix $\bar{B}$ of size 12×46 is 2-resilient:

$$\bar{B}^\top = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\
-1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
-1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\
-1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 \\
-1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 \\
-1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 \\
-1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
-1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
-1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 \\
-1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
-1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 \\
-1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \\
-1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 \\
-1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 \\
-1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\
-1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \\
-1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\
-1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\
-1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\
-1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\
-1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 \\
-1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 \\
-1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\
-1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 \\
-1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 \\
-1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 \\
-1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 \\
-1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\
-1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 \\
-1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 \\
-1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\
-1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\
-1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
-1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\
-1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 \\
-1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 \\
-1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 \\
-1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\
-1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
-1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & -1
\end{bmatrix}.$$

These matrices were constructed using the methods described at the end of Section IV.

B Comparison with Robust Control

We provide further details of the computation of the ellipsoidal internal bounds $\mathcal{E}\big(x_-(T), X_-(T)\big) \quad \subseteq \quad \mathcal{X}[T]$ on the reach set in Section VI.2.

The center $x_-(t)$ of each of the internal ellipsoids follows the dynamics

$$\dot{x}_- = Ax_- + Bu_c + Cw_c, \quad \text{with} \quad x_-(0) = x_0 \in \mathbb{R}^n, \tag{23}$$

and u_c and w_c the respective centers of the control ellipsoid and of the disturbance ellipsoid.

The disturbance ellipsoid is $\mathcal{W} = \mathcal{E}(w_c, Q)$, with its center $w_c := \frac{1}{2}(w_{max} + w_{min})$. The disturbance bounds w_{min} and w_{max} are the mechanical bounds of the uncontrolled actuator defined in (22). We consider loss of control over only one actuator. Thus, Q is a scalar, so $Q(w - w_c)^2 \leq 1$ and $w_{min} \leq w \leq w_{max}$. Hence, $Q = \frac{4}{(w_{\max} - w_{\min})^2}$.

Defining the control ellipsoid is more complicated. To have a fair comparison with the results of our paper, we would need to enforce $\mathcal{L}_2$ bounds on the inputs. However, this is not possible in the framework of [12]: it allows only for time-invariant ellipsoidal sets of admissible control inputs. Let us find a compromise. We start from the bounds defined in (3): $\|u\|_{\mathcal{L}_2} \leq 1$ and $\|w\|_{\mathcal{L}_2} \leq 1$. So, we want to enforce

$$\int_0^T \|u(t)\|^2 dt \leq 1 \qquad \text{and} \qquad \int_0^T \|w(t)\|^2 dt \leq 1,$$

which can be done by choosing $\|u(t)\|^2$, $\|w(t)\|^2 \leq \frac{1}{T}$ for all $t \in [0, T]$. What matters here is the fact that $\|u(t)\|$ and $\|w(t)\|$ have the same bound. Therefore, we choose to limit each input to the smallest of the two intervals $[w_{min}, w_{max}]$ and the interval from (22). The control ellipsoid is then $\mathcal{E}\big(u_c, P\big)$, with its center $u_c := \frac{1}{2}(u_{max} + u_{min})$ and a diagonal shape matrix P with $P_{ii} = \min\left\{\frac{2^2}{\left(u^i_{\max} - u^i_{\min}\right)^2}, Q\right\}$.

The differential equation for the shape matrix $X_-(t)$ of the internal ellipsoid [12] is

$$\begin{aligned} \dot{X}_- \;&= AX_- + X_-A^\top + \sqrt{X_-}S_1(t)B\sqrt{P} + \sqrt{P}B^\top S_1(t)\sqrt{X_-^\top} \\ &\quad + \mu\Big(\sqrt{X_-}S_2(t) + S_2(t)\sqrt{X_-^\top}\Big) - \pi(t)X_- - \frac{CQC^\top}{\sqrt{\pi(t)}}, \end{aligned} \tag{24}$$

with $X_-(0) = X^0$. The functions π, S_1 and S_2 are defined as follows for a given vector $l \in \mathbb{R}^n$:

$$\begin{aligned} l(t) \;&:= e^{A^\top t} l & \qquad \pi(t) \;&:= \sqrt{l(t)^\top CQC^\top l(t)} \\ S_1(t)B\sqrt{P} \;&:= \sqrt{\tfrac{l(t)^\top BPB^\top l(t)}{l(t)^\top X_- l(t)}}\sqrt{X_-} & \qquad S_2(t) \;&:= \tfrac{\|l(t)\|}{\sqrt{l(t)^\top X_- l(t)}}\sqrt{X_-}. \end{aligned}$$

We can now compute the trajectory of the center of the ellipsoid $x_-(t)$ with (23), and the evolution of the shape matrix $X_-(t)$ of the ellipsoid with (24) and (25). When the radius μ of the target ball is too small for the target to be reached, then the shape matrix X_- is not positive definite. We investigated for the smallest μ such that $X_-(T) \succ 0$, and found $\mu = 5.9$. Therefore, the smallest target ball the robust method guarantees to reach has a radius of 5.9.

Acknowledgment

The authors would like to thank Dr. Kenneth Bordignon and Dr. Wayne Durham for providing us the ADMIRE model that enabled our simulations.

References

[1] C. Belcastro and J. Foster, "Aircraft loss-of-control accident analysis," in *AIAA Guidance, Navigation, and Control Conference*, 2010, p. 8004.

[2] J. Bouvier and M. Ornik, "Resilient reachability for linear systems," in *IFAC World Congress*, 2020, in press. [Online]. Available: https://mornik.web.illinois.edu/wp-content/uploads/BO20.pdf

[3] R. C. Suich and R. L. Patterson, "How much redundancy: Some cost considerations, including examples for spacecraft systems," NASA Technical Memorandum 103197, Tech. Rep., 1990.

[4] R. P. Ocampo, "Limitations of spacecraft redundancy: A case study analysis," in *44th International Conference on Environmental Systems*, 2014.

[5] W. Zhang and C. Van Luttervelt, "Toward a resilient manufacturing system," *CIRP Annals*, vol. 60, no. 1, pp. 469 – 472, 2011.

[6] M.-L. Li, P. Ramachandran, S. K. Sahoo, S. V. Adve, V. S. Adve, and Y. Zhou, "Understanding the propagation of hard errors to software and implications for resilient system design," *ACM Sigplan Notices*, vol. 43, no. 3, pp. 265 – 276, 2008.

[7] M. Bucić, M. Ornik, and U. Topcu, "Graph-based controller synthesis for safety-constrained, resilient systems," in *56th Annual Allerton Conference on Communication, Control, and Computing*, 2018, pp. 297 – 304.

[8] X. Tang, G. Tao, and S. M. Joshi, "Adaptive actuator failure compensation for nonlinear mimo systems with an aircraft control application," *Automatica*, vol. 43, pp. 1869 – 1883, 2007.

[9] W. Wang and C. Wen, "Adaptive actuator failure compensation control of uncertain nonlinear systems with guaranteed transient performance," *Automatica*, vol. 46, pp. 2082 – 2091, 2010.

[10] D. Bertsekas and I. Rhodes, "On the minimax reachability of target sets and target tubes," *Automatica*, vol. 7, pp. 233 – 247, 1971.

[11] D. Bertsekas, "Infinite-time reachability of state-space regions by using feedback control," *IEEE Transactions on Automatic Control*, vol. 17, no. 5, pp. 604 – 612, October 1972.

[12] A. Kurzhanski and P. Varaiya, "Reachability analysis for uncertain systems-the ellipsoidal technique," *Dynamics of Continuous Discrete and Impulsive Systems Series B*, vol. 9, pp. 347 – 368, 2002.

[13] S. Raković, E. Kerrigan, D. Mayne, and J. Lygeros, "Reachability analysis of discrete-time systems with disturbances," *IEEE Transactions on Automatic Control*, vol. 51, no. 4, pp. 546 – 561, April 2006.

[14] A. Marzollo and A. Pascoletti, "On the reachability of a given set under disturbances," *Control and Cybernetics*, vol. 2, no. 3, pp. 99 – 106, 1973.

[15] I. Mitchell and C. Tomlin, "Overapproximating reachable sets by hamilton-jacobi projections," *Journal of Scientific Computing*, vol. 19, pp. 323 – 346, December 2003.

[16] M. C. Delfour and S. K. Mitter, "Reachability of perturbed systems and min sup problems," *SIAM Journal on Control and Optimization*, vol. 7, no. 4, pp. 521 – 533, November 1969.

[17] D. A. Harville, *Matrix Algebra From a Statistician's Perspective*. Springer, 1997.

[18] G. H. Golub and C. F. V. Loan, *Matrix Computations*, 4th ed. John Hopkins University Press, 2013.

[19] M. Gu and S. C. Eisenstat, "Downdating the singular value decomposition," *SIAM Journal on Matrix Analysis and Applications*, vol. 16, no. 3, pp. 793 – 810, July 1995.

[20] J. B. Conway, *A Course in Functional Analysis*. New York City: Springer, 1990.

[21] A. Hedayat, W. D. Wallis *et al.*, "Hadamard matrices and their applications," *The Annals of Statistics*, vol. 6, no. 6, pp. 1184 – 1238, 1978.

[22] U. N. Lars Forssell, "ADMIRE the aero-data model in a research environment version 4.0, model description," FOI - Swedish Defence Research Agency, Tech. Rep., December 2005.

[23] S. T. G. Ola Härkegård, "Resolving actuator redundancy - optimal control vs. control allocation," *Automatica*, vol. 41, pp. 137 – 144, 2005.

[24] A. Khelassi, P. Weber, and D. Theilliol, "Reconfigurable control design for over-actuated systems based on reliability indicators," in *Conference on Control and Fault-Tolerant Systems*, 2010, pp. 365 – 370.

[25] W. Durham, K. A. Bordignon, and R. Beck, *Aircraft Control Allocation*. John Wiley and Sons, 2017.