Stability of switched systems with switching delay

Application to remote operation of aircraft under distributed control

by

Nikolai Matni

B. Applied Sciences, University of British Columbia, 2008

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Applied Science

in

THE FACULTY OF GRADUATE STUDIES
(Electrical and Computer Engineering)

The University Of British Columbia
(Vancouver)

August 2010

Abstract

Unmanned aerial vehicles are becoming more and more useful tools for not only the military, but law enforcement, search and rescue and scientific data collection. With the advent of inexpensive and reliable wireless communication, remote operators are now able to control fleets of UAVs cooperating towards the accomplishment of their tasks. As the complexity and size of these fleets increase, distributed control methods are needed – large fleet sizes will lead to intractable centralized problems. Furthermore, UAVs, like most aircraft, are inherently hybrid systems, combining both discrete and continuous dynamics. This thesis attempts to combine hybrid and distributed control theories in a way useful for the operation of UAVs, while taking communication delays inherent to a remote operator into account.

Specifically, we consider the stability of block upper-triangular switched linear systems with switching delay, when switching between stable modes. We show that the problem of proving globally uniformly asymptotic stability (GUAS) of a block upper-triangular switched linear system can be reduced to proving GUAS for each of its block diagonal subsystems. This allows for a scalable LMI-based computational test for GUAS under arbitrary switching whose complexity depends linearly on the number of block diagonal elements of the system. In cases for which the system is not GUAS under arbitrary switching, we partition the state space into regions in which switching will preserve GUAS despite a delay between the state measurements and switching time. This is accomplished by adding a delay buffer to standard Piecewise Lyapunov based partitions. Additionally, we show that the effect of the delay buffer on the standard Piecewise Lyapunov based partitions asymptotically approaches zero. Although we tailor these results to block upper-triangular switched linear systems, they are applicable to any switched linear

system with switching delay. These results are then extended to nonlinear switched systems. We apply our results to the control of a formation of vehicles under supervisory discrete control, and to switched systems under remote control. We then finish by addressing the issue of interface design for continuous systems under shared control, motivated by applications to pilot-automation interactions.

Preface

The work presented here has been published in or submitted to several conferences and journal publications.

Results from Chapters 3 and 4 are presented in

- N. Matni and M. Oishi, "Stability of block upper-triangular switched linear systems with switching delay," Submitted to *Systems & Control Letters*, Feb 2010. (15 pages)

Results from Chapter 5 will be presented in

- N. Matni and M. Oishi, "Stability of switched nonlinear systems with bounded switching delay," Submitted to *IEEE Trans. on Automatic Control*, 2010.
- M. Oishi, N. Matni and A. Ashoori, "Stability of switched nonlinear systems with bounded switching delay," To appear in *Journal of Nonlinear Systems and Applications*, August 2010.

Results from Chapter 6 are published in

- N. Matni and M. Oishi, "Reachability-based abstraction for an aircraft landing under shared control," *American Control Conference, 2008* , vol., no., pp.2278-2284, 11-13 June 2008
- N. Matni and M. Oishi, "Reachability analysis for continuous systems under shared control: Application to user-interface design," *Proc. of the IEEE Conf. on Decision and Control/Chinese Control conference, 2009*, pp.5929-5934, 15-18 Dec. 2009. Awarded **General Chairs' Recognition Award for Interactive Papers**.

In all articles for which I am the first author, I was the lead investigator. I determined the problems to solve, conducted the theoretical research and confirmed the results via simulation. I was responsible for the bulk of the writing of each article, with my supervisor Professor M. Oishi providing technical and stylistic feedback on my work. The results found in Chapter 6 are an extension of Professor M. Oishi's previous work.

The article for which Professor M. Oishi is first author represents a synthesis of my work on switched systems with delay, and my lab mate Ahmad Ashoori's work on Parkinson's disease. Professor Oishi wrote the article and found an appropriate way of merging my results with those of Mr. Ashoori.

Table of contents

List of tables

List of figures

Acknowledgements

This thesis would not have been possible without the support, guidance and expertise of my supervisor, Professor Meeko Oishi. Her consistent feedback, insight and advice, as well as her willingness to allow me the freedom to work in my own way, have been invaluable in my development as a researcher, and for that I will always be grateful.

I would also like to take this opportunity to express my gratitude to my committee members, Professors Ryozo Nagamune and Vikram Krishnamurthy, for taking the time to consider my candidacy. I would also like to thank Professors Philip Loewen and Ian Mitchell, who were always willing to support me in my academic endeavours and from whom I learned so much during my time at UBC.

I have had the pleasure of working in a great lab group. I am indebted to all of my labmates for the support that they have offered over the years. However I would like to thank Shahab Kaynama in particular, as he has been both a fantastic technical resource, and a great friend. I would also like to thank all of the student and faculty members of the Control Systems Reading Group – our weekly meetings were always informative, and have helped me understand just how beautiful and broad controls research is.

My time at UBC has been an incredible experience, and a huge reason for this has been the great people that I have met while here. Bryce, Christine, Tony, Graham, Erica, Danaka, the men's varsity soccer team, they've all made Vancouver feel like home to me, and given me memories I to cherish for the rest of my life.

Finally, I have to thank my family for their love and support. The faith that they have always had in me has given me the confidence to follow my dreams, and I could not have done this without them.

Chapter 1

Introduction

1.1 Background and motivation

With the advent of inexpensive and reliable wireless communication, research on remote and cooperative control of unmanned aerial vehicles (UAVs) became an area of focus in the United States during the late 1990s and early 2000s [12]. These versatile vehicles have many applications beyond traditional military uses, including police surveillance and reconnaissance, search and rescue, and scientific data collection [66]. The benefits of using UAVs over traditional manned aircraft are tangible – for example, they eliminate the need to place highly trained operators in harmful situations, and allow for extended periods of operation by switching operators on the fly.

Although all of the aforementioned uses can be accomplished by a single UAV, the efficiency and effectiveness of their completion can benefit substantially from cooperation amongst a fleet of UAVs to accomplish the task. For example, in a search and rescue mission, it is obvious that a fleet of 100 UAVs can cover more terrain than a single UAV during the same timespan. However, an increase in vehicle number invariably leads to an increase in system complexity, especially when cooperation amongst the vehicles is necessary. If this complexity reaches a level at which centralized control of the fleet is no longer feasible, then distributed cooperative control methods are needed. Communication and physical constraints can also lead to the need for distributed, rather than centralized, control schemes.

Distributed control reduces the complexity of large, centralized problems by dividing them into several smaller local problems. These techniques allow for guarantees of global behavior, despite each vehicle accessing only local information – an important and useful property when considering the applications of fleets of UAVs. As such, distributed control of vehicles has been an area of much research in recent years. For an excellent survey of recent results in multivehicle formation control, see [53]. Recent research in distributed control has included work in vehicle formation control [14, 22, 25, 68], consensus and swarming [36, 55, 56], mobile sensor networks [13, 30, 35], control over uncertain channels [27–29], and optimal control [24, 58], all under topological constraints. These methods all assume that the dynamics of each subsystem can be represented by a continuous system.

However, UAVs, like most aircraft systems, have several discrete modes of operation, each with different continuous dynamics, and therefore belong to a class of systems known as *hybrid systems*. Hybrid systems, which combine discrete and continuous dynamics, have become commonplace as cheap microcontrollers, fundamentally discrete devices, have become more or less ubiquitous in the control of physical processes. Common examples of hybrid systems include thermostats, smart cruise control and aircraft autopilots. Furthermore, in more advanced systems, hybrid controllers are often used, as they enable performance not achievable with strictly continuous controllers. For example, a properly designed hybrid controller is capable of having both fast response times and a robustness to noise [32], a key property for real world systems. However, combining discrete and continuous dynamics introduces further complexity to the analysis, as the discrete mode switching pattern may now affect system stability.

Hybrid systems have received considerable attention in the past few decades. Many results have been borrowed and extended from nonlinear theory, and hence are mostly based on Lyapunov theory. In order to prove stability of a hybrid system under arbitrary switching, a common Lyapunov function approach is used [46, 52]. However, there is as of yet no systematic way of constructing such a function for a general hybrid system, if it exists, although there are results for when the family of continuous dynamics satisfy certain Lie-algebraic conditions [2, 47]. Furthermore, there exist converse Lyapunov theorems which are able to prove that a common Lyapunov function does not exist for a given system [17, 38]. Regardless, if such

a function cannot be found, the common recourse is to then use techniques based on multiple Lyapunov functions, as introduced in [9, 38, 46, 57]. The essential concept in these results is to ensure that the value of a piecewise Lyapunov function constructed from the multiple Lyapunov functions decreases at a given rate over time. Alternatively, as presented in [31], a dwell time approach can be used, in which the average dwell time in each mode is bounded from below, and has a direct effect on the convergence rate of the system. Finally, there have been some strong results on the parametrization of switched stabilizing controllers [5, 33].

In the case of UAVs, all of the issues traditionally associated with hybrid systems are present. However, since these systems are generally remotely operated, new challenges emerge. Specifically, a remote operator will have to contend with communication delays caused by wireless protocols and physical distance. Alternatively, if a fleet of UAVs is autonomous, but is attempting to coordinate mode switches (a key requirement for provable stability, as will be explained in later chapters), then the local "operator" will need to take into account synchronization delays as well.

Although not directly related, there is a rich body of work on delay differential equations, of which [23] is an excellent example. There has been some related work on switched systems with delays in their dynamics [10, 26, 42] as well as delays in detecting autonomous mode switches [37, 69, 70]. However, most relevant to our work is [67], where a delay between state measurements and switching time is explicitly accounted for. This *switching delay*, along with delays in the state feedback, are addressed by providing upper bounds on the state delays and a lower bound on the average dwell-time such that asymptotic stability of the closed loop is guaranteed. We distinguish our method from the approach taken in [67] – rather than using a dwell-time argument, we provide state based constraints for switching to guarantee asymptotic stability. It will be argued in Chapter 4 that these two approaches are in fact complementary, each proving more useful for specific applications.

It is clear that the benefits of UAVs, both as individual vehicles, and as fleets under cooperative control, are substantial. These systems are inherently hybrid, and in order to exploit their full potential, this should be taken into account in their analysis and design. Merging the theories of hybrid systems and distributed control

will lead to large, scalable systems that incorporate the benefits and flexibility of hybrid control. In light of this, this thesis addresses two main problems:

Problem 1. *Find a scalable test for stability under arbitrary switching of a fleet of identical vehicles with hybrid dynamics.*

Problem 2. *Find a method of synthesizing state constrained switching schemes that are robust to a switching delay for a fleet of identical vehicles with hybrid dynamics.*

Of course, in real world applications, safety and performance requirements are generally much more restrictive than simply proving stability of a system. In these cases, formal verification techniques, such as model checking and reachability, can be applied in order to ensure that these performance and safety criteria are satisfied. When a user is introduced into the loop, this task becomes even more complex. While verification techniques have been successfully applied to human-automation systems modeled as discrete event systems (DES) [6, 11, 15, 19, 60, 61], less work has been done on verification of continuous or hybrid human-automation systems [45, 65]. In [54], an invariance-preserving abstraction was formulated for supervisory hybrid systems: that is, the human input was limited to discrete inputs. In the case of UAVs, and aircraft in general, there may also be a shared continuous input to the system. In general, one does not want to limit the input of the human, but rather provide them with the information they need to make informed decisions with respect to safety. Thus, this thesis will also address the following problem:

Problem 3. *How to present the user of a human-automation system under shared continuous control the information necessary to preserve safety (defined in the sense of reachable sets).*

1.2 Contributions

The work presented in this thesis contributes to merging the theories of distributed and hybrid systems. In particular, I focus on formations of vehicles under distributed control, wherein each vehicle's dynamics are hybrid . My main contributions are, for formations of switched linear vehicles:

- a scalable, computationally efficient test for stability under arbitrary switching of block upper-triangular systems.
- a proof that for state constraint based switching, only that subset of the state space corresponding to the block diagonal subsystems that are not stable under arbitrary switching need to be taken into consideration.

and for general switched systems under remote supervisory control:

- a method of synthesizing state constraints that guarantee stability despite a switching delay.
- a proof that these state constraints asymptotically approach standard (delay-free) Lyapunov based constraints.

Finally, in the design of user-interfaces for systems under shared control, my main contributions are:

- formal definitions of invariance, user-invariance, and user-assisted invariance for shared control systems, and their relationship to computed reachable sets.
- a method to abstract the resulting reachable sets to a DES that contains minimal information regarding the effect of continuous human input on safety
- an application of these methods to a model of an actual aircraft incident [44].

1.3 Outline

This thesis is organized as follows:

Chapter 2 presents requisite mathematical preliminaries for hybrid system stability and modeling of vehicle formations via graph theory.

Chapter 3 presents definitions of stability for a switched linear system, and a scalable test for asymptotic stability of block upper-triangular switched linear systems. The results are illustrated through two examples.

Chapter 4 presents conditions on the state constraints and switching delay for stability of a switched linear system.

Chapter 5 extends the results of Chapter 4 to switched nonlinear systems with stable mode dynamics.

Chapter 6 first presents a brief review of reachability analysis for continuous and hybrid systems. Definitions of different levels of invariance are presented, and methods of computing them using standard reachability tools are developed. Finally I present an abstraction method which results in a *safety-informative* discrete user-interface, and apply it to an example motivated by a documented aircraft incident [44].

Chapter 7 offers directions for future work, and conclusions for the work presented here. Key results are summarized.

The work presented here has been published in or submitted to several conferences and journal publications.

Results from Chapters 3 and 4 are presented in

- N. Matni and M. Oishi, "Stability of block upper-triangular switched linear systems with switching delay," Submitted to *Systems & Control Letters*, Feb 2010. (15 pages)

Results from Chapter 5 will be presented in

- N. Matni and M. Oishi, "Stability of switched nonlinear systems with bounded switching delay," Submitted to *IEEE Trans. on Automatic Control*, 2010.
- M. Oishi, N. Matni and A. Ashoori, "Stability of switched nonlinear systems with bounded switching delay," To appear in *Journal of Nonlinear Systems and Applications*, August 2010.

Results from Chapter 6 are published in

- N. Matni and M. Oishi, "Reachability-based abstraction for an aircraft landing under shared control," *American Control Conference, 2008* , vol., no., pp.2278-2284, 11-13 June 2008
- N. Matni and M. Oishi, "Reachability analysis for continuous systems under shared control: Application to user-interface design," *Proc. of the IEEE*

Conf. on Decision and Control/Chinese Control conference, 2009, pp.5929-5934, 15-18 Dec. 2009. Awarded **General Chairs' Recognition Award for Interactive Papers**.

Chapter 2

Mathematical preliminaries

This chapter presents some basic results on the stability of hybrid systems, and introduces some key concepts of graph theory. Finally, a model of a formation of identical linear vehicles under distributed control is presented, along with some key results on the stability of such systems.

2.1 Uniform asymptotic stability of hybrid systems

Due to the interaction between discrete and continuous dynamics in hybrid systems, stability of the system depends not only on the continuous dynamics of each mode, but also on the switching pattern between these modes. It is well known (cf. Example 2.1, [9]) that switching amongst stable modes can lead to an unstable system. Basic introductions to hybrid systems can be found in [8, 62], and an overview of recent research efforts can be found in [18, 20].

We focus on systems in which the user has control over mode switches, but the continuous dynamics are fully autonomous. In order to analyze the stability of such a hybrid system, it is convenient to cast it into a switched system framework

$$\dot{x} = f_{\sigma(t)}(t,x) \tag{2.1}$$

where $x \in \mathbb{R}^n$, $\sigma : \mathbb{R}_+ \to \mathscr{P} \subset \mathbb{N}$ is a piecewise constant switching signal (we denote the set of all piecewise constant switching signals Σ), and $\mathscr{F} := \{f_p : \mathbb{R}_+ \times \mathscr{D} \to \mathbb{R}^n \ : \ p \in \mathscr{P}\}$ is a family of functions indexed by p that are piece-

wise continuous in t and locally Lipschitz in x on $\mathbb{R}_+ \times \mathscr{D}$, with $\mathscr{D} \subset \mathbb{R}^n$ a domain containing the origin. We assume the origin to be an equilibrium point for each $f_p \in \mathscr{F}$ without loss of generality.

Definition 1. *From [46]: A system (2.1) is locally* uniformly asymptotically stable *(UAS) if there exist positive constant δ and class $\mathscr{KL}$ function β such that the solutions of 2.1, for all $||x(t_0)|| \leq \delta$, satisfty*

$$||x(t)|| \leq \beta(||x(t_0)||, t - t_0), \ \forall t \geq t_0 \tag{2.2}$$

Consider the following two well established stability theorems:

Theorem 1. ***(Common Lyapunov Function)***. *From [46]: If all systems $\dot{x} = f_p(x,t)$, $f_p \in \mathscr{F}$, share a common Lyapunov function, then (2.1) is UAS.*

Theorem 2. ***(Multiple Lyapunov Functions)***. *From [9]: Consider a switched system (2.1). Let Σ^* be the set of all piecewise constant switching signals $\sigma : \mathbb{R}_+ \to \mathscr{P}$ for which*

$$V_{\sigma(\tau^-)}(x) - V_{\sigma(\tau)}(x) > 0 \tag{2.3}$$

for each switching time τ. Then (2.1) is UAS for all $\sigma \in \Sigma^*$.

Theorem 1 can be used to prove UAS under arbitrary switching for (2.1). If a common Lyapunov function (CLF) does not exist or cannot be found, UAS may still be proven for specific classes of switching schemes using Theorem 2.

Remark 1. *Less conservative versions of Theorem 2 exist (cf. Chapter 3, [46]) – however they result in more complex switching constraints, and are less suited to our purposes.*

In the case of linear switched systems, efficient linear matrix inequality based computational methods allow for the rapid calculation of Lyapunov functions.

2.2 Introductory graph theory

There are many excellent texts on graph theory, including a recent text [21], and those that focus on the Laplacian and its spectral properties [1, 3, 50].

We describe the information flow between vehicles by defining a directed graph $\mathscr{G}$, consisting of a set of N nodes $\mathscr{V}$ (a node for each vehicle), and a set of edges $\mathscr{E} \in \mathscr{V} \times \mathscr{V}$, where an edge $e = (v_1, v_2) \in \mathscr{E}$, with $v_1, v_2 \in \mathscr{V}$. The edges define the direction of information flow between vehicles, with the first element of e, denoted tail(e), the information source, and the second element, denoted head(e), the information sink.

The in-degree of a node $d^i(v)$, is the number of edges with v as its head. We define the normalized adjacency graph, $A(\mathscr{G})$, a square matrix of size $|\mathscr{V}|$, as

$$A_{ij} = \left\{ \begin{array}{ll} 1/d^i(v_i) & \text{if} \quad (v_j, v_i) \in \mathscr{E} \\ 0 & \text{otw} \end{array} \right\} \tag{2.4}$$

A path on $\mathscr{G}$ is an ordered set of vertices $\{v_0, v_1, ..., v_n\}$ such that $(v_{i-1}, v_i) \in \mathscr{E}$ for $i \in \{1, ..., n\}$. A graph $\mathscr{G}$ is said to be *strongly connected* if there exists a path from every vertex to every vertex.

As in [25], we define the graph *Laplacian* as

$$L = I - A \tag{2.5}$$

and state some key results on its spectral properties, as these play an important role in the stability of a fleet of vehicles flying in formation under distributed control.

Proposition 1. *Zero is an eigenvalue of L, and its corresponding eigenvector is* 1^T.

Proposition 2. *All eigenvalues of L lie in a disk of radius 1 centered at* $1 + 0j$ *in the complex plane.*

Proposition 3. *If* $\mathscr{G}$ *is strongly connected, the zero eigenvalue is simple.*

2.3 Distributed control of vehicle formations

This section summarizes key results on formations of identical linear vehicles from [25, 68]. Consider a fleet of N identical vehicles, where the i^{th} vehicle's dynamics are given by

$$\dot{x}_i = Ax_i + Bu_i \tag{2.6}$$

where $x_i \in \mathbb{R}^n$ and $u_i \in \mathbb{R}^m$. A local full-state feedback controller is assumed to operate on each vehicle such that the closed loop dynamics A_{cl} of the individual vehicles are stable.

It has been shown that the formation dynamics of a fleet of linear vehicles with dynamics (2.6) can be described by [25, 68]

$$\dot{x} = (I_N \otimes A_{cl} + L \otimes BK)x \tag{2.7}$$

where I_N is the $N \times N$ identity matrix, $\otimes$ denotes the Kronecker product, $x = [x_1^T, x_2^T, \ldots, x_N^T]^T \in \mathbb{R}^{nN}$, $K \in \mathbb{R}^{m \times n}$ is the linear formation feedback controller, identical for all vehicles, and $L \in \mathbb{R}^{N \times N}$ is the graph Laplacian describing the fixed communication topology of the formation.

As in [25, 68], we introduce a Schur transformation matrix U such that $\widetilde{L} = U^{-1}LU$ is upper triangular, and the diagonal entries of $\widetilde{L}$ are the eigenvalues of L. Applying the transformation $T = U \otimes I_n$ to (2.7) results in a block upper-triangular system in the transformed coordinates $z = T^{-1}x$.

$$\dot{z} = (I_N \otimes A_{cl} + \widetilde{L} \otimes BK)z \tag{2.8}$$

with block diagonal subsystems

$$\dot{z}_i = (A_{cl} + \lambda_i BK)z_i \tag{2.9}$$

where λ_i is an eigenvalue of L. This transformation allows for the following results.

Theorem 3. *From [25]: A formation feedback controller K stabilizes the formation dynamics in (2.7) if and only if it simultaneously stabilizes (2.9) for all eigenvalues λ_i of the graph Laplacian L describing the communication topology of the formation.*

Corollary 1. *From [25]: A formation is stabilizable (in a distributed sense) if and only if its communication graph is strongly connected.*

Chapter 3

Stability of block upper-triangular switched linear systems under arbitrary switching

We focus on switched linear systems under arbitrary switching. While the existence of a CLF is sufficient to prove stability, for systems of large dimension (e.g. formations of vehicles under distributed control), standard LMI tools may fail due to memory issues. Hence we focus on the same stability problem, but aim to solve it by analyzing several LMIs of lower dimension rather than one full dimensional problem. We do so by exploiting a transformation which results in the formation being in block upper triangular form. We demonstrate the usefulness of our method on a 100-vehicle formation under distributed control.

3.1 Problem formulation

Consider a switched linear system

$$\dot{x} = M_\sigma x \tag{3.1}$$

where $x \in \mathbb{R}^n$, $\sigma : [0,\infty) \to \mathscr{P} \subset \mathbb{N}$ is a piecewise constant switching signal, and $\mathscr{M} := \{M_p \in \mathbb{R}^{n\times n} : p \in \mathscr{P}\}$, is a family of block upper-triangular Hurwitz state matrices indexed by p.

Definition 2. *Consider a family of block upper-triangular state matrices* $\mathscr{M} := \{M_p \in \mathbb{R}^{n\times n} : p \in \mathscr{P} \subset \mathbb{N}\}$*, indexed by p, with*

$$M_p = \begin{bmatrix} A_p^1 & X_{12} & \cdots & X_{1N} \\ 0 & A_p^2 & \cdots & \vdots \\ \vdots & \vdots & \ddots & X_{(N-1)N} \\ 0 & 0 & \cdots & A_p^N \end{bmatrix} \tag{3.2}$$

and $A_p^i \in \mathbb{R}^{n_i\times n_i}$*, where* $\sum_{i=1}^{N} n_i = n$*,* $i \in \{1,...,N\}$*, and* X_{ij} *are the non-zero, off-diagonal elements of* M_p *of appropriate dimension. For* $\mathscr{A}^i := \{A_p^i \in \mathbb{R}^{m_i\times n_i} : p \in \mathscr{P}\}$*,* $x_i \in \mathbb{R}^{n_i}$ *the corresponding subset of the state vector* $x \in \mathbb{R}^n$*, and* $\sigma : \mathbb{R}_+ \to \mathscr{P}$ *a piecewise constant switching signal,*

$$\dot{x}_i = A_\sigma^i x_i \tag{3.3}$$

is the i^{th} block diagonal subsystem *of the switched linear system (3.1). Furthermore, the* j^{th} *block diagonal subsystem is said to be lower (higher) than the* i^{th} *block diagonal subsystem if* $j > i$ *(*$j < i$*).*

Definition 3. *From [46]: a system (3.1) is* globally uniformly asymptotically stable (GUAS) under Σ^**, a set of piecewise constant switching signals, if there exist positive constants c and* μ *such that the solution* $x(t) = \Phi_\sigma(t,0)x(0)$ *to (3.1), with* $\Phi_\sigma(t,0)$ *the state transition matrix of (3.1), satisfies the following two equivalent conditions:*

$$||x(t)|| \leq ce^{-\mu t}||x(0)|| \tag{3.4}$$

$$||\Phi_\sigma(t,0)|| \leq ce^{-\mu t} \tag{3.5}$$

for all $t \geq 0$*, any initial state* $x(0)$ *and* any switching signal $\sigma(\cdot) \in \Sigma^*$

Remark 2. *If* $\Sigma^* = \{p\},\ p \in \mathscr{P}$*, (i.e.* $\sigma(t) \equiv p$*), Definition 3 is equivalent to GUAS of a linear system.*

Remark 3. *If Σ^* is the set of all piecewise constant switching signals, then (3.1) is* GUAS under arbitrary switching.

For the cooperative control of distributed systems, the block diagonal subsystems of (3.1) have the same number of states as the individual subsystems. Thus the main advantage of proving the stability of (3.1) by solely analyzing its block diagonal subsystems it that it is highly scalable, as its complexity would be linear in the number of subsystems. This is particularly relevant for N large enough to be computationally prohibitive for current LMI solvers.

3.2 Scalable test for stability

We show that (3.1) is GUAS under a set of piecewise constant switching signals Σ^* if and only if each of its block diagonal subsystems is GUAS under Σ^* by exploiting its block upper-triangular structure. This is an extension of a well-known result in which a switched linear system (3.1) with $\mathscr{M}$ a family of Hurwitz upper-triangular state matrices is GUAS under arbitrary switching [2, 46, 47, 52]. Although we focus on systems with static full-state feedback, the results are easily extendable to dynamic controllers with partial state feedback, assuming detectability and stabilizability of the system (cf. [25]).

Recall that for a linear system $\dot{x} = Ax + Bu$ with Hurwitz matrix A, the state trajectory $x(t)$ can be exponentially bound, as in 3.4, if the input u is exponentially decaying, i.e. there exist positive constants c, μ satisfying $||u(t)|| \leq ce^{-\mu t}||u(0)||$. Additionally, we define $||H|| := \max_{x\neq 0} \dfrac{||Hx||}{||x||}$ for $H \in \mathbb{R}^{m\times n}$, $x \in \mathbb{R}^n$, in the usual manner; hence $||Hx|| \leq ||H||||x||$.

Theorem 4. *A switched linear system (3.1) is GUAS under a set of piecewise constant switching signals Σ^*, if and only if each block diagonal subsystem of (3.1) is also GUAS under Σ^*.*

Proof. Assume without loss of generality that for the switched linear system (3.1),

$$M_p \quad = \quad \begin{bmatrix} A_p^1 & B_p \\ 0 & A_p^2 \end{bmatrix} \tag{3.6}$$

with $A_p^i \in \mathbb{R}^{n_i \times n_i}$, $n_1 + n_2 = n$, $B_p \in \mathbb{R}^{n_1 \times n_2}$, and $x = [x_1^T, x_2^T]^T$, with $x_1 \in \mathbb{R}^{n_1}$, $x_2 \in \mathbb{R}^{n_2}$.

If: Assume that $\dot{x}_1 = A_\sigma^1 x_1$ and $\dot{x}_2 = A_\sigma^2 x_2$ are GUAS under Σ^*. From Definition 3, $||x_2(t)|| \leq c_2 e^{-\mu_2 t}||x_2(0)||$, $\forall \sigma \in \Sigma^*$ for some c_2, $\mu_2 > 0$. Treating x_2 as an exponentially decaying input to x_1,

$$x_1(t) \quad = \quad \Phi_\sigma^1(t,0)x_1(0) + \int_0^t \Phi_\sigma^1(t,\tau)B_{\sigma(\tau)}x_2(\tau)d\tau \tag{3.7}$$

with $||\Phi_\sigma^1(t,\tau)|| \leq ae^{-\mu(t-\tau)}$, $\forall \sigma \in \Sigma^*$, for a, $\mu > 0$, as in Definition 3. Since $||B_{\sigma(\tau)}|| \leq \max_{p \in \mathscr{P}} ||B_p|| := ||B_{\max}||$,

$$\begin{aligned} ||x_1(t)|| &\leq ||\Phi_\sigma^1(t,0)||||x_1(0)|| \\ &\quad + ||B_{\max}|| \int_0^t ||\Phi_\sigma^1(t,\tau)||||x_2(\tau)||d\tau \\ &\leq c_1 e^{-\mu_1 t}||x_1(0)||, \ \forall \sigma \in \Sigma^* \end{aligned} \tag{3.8}$$

for c_1, $\mu_1 > 0$, hence (3.1) is GUAS under Σ^*.

Only if: Assume (3.1) is GUAS under Σ^*. Then by Definition 3, there exist positive constants c, μ such that $||x(t)|| \leq ce^{-\mu t}$. It is clear that this holds for $x(t)$ if and only if it holds for all subsets $x_i(t)$ of $x(t)$. If there do not exist positive constants c_i, μ_i, satisfying $||x_i(t)|| \leq c_i e^{-\mu_i t}||x_i(0)||$ $\forall \sigma \in \Sigma^*$ for $i = \{1,2\}$, then the required constants c, μ do not exist, which is a contradiction. □

These results can be extended to N-block upper-triangular matrices of arbitrary dimension by induction, beginning with the bottom block diagonal subsystem and working upwards.

Corollary 2. *A switched linear system (3.1) is GUAS under arbitrary switching if and only if each block diagonal subsystem of (3.1) is also GUAS under arbitrary switching.*

To illustrate the benefits of our approach, consider a P mode, N block system (3.1), with each subsystem (3.3) of dimension n. Analysis of (3.1) as a whole would involve solving $P+1$ LMIs in $\mathbb{R}^{Nn \times Nn}$ – for large N this quickly becomes prohibitively expensive in terms of memory requirements. However, applying Corollary 2, we solve N sets of $(P+1)$ LMIs in $\mathbb{R}^{n \times n}$, each easily computed. To quantify

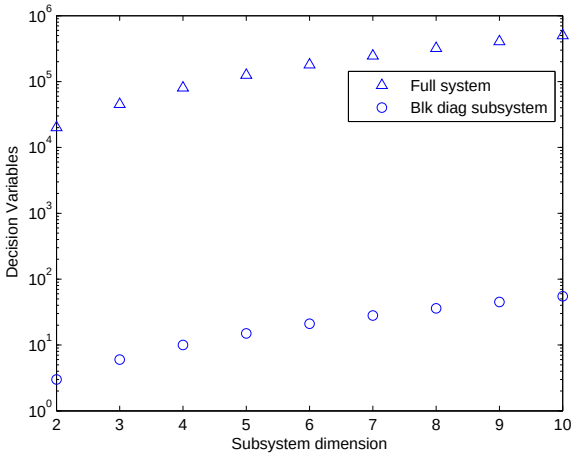

Figure 3.1: Shown on a log scale are the number of decision variables Matlab requires to solve an LMI proving GUAS under arbitrary switching for (1) a two mode distributed system with 100 subsystems ($\triangle$) and (2) a single block diagonal two mode subsystem ($\circ$).

the benefits of our method, we compare the number of decision variables Matlab requires to solve an LMI proving GUAS under arbitrary switching for a full system as opposed to for an individual subsystem. Figure 3.1 shows, on a log scale, the number of decision variables needed for a two mode distributed system with 100 subsystems, with subsystem dimension ranging from 2 to 10.

The derivation of Theorem 4 and Corollary 2 hinges on three key assumptions: (1) a fixed communication topology, (2) all vehicles are identical at all times and (3) all vehicles have linear dynamics. These assumptions are required to preserve the properties of Kronecker multiplcation so that the system can be transformed into block upper-triangular form. If the communication topology changes, then the graph Laplacian will as well, requiring a new coordinate transformation to apply Theorem 4. However, if the communication topology is fairly reliable, this should not cause instability – so long as topology changes do not occur too quickly, a dwell time argument [31] can be used to show that this will not destabilize the system. Once the new communication framework has been established, our results can once again be applied to prove GUAS under arbitrary switching.

The case of addressing fleets of either non-identical or nonlinear systems is much more difficult. The properties of the Kronecker product break down, and the system can no longer be transformed into block upper-triangular form, although preliminary results based on Lyapunov [14] and optimal control [22] theory do exist. We assume the existence of a supervisory discrete controller that coordinates mode switches – we believe this to be reasonable since the communication cost of transmitting a mode switch is very low compared to transimitting continuous state information. Furthermore, UAV systems have inner control loops that, through dynamic extension and feedback linearization, allow for a vehicle's dynamics to be reasonably approximated by a double integrator [59]. Hence our results are applicable to outer control loop design for actual fleets of UAVs.

Finally, we note that although the examples in the following section have been tailored to UAV applications, the results are much more general. Theorem 4 and Corollary 2 can be used to prove scalable stability of any distributed switched linear system with a supervisory discrete controller. Possible application areas include interconnected pulp and paper mills, chemical and biological batch processes, and network flow control, to name a few.

3.3 Examples: formations of double integrators

Consider a fleet of N identical vehicles as described by (2.7), in which the three position variables are decoupled, and the acceleration in each direction is controlled separately. We can thus limit our analysis, without loss of generality, to vehicles moving in one dimension with vehicle dynamics

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{3.9}$$

with $x_i \in \mathbb{R}^2$, $u_i \in \mathbb{R}$.

Mode switches amongst the vehicles must occur simultaneously, since asynchronous switching causes the system to lose its block upper-triangular structure. Hence, we consider the case in which a supervisory logic controller switches the linear formation feedback controller of all vehicles, such that $K = K_\sigma : \mathbb{R}^2 \to \mathbb{R}$, with σ a piecewise constant switching signal that maps to $\mathscr{P} \subset \mathbb{N}$. This remote

supervisory controller is meant to represent a UAV operator remotely changing the UAVs' operation modes in order to meet mission objectives or in response to environmental disturbances.

Thus the transformed system (2.8) becomes

$$\dot{z} \quad = \quad (I_N \otimes A_{cl} + \widetilde{L} \otimes BK_\sigma)z \tag{3.10}$$

with block diagonal subsystems

$$\dot{z}_i \quad = \quad (A_{cl} + \lambda_i BK_\sigma)z_i \tag{3.11}$$

with λ_i an eigenvalue of L. We assume that K_p has been chosen such that (3.11) is Hurwitz for all $p \in \mathscr{P}$ and all eigenvalues of L. Traditional LMI methods can then be applied to the block diagonal subsystems, rather than to the entire system, to show GUAS under arbitrary switching (Theorem 4). For a P mode system, we have thus reduced the problem to N sets of $P+1$ LMIs in $\mathbb{R}^{2\times 2}$ as opposed to $P+1$ LMIs in $\mathbb{R}^{2N\times 2N}$.

Five vehicle system

Consider first an illustrative example, a five vehicle system with

$$A_{\text{cl}} = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \qquad \begin{array}{l} K_1 = [-20 \ -5] \\ K_2 = [-4 \ -6] \end{array} \tag{3.12}$$

and

$$L = \begin{bmatrix} 4 & -1 & -1 & -1 & -1 \\ 0 & 2 & -1 & 0 & -1 \\ -1 & -1 & 3 & -1 & 0 \\ -1 & 0 & -1 & 3 & -1 \\ -1 & -1 & 0 & 0 & 2 \end{bmatrix} \tag{3.13}$$

switching randomly between K_1 and K_2. The communication topology defined by the unnormalized Laplacian (3.13) is illustrated in Figure 3.2, in which arrows indicate the flow of information (state measurements), obtained through the UAVs' sensors. Note that the graph is strongly connected, satsifying the condition for

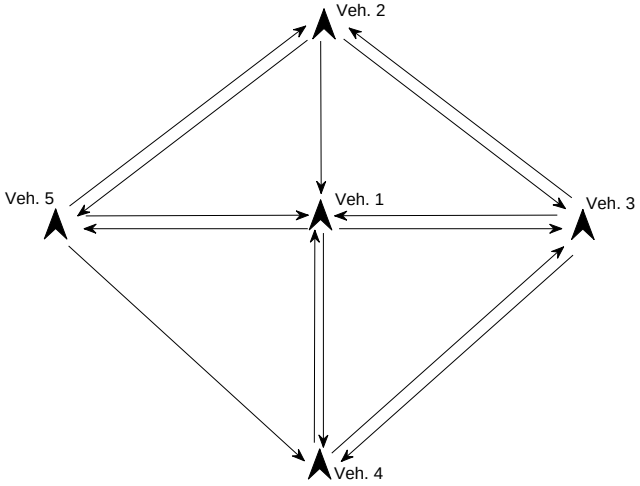

Figure 3.2: Communication topology defined by the graph Laplacian (3.13) used in the 5 vehicle example. Arrows indicate the flow of information (state measurements). The graph is fully connected, satisfying Corollary 1, but each vehicle has access to only a subset of the fleet's total state.

stabilizability imposed by Corollary 1, but that each vehicle only has access to a subset of the fleet's total state, a consequence of the vehicles' limited sensing abilities. The block diagonal subsystems are given by (3.11), with $\lambda_i \in \{3.0108, 4.6180, 4.6180, 2.3819, 2.3819\}$. For each of the five block diagonal subsystems, a GQLF was found by solving three LMIs in $\mathbb{R}^{2\times 2}$ to obtain five symmetric positive definite matrices:

$$\begin{aligned} P_1 &= \begin{bmatrix} 88.8184 & -27.8822 \\ -27.8822 & 64.5339 \end{bmatrix}, \\ P_2 = P_3 &= \begin{bmatrix} 0.0041 & -0.0099 \\ -0.0099 & 0.0831 \end{bmatrix}, \\ P_4 = P_5 &= \begin{bmatrix} 1.6822 & -3.3996 \\ -3.3996 & 22.0348 \end{bmatrix}. \end{aligned} \tag{3.14}$$

By Corollary 2, the GQLFs $V^i(x_i) = x_i^T P_i x_i$, $i \in \{1,...,5\}$ prove GUAS under arbitrary switching for the system as a whole. Figure 3.3 shows simulation results (top plot) for an arbitrary switching signal (bottom plot).

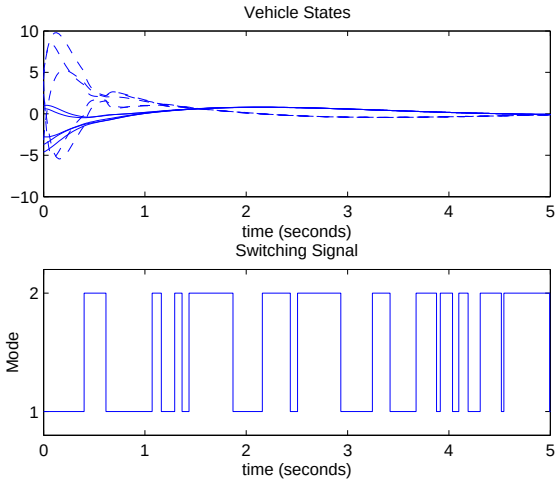

Figure 3.3: Simulation results for the five vehicle system given by (2.8), (3.12) and Laplacian (3.13), with mode switches occurring according to the arbitrary switching signal σ shown in the bottom plot. Shown are the position (top plot, solid) and velocity (top plot, dashed) variables of each of the vehicles.

100 vehicle system

Consider a 100 vehicle system with the same A_{cl}, K_1 and K_2 as in (3.12). The Laplacian L (not presented) is normalized such that all of its eigenvalues lie within a disk of radius 1 centered at $1+0j$ in the complex plane (cf. Proposition 2), and strongly connected such that its zero eigenvalue is simple (cf. Proposition 3), a necessary condition for the stability of such systems (cf. Corollary 1). For both K_1 and K_2, the block diagonal subsystems given by (3.11) are stable for all eigenvalues of L.

Solving three LMIs in $\mathbb{R}^{200\times 200}$ in Matlab was not possible on a dual core 2.40Ghz Intel-based machine with 4GB RAM due to the dimensionality of the system and ensuing memory requirements. Exploiting Corollary 2, we solve 100 sets of three LMIs to obtain a GQLF for each block diagonal subsystem instead. The LMIs solved are in $\mathbb{R}^{2\times 2}$ for block diagonal subsystems for which λ_i is real, and are in $\mathbb{R}^{4\times 4}$ when λ_i is complex. Simulation results are shown in Figure 3.4 for an arbitrary switching signal, depicted in Figure 3.5. As expected, despite

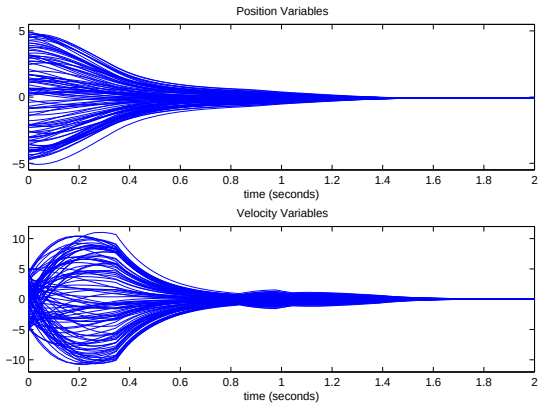

Figure 3.4: Simulation results for the 100 vehicle system given by (2.8), (3.12) and a strongly connected normalized Laplacian, with arbitrary switching signal σ shown in Figure 3.5. For such a large system, showing GUAS under arbitrary switching for the entire system proves to be computationally prohibitive unless stability is proven via Corollary 2. Shown are the position and velocity variables of each of the vehicles.

arbitrary switching, the vehicles' positions and velocities converge to zero. These results are equally applicable when the states are not driven to zero, but to some internally consistent offset values [24].

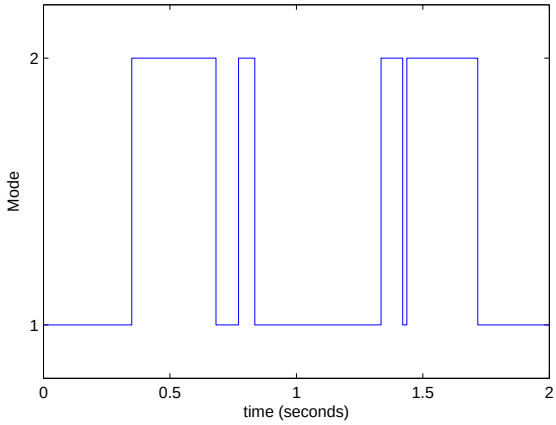

Figure 3.5: Arbitrary switching signal σ for the 100 vehicle system given by (2.8), (3.12) and a strongly connected normalized Laplacian. The simulation results are presented in Figure 3.4.

Chapter 4

Stability of switched linear systems under constrained switching

Communication and other types of delays are often present in distributed systems under cooperative control. This delay can represent a remote supervisory discrete controller (such as a human operator triggering mode changes) receiving delayed measurements, or the time required to synchronize a simultaneous mode switch amongst several subsystems. In the previous chapter, GUAS under *arbitrary* switching for a fleet of UAVs was proven by finding a CLF for each block diagonal subsystem. If this can be accomplished for all block diagonal subsystems, communication delays do not need to be taken into account – all switching sequences, delayed or not, will preserve stability.

However, not all systems have a CLF. The following delay-free canonical example from [9] illustrates how, for some systems, the switching sequence determines if the global behavior of the system is stable or not.

Example 1. *From [9]: Consider a two mode switched linear system*

$$\dot{x} = A_\sigma x \tag{4.1}$$

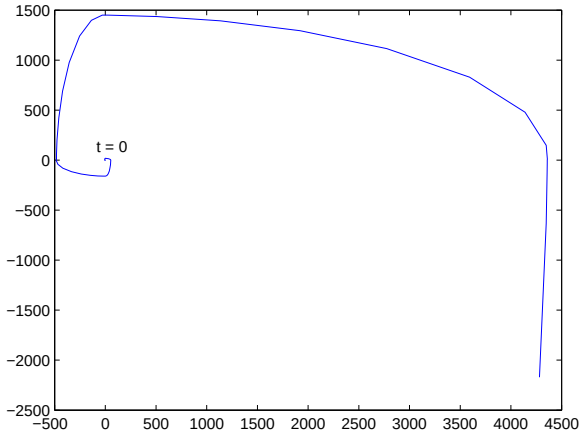

Figure 4.1: Trajectory for (4.1), with switching sequence such that $\dot{x} = A_1 x$ in the second and fourth quadrants, and $\dot{x} = A_2 x$ in the first and third quadrant, with initial conditions $x(0) = [10^{-6}, 0]^T$ over the time span $[0,1]$s. Despite individual modes having stable dynamics, the overall system behavior is that of an unstable one.

with $\mathscr{A} := \{A_1, A_2\}$, *where*

$$A_1 = \begin{bmatrix} -1 & 10 \\ -100 & -1 \end{bmatrix} \quad A_2 = \begin{bmatrix} -1 & 100 \\ -10 & -1 \end{bmatrix} \tag{4.2}$$

By switching modes such that $\dot{x} = A_1 x$ *in the second and fourth quadrants, and* $\dot{x} = A_2 x$ *in the first and third quadrant, the system exhibits unstable behavior. Shown in Figure 4.1 is the system trajectory in phase space starting from initial conditions* $x(0) = [10^{-6}, 0]^T$ *over the time span* $[0,1]$*s. However, if we reverse the switching scheme such that* $\dot{x} = A_1 x$ *in the first and third quadrant, and* $\dot{x} = A_2 x$ *in the second and fourth quadrant, the resulting system is stable. Shown in Figure 4.2 is the system trajectory in phase space starting from initial conditions* $x(0) = [1, 0]^T$ *over the time span* $[0,1]$*s.*

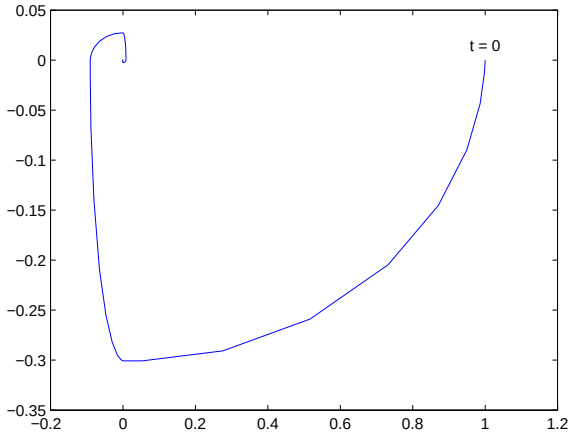

Figure 4.2: Trajectory for (4.1), with switching sequence such that $\dot{x} = A_1 x$ in the first and third quadrants, and $\dot{x} = A_2 x$ in the second and fourth quadrant, with initial conditions $x(0) = [1,0]^T$ over the time span $[0,1]$s. With this switching sequence, the system is GUAS.

4.1 Stability under state constrained switching

Example 1 clearly demonstrates how different *state-constraint* based switching rules can affect the GUAS of a system for which no CLF exists. Suppose that that for some of the block diagonal subystems (3.3) of (3.1), no CLF can be found. While stability under arbitrary switching is not possible, stability may hold for certain classes of switching signals. We address Problem 2 by first developing state constraint based switching signals such that (3.1) is GUAS under delay-free switching. We then introduce a *delay buffer* which adjusts the delay-free state constraints to be robust to switching delays.

Specifically, we focus on the i^{th} block diagonal subsystem (3.3), and for ease of notation, omit the i (sub)superscripts. For each mode $p \in \mathscr{P}$, let $V_p(x) = x^T P_p x$ be the associated Lyapunov function, where $x \in \mathbb{R}^n$ and $P_p = P_p^T > 0$ is a real symmetric positive definite matrix.

Theorem 5. *Consider a delay free switched system (3.1). Let Σ^* be the set of piecewise constant switching signals $\sigma : \mathbb{R}_+ \to \mathscr{P}$ such that, for each switching*

instant τ, $x(\tau) \in \bar{\mathscr{S}}(\sigma(\tau), \sigma(\tau^-))$, *where*

$$\bar{\mathscr{S}}(q,p) \quad := \quad \{x \in \mathbb{R}^n \,:\, V_p(x) - V_q(x) = x^T(P_p - P_q)x > 0\} \tag{4.3}$$

Then (3.1) is GUAS under Σ^*.

Proof. As in [9], Theorem 2.7. □

The condition imposed by Theorem 5 ensures that the piecewise Lyapunov function (PLF) $V_{\sigma(t)}(x)$ constructed from the the multiple Lyapunov functions $V_p,\ p \in \mathscr{P}$, is strictly decreasing at switching instants. However, in remote supervisory control, communication and other delays introduce a switching delay between state measurements and mode switches. Consequently, we include a switching delay T_D between the state measurements and switching time in our model – the discrete controller will only have access to a delayed state measurement $x(\tau - T_D)$ in determining whether the condition imposed by Theorem 5 will be violated if a mode switch occurs at time τ.

The premise behind our results is the same as that of Theorem 5: we impose conditions such that the PLF $V_{\sigma(t)}(x)$ is strictly decreasing, despite a switching delay. In order to accomodate the effect of the time delay, we introduce a *delay buffer* γ – this delay buffer introduces "no-switch" zones along the boundaries of $\bar{\mathscr{S}}(q,p)$ to ensure that system trajectories do cross over into $\bar{\mathscr{S}}(q,p)^c$ during the switching delay period. We compute γ by tracking the possible variations in the current and next modes' Lyapunov functions during the switching delay.

Lemma 1. *For a switched system (5.1), assume that* $\sigma(t) \equiv p$ *for* $t \in [\tau - T_D, \tau)$. *Then there exists positive constants* c_i *and* μ_i *such that*

$$\begin{array}{rcl} ||x_i(t)|| & \leq & c_i e^{-\mu_i(t-(\tau-T_d))}||x_i(\tau - T_D)|| \\ & & \forall t \in [\tau - T_D, \tau) \end{array} \tag{4.4}$$

for any x_i *corresponding to the* i^{th} *block diagonal subsystem, and* $\tau \geq T_D$.

Proof. Consider $||[x_{i+1}^T, ..., x_N^T]^T||$ as an exponentially decaying input to the dynamics of x_i, and apply Remark 2. □

In the following, we define $Q_p(q) := -(A_q^T P_p + P_p A_q)$ to track the evolution of mode q's Lyapunov function while $\sigma(t) = p$. Note that $Q_p(q) = Q_p^T(q)\ \forall p,q \in \mathscr{P}$.

Theorem 6. *Let Σ^{T_D} be the set of piecewise constant switching signals $\sigma : \mathbb{R}_+ \to \mathscr{P}$ such that, for each switching instant τ, $x(\tau - T_D) \in \mathscr{S}(\sigma(\tau), \sigma(\tau^-), \tau)$, with*

$$\mathscr{S}(q,p,\tau) \quad := \quad \{x \in \mathbb{R}^n \ : \ \tfrac{x^T(P_p - P_q)x}{||x||^2} > \gamma(q,p,\tau)\} \tag{4.5}$$

the set of states for which switching from mode p to q is allowed for a time-varying delay buffer

$$\gamma(q,p,\tau) \quad = \quad \tfrac{c_p^2 e^{-2\lambda_p \tau}}{2\lambda_p}(e^{2\lambda_p T_D} - 1)(\lambda_{max}(Q_p(p)) - \min(0, \lambda_{min}(Q_q(p)))) \tag{4.6}$$

and constants $c_p, \lambda_p > 0$ for mode p as in Definition 3. Then (3.1) is GUAS under Σ^{T_D}.

Proof. By Theorem 5, a sufficient condition for $\sigma \in \Sigma^*$ is that at each switching instant τ

$$V_p(x(\tau)) - V_q(x(\tau)) > 0 \tag{4.7}$$

where $\sigma(\tau^-) = p$ and $\sigma(\tau) = q$. We show that $\Sigma^{T_D} \subseteq \Sigma^*$ by finding a lower bound for (4.7) given only $x(\tau - T_D)$, and partitioning the state space accordingly.

We seek to bound $V_p(x)$ and $V_q(x)$ from below and above, respectively.

$$\begin{array}{rcl} V_p(x(\tau)) & = & V_p(x(\tau - T_D)) + \int_{\tau - T_D}^{\tau} \dot{V}_p(x(t))dt \\ & = & V_p(x(\tau - T_D)) - \int_{\tau - T_D}^{\tau} x^T(t) Q_p(p) x(t) dt \end{array} \tag{4.8}$$

By the Courant-Fischer theorem

$$\lambda_{min}(Q_p(p))||x||^2 \ \leq \ x^T Q_p(p) x \ \leq \ \lambda_{max}(Q_p(p))||x||^2 \tag{4.9}$$

and $\lambda_{min}(Q_p(p)) > 0$, we obtain

$$V_p(x(\tau)) \quad \geq \quad V_p(x(\tau - T_D)) - \int_{\tau - T_D}^{\tau} \lambda_{max}(Q_p(p))||x(t)||^2 dt \tag{4.10}$$

Applying (3.4) and evaluating the integral, we obtain a lower bound for $V_p(x(\tau))$.

$$\begin{aligned} V_p(x(\tau)) &\geq V_p(x(\tau - T_D)) \\ &\quad -\frac{c_p^2 e^{-2\lambda_p \tau}}{2\lambda_p}(e^{2\lambda_p T_D} - 1)\lambda_{max}(Q_p(p))||x(\tau - T_D)||^2 \end{aligned} \tag{4.11}$$

Similarly, to find an upper bound to $V_q(x(\tau))$,

$$\begin{aligned} V_q(x(\tau)) &= V_q(x(\tau - T_D)) - \int_{\tau - T_D}^{\tau} x^T(t) Q_p(q) x(t) dt \\ &\leq V_q(x(\tau - T_D)) - \int_{\tau - T_D}^{\tau} \lambda_{min}(Q_p(q))||x(t)||^2 dt \end{aligned} \tag{4.12}$$

If $\lambda_{min}(Q_p(q)) < 0$, the integral term is positive, and we use the upper bound for $||x(t)||$ given by (3.4) to further bound (4.10), and obtain a result similar to (4.11). However, if $\lambda_{min}(Q_p(q)) \geq 0$, the integral term is negative, and we require a lower bound for $||x(t)||$ to further bound (4.10). In general, such a lower bound is unavailable, but can be conservatively approximated as 0. Combining these two cases, an upper bound for (4.12) is

$$\begin{aligned} V_q(x(\tau)) &\leq V_q(x(\tau - T_D)) \\ &\quad -\frac{c_p^2 e^{-2\lambda_p \tau}}{2\lambda_p}(e^{2\lambda_p T_D} - 1)\min(0, \lambda_{min}(Q_p(q))))||x(\tau - T_D)||^2 \end{aligned} \tag{4.13}$$

Combining (4.11), (4.13) with (4.7),

$$\frac{V_p(x(\tau - T_D)) - V_q(x(\tau - T_D))}{||x(\tau - T_D)||^2} > \gamma(q, p, \tau) \tag{4.14}$$

where γ is as given in (4.6). Noticing that $V_m(x) = x^T P_m x$ for $m \in \mathscr{P}$, and letting $\mathscr{S}(q, p, \tau)$ be the subset of $\mathbb{R}^n$ where (4.14) holds, we obtain (4.5).

Thus, for any piecewise constant switching signal $\sigma \in \Sigma^{T_D}$, we have $\sigma \in \Sigma^*$, thus $\Sigma^{T_D} \subseteq \Sigma^*$. □

An interesting consequence of this approach is that the delay buffer γ is in fact a time varying quantity. This time dependence occurs because the upper bound of the time derivative of the Lyapunov functions (4.9) is proportional to the norm of the state $||x(t)||$, a time varying quantity. For switching signals $\sigma \in \Sigma^{T_D}$, a system (3.1) is GUAS, and the state norm asymptotically approaches zero – consequently, *so does the time derivative of each Lyapunov function*. This observation,

and its consequences on the time-varying parititions, are summarized in the following corollary:

Corollary 3. *For $\sigma \in \Sigma^{T_D}$, as $t \to \infty$, the delay buffer adjusted partition $\mathscr{S}(q,p,\tau) \to \bar{\mathscr{S}}(q,p)$ for all $p,q \in \mathscr{P}$.*

Proof. We fix a "next mode" q and study the evolution of $\mathscr{S}(q,\sigma(t),t)$ under a switching signal $\sigma \in \Sigma^{T_D}$ in order to determine how these regions evolve over time. We define the functional $\gamma(q,\cdot,\cdot) : \mathscr{P} \times \mathbb{R}_+ \to \mathbb{R}$, evolving under a switching signal $\sigma \in \Sigma^{T_D}$, as

$$\gamma(q,\sigma(t),t) = \frac{c_{\sigma(t)}^2 e^{-2\lambda_{\sigma(t)}t}}{2\lambda_{\sigma(t)}}(e^{2\lambda_{\sigma(t)}T_D}-1)(\lambda_{max}(Q_{\sigma(t)}(\sigma(t))) - \min(0,\lambda_{min}(Q_q(\sigma(t)))))) \tag{4.15}$$

For all $p,q \in \mathscr{P}$, $t \geq T_D$, $\gamma(q,p,t) \geq 0$. It follows that $\gamma(q,\sigma(t),t) \geq 0 \ \forall \sigma \in \Sigma^{T_D}$.

Define

$$\begin{aligned} \alpha &= \max_{\sigma(t)} \frac{c_{\sigma(t)}^2}{2\lambda_{\sigma(t)}}(e^{2\lambda_{\sigma(t)}T_D}-1) \\ \beta &= \max_{\sigma(t)}(\lambda_{max}(Q_{\sigma(t)}(\sigma(t))) - \min(0,\lambda_{min}(Q_q(\sigma(t))))) \\ \Lambda &= \min_{\sigma(t)} \lambda_{\sigma(t)} \end{aligned} \tag{4.16}$$

Then

$$0 \leq \gamma(q,\sigma(t),t) \leq \alpha\beta e^{-2\Lambda t} \tag{4.17}$$

Thus $\gamma(q,\sigma(t),t) \to 0$ as $t \to \infty$ for all $\sigma \in \Sigma^{T_D}$. Letting the final active mode of σ be p, the result follows. □

Corollary 3 shows that by waiting long enough before switching, the delay buffer γ for any mode pair can be made as small as desired. Specifically, if for some $\tau^*, \gamma^* \in \mathbb{R}$, $\gamma(p,q,\tau^*) < \gamma^*$, then $\gamma(p,q,t) < \gamma^*$ for all $t \geq \tau^*$ – once this condition is satisfied, it is satisfied for all future times, and hence can be thought of as a *wait-time* condition. In contrast, the average dwell-time condition presented in [31], and its extension to switched systems with switching and state delays [67], must be satisfied after each mode switch in order to guarantee asymptotic stability

of a switched linear system. Wait-time instead provides a time τ^* after which the effect of the delay buffer becomes negligible. In practical applications, the wait-time condition and the average dwell-time conditions can in fact be seen as being complementary. Our method will prove useful when mode switches need to occur rapidly, and may violate dwell-time conditions; on the other hand, dwell-time arguments can be used when mode switches occur at a slower pace, elminating the need for state measurements to be transmitted back to the remote operator.

Alternatively, we can consider $\mathscr{S}(q,p,\tau)$ as a conservative estimate of $\bar{\mathscr{S}}(q,p)$ that has been propagated backwards in tme for T_D seconds. It can be argued that a natural alternative to our method would be to use reachability techniques (cf. [4, 43, 51, 63], among others) to compute this backwards propagation, rather than using our initially conservative estimate. This reachability computed set may initially be less conservative, as it does not rely on bounds on derivatives in its computation. Although in some cases, this might yield useful results, we argue that our approach has some important advantages over reachability based techniques. Most importantly, the computed reachable set is static, and hence does not allow the remote operator to take advantage of the decreasing effect of the delay buffer.

4.2 Design and implementation strategies

Theorems 4 and 6 aid in the design and analysis for switched linear systems under distributed control. Theorem 4 is first used to prove GUAS under arbitrary switching for as many block diagonal subsystems as possible. Theorem 6 is then used to synthesize state based constraints for the remaining block diagonal subsystems. Specifically, consider a switch from mode p to mode q occuring at time $t=\tau$, and an index set $\mathscr{I} \subseteq \{1,...,N\}$ comprised of the indices of all block diagonal subsystems that are not GUAS under arbitrary switching. For each $i \in \mathscr{I}_{na}$, thetime-varying partition $\mathscr{S}^i(q,p,\tau)$ corresponding to the i^{th} block diagonal subsystem needs to be computed. Only when the delayed measurement $x_i(\tau - T_D) \in \mathscr{S}^i(q,p,\tau)$ *for all* $i \in \mathscr{I}$, that is for all block diagonal subsystems for which a CLF does not exist, will a mode switch from p to q be guaranteed to preserve GUAS despite a switching delay.

To reduce the complexity of these state based constraints as much as possible,

the designer of such systems will want to minimize the number of block diagonal subsystems (3.3) that are not GUAS under arbitrary switching. From Lemma 1, we see that for block diagonal subsystems of lower index, the effect of other states on its bounding constants is more significant. If these subsystems are not GUAS under arbitrary switching, these larger bounding constants will in turn increase the effect of the delay buffer (4.6) on the state partitions. Hence, a prudent design strategy would be to (1) choose a communication topology that minimizes the number of block diagonal subsystems that are not GUAS under arbitrary switching and (2) to exploit the Schur transformation's ability to arbitrarily order eigenvalues to ensure that all of these unstable block diagonal subsystems are placed in the lowest blocks possible. State constraints can then be developed according to Theorem 6 for each of these block diagonal subsystems.

In some cases, the structure of the sets $\mathscr{S}(q,p,\tau)$ (4.5) can be quickly determined by examining the spectral properties of $P_p - P_q$. If $\lambda_{\min}(P_p - P_q) > \gamma(q,p,\tau)$, then $\mathscr{S}(q,p,\tau) = \mathbb{R}^n$ – the safe switching region from mode p to mode q constitutes the entire state space, so a switch from mode p to q can be triggered at any time. Similarly, if $\lambda_{\max}(P_p - P_q) < \gamma(q,p,\tau)$, then $\mathscr{S}(q,p,\tau) = \emptyset$, and the safe switching region is empty – a remote operator will have to wait for γ to decrease enough such that $\lambda_{\max}(P_p - P_q) > \gamma(q,p,\tau)$ before a switch may be triggered safely. By computing these minimum (maximum) eigenvalues beforehand, it can quickly be determined if a given mode switch at time $t = \tau$ will always (never) be guaranteed to preserve GUAS despite a switching delay.

4.2.1 Application to fleets of UAVs

The wait-time condition has a very important consequence when applied to UAV systems: often times a UAV will operate in a given mode for an extended period of time (e.g. "return to base") before switching through other modes more rapidly (e.g. "lower landing gear", "change flaps configuration", "acquire glide slope"). However, since the wait-time is not reset after each mode switch, the effect of the delay buffer on the state partitions during the final sequence of rapid mode switches will already have decayed to a negligible level.

4.3 Example: remote supervisory control of a switched linear system

The application in this section is a continuation of Example 1. Although the dynamics are not directly related to a UAV system, they illustrate both the effectiveness and generality of the developed methods. It is also important to note that although the results were derived in the context of fleets of identical switched linear vehicles, they are equally applicable to any switched linear system.

Consider the two mode switched linear system (4.1) described in Example 1 with a switching delay $T_D = .1$s. As illustrated previously, unstable switching sequences exist, and hence no CLF exists for this switched linear system. According to Theorem 6, we partition the state space into delay buffer adjusted regions $\mathscr{S}(2,1,t)$ and $\mathscr{S}(1,2,t)$, which provide switching restrictions that preserve GUAS despite the switching delay. Figure 4.3 shows snapshots of $\mathscr{S}(2,1,t)$ (white) evolving over time under the switching signal $\sigma(t) \equiv 1$. In accordance to Corollary 3, $\mathscr{S}(2,1,t)$ converges to the standard Lyapunov based partitioning $\bar{\mathscr{S}}(2,1)$ as the delay buffer $\gamma(2,1,t)$ approaches zero.

Figure 4.4 shows the evolution of $\gamma(2,\sigma(t),t)$ and of $V_{12}(t) := (x(t)^T(P_1 - P_2)x(t))/(||x(t)||^2)$, and the switching signal $\sigma \in \Sigma^{T_D}$ generated by switching whenever possible without violating the constraints imposed by Theorem 6. Initially $\gamma(2,1,t) > \lambda_{\max}(P_1 - P_2)$ is too large to allow any mode switches and $\mathscr{S}(2,1,t) = \emptyset$. After approximately 1.3s, the delay buffer has decayed enough such that $\gamma(2,1,t) < \lambda_{\max}(P_1 - P_2)$, and a mode switch is triggered as soon as the delayed trajectory $x(t - T_D)$ enters $\mathscr{S}(2,1,t)$. In Figure 4.5, we zoom in on when $x(t - T_D) \in \mathscr{S}(2,1,t)$ for the first time, at $t = \tau$. Clearly, $V_{12}(\tau) > 0$, satisfying the stability requirements imposed by Theorem 5. The resulting trajectory in the phase space is presented in Figure 4.6, with subsets of the trajectory evolving according to $\dot{x} = A_1 x$ plotted in black (dark), and those evolving according to $\dot{x} = A_2 x$ plotted in cyan (light), where a switch occurs as soon as the trajectory enters a region of the state space in which switching is allowed. Notice that convergence to the origin is much faster once switching begins to occur more regularly, illustrating the potential benefits of applying hybrid control to a system.

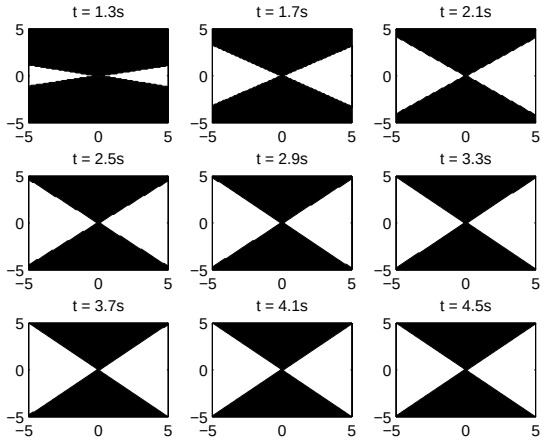

Figure 4.3: Snapshots of the $\mathscr{S}(2,1,t)$ (white) evolving over time under the switching signal $\sigma(t) \equiv 1$. $\mathscr{S}(2,1,t)$ converges to the standard Lyapunov based partitioning $\mathscr{S}(2,1)$ (Corollary 3).

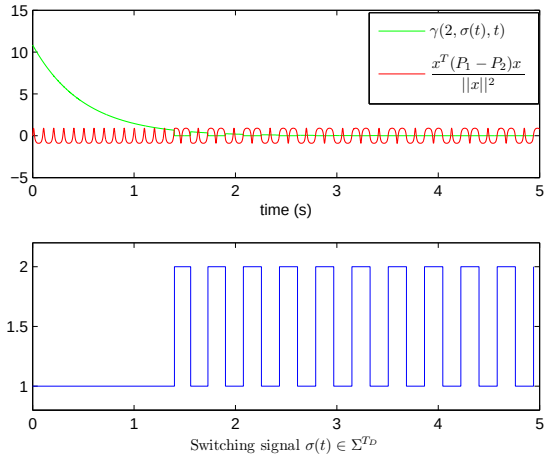

Figure 4.4: Evolution of the delay buffer $\gamma(2,\sigma(t),t)$ overlaid with $V_{12}(t) \triangleq (x(t)^T(P_1-P_2)x(t))/(||x(t)||^2)$, and the switching signal generated by switching whenever possible without violating the constraints imposed by Theorem 6. Initially $\gamma(2,1,t) > \lambda_{\max}(P_1-P_2)$ is too large to allow any mode switches, and consequently, $\mathscr{S}(2,1,t) = \emptyset$. After approximately 1.3s, $\gamma(2,1,t) < \lambda_{\max}(P_1-P_2)$, and a mode switch is triggered as soon as the delayed trajectory $x(t-T_D)$ enters $\mathscr{S}(2,1,t)$.

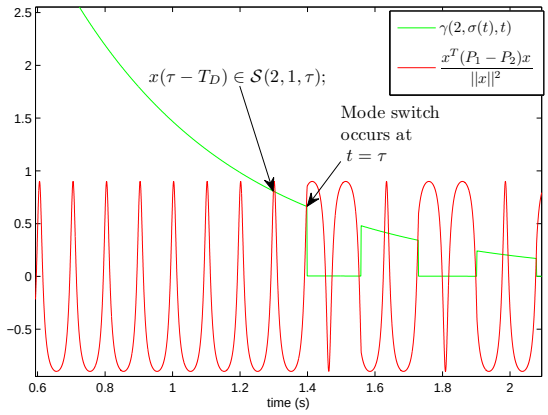

Figure 4.5: From Figure 4.4, a close view of when $x(\tau - T_D) \in \mathscr{S}(2,1,\tau)$ for the first time at $t = \tau$. Clearly, $V_{12}(\tau) > 0$, satisfying the stability requirements imposed by Theorem 5.

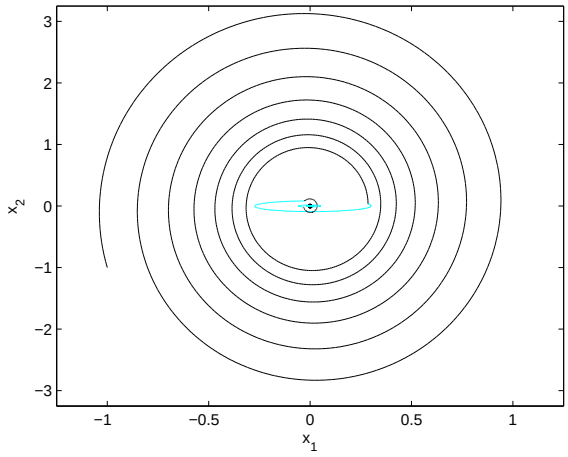

Figure 4.6: Trajectory in the phase space generated by system (4.2), switching according to a signal $\sigma \in \Sigma^{T_D}$, with subsets of the trajectory evolving according to $\dot{x} = A_1 x$ plotted in black (dark), and those evolving according to $\dot{x} = A_2 x$ plotted in cyan (light).

Chapter 5

Stability of switched nonlinear systems under constrained switching

Although a rich and wide range of systems can be modeled as having linear dynamics, many systems exist which have inherently nonlinear properties. In this chapter, we extend results from Chapter 4 to nonlinear switched systems. We begin by introducing the switched nonlinear systems to be studied in this chapter, as well as the relevant definitions of stability. Similarly to Chapter 4, we use a PLF approach to stable switching despite a switching delay by introducing a delay buffer to quantify the effect of the switching delay on the delay free PLF based partitions. We then present two examples of stable switching despite a switching delay.

5.1 Problem formulation

Consider a switched nonlinear system

$$\dot{x} = f_{\sigma(t)}(t,x) \tag{5.1}$$

with $x \in \mathbb{R}^n$, $\sigma : \mathbb{R}_+ \to \mathscr{P} \subset \mathbb{N}$ a piecewise constant switching signal, and $\mathscr{F} := \{ f_p : \mathbb{R}_+ \times \mathscr{D} \to \mathbb{R}^n \, : \, p \in \mathscr{P} \}$ a family of functions indexed by p that are piecewise

continuous in t and locally Lipschitz in x on $\mathbb{R}_+ \times \mathscr{D}$, $\mathscr{D} \subset \mathbb{R}^n$ a domain containing the origin. We assume the origin to be an equilibrium point for each $f_p \in \mathscr{F}$ without loss of generality. The following definitions all deal with local stability, unless specificed otherwise.

Definition 4. *Modified from [41]: the equilibrium point $x = 0$ of (5.1) is* stable under Σ^**, a set of piecewise constant switching signals, if* $\forall \varepsilon > 0\ \exists \delta = \delta(\varepsilon, t_0) > 0$ *such that*

$$||x(t_0)|| < \delta \ \Rightarrow\ ||x(t)|| < \varepsilon,\ \forall t \geq t_0 \geq 0 \tag{5.2}$$

for all $\sigma \in \Sigma^*$.

Lemma 2. *Modified from [41]: the equilibrium point $x = 0$ for (5.1) is*

- uniformly stable (US) under Σ^* *if and only if there exists a class $\mathscr{K}$ function α and a positive constant c, independent of t_0, such that*

$$||x(t)|| \leq \alpha(||x(t_0)||),\ \forall t \geq t_0 \geq 0,\ \forall ||x(t_0)|| < c \tag{5.3}$$

  for all $\sigma \in \Sigma^*$.

- uniformly asymptotically stable (UAS) under Σ^* *if and only if there exists a class $\mathscr{K}\mathscr{L}$ function β and a positive constant c, independent of t_0, such that*

$$||x(t)|| \leq \beta(||x(t_0)||, t - t_0),\ \forall t \geq t_0 \geq 0,\ \forall ||x(t_0)|| < c \tag{5.4}$$

  for all $\sigma \in \Sigma^*$.

Remark 4. *If $\Sigma^* = \{p\}$, (i.e. $\sigma(t) \equiv p$), the previous definition and lemma are equivalent to standard definitions of stability for a nonlinear system.*

Remark 5. *The results of Lemma 2 will hold globally for $c = \infty$.*

We focus on systems which cannot be shown to be stable under arbitrary switching. Specifically, we address the problem of determining state based switching constraints such that (5.1) is stable, US, UAS or GUAS, despite a bounded delay between state measurements and switching time, or *switching delay*. We focus on systems (5.1) for which $\mathscr{F}$ is comprised of functions that have the same type of stability.

5.2 Stability under state constrained switching

We begin by assuming that for system (5.1), $\dot{x} = f_p(t,x),\ p \in \mathscr{P}$ has a *stable* equilibrium point $x^* = 0$ over a domain $\mathscr{D} \subset \mathbb{R}^n$. We assume that there exists a continuously differentiable Lyapunov function $V_p(t,x) : \mathbb{R}_+ \times \mathscr{D} \to \mathbb{R}$ satisfying the following standard conditions (cf. [41])

$$V_p(t,x) > 0 \tag{5.5}$$

$$\frac{\partial V_p}{\partial t} + \frac{\partial V_p}{\partial x} f_p(t,x) \leq 0 \tag{5.6}$$

for all $t \geq 0$ and all $x \in \mathscr{D}\backslash\{0\}$. In addition, we assume that the function $\delta(\varepsilon, t_0)$ as given in Definition 4 is invertible, such that for any $\delta, t_0 \in \mathbb{R}_+$, one can compute

$$\varepsilon = \varepsilon(\delta, t_0) \tag{5.7}$$

satisfying (5.2).

In order to establish stability of (5.1), we define a piecewise continuous Lyapunov function

$$V(t,x) = V_{\sigma(t)}(t,x) \tag{5.8}$$

and characterize a class of switching signals such that (5.8) is non-increasing, despite a switching delay of duration T_D. As in the linear case, we first develop delay free state paritions that ensure (5.8) is strictly decreasing, and then introduce a delay buffer to compensate for the effect of the switching delay. Once again, we compute the delay buffer by bounding the possible changes in the Lyapunov function of the current mode ($V_p(t,x)$) and the Lyapunov function of the next mode ($V_q(t,x)$) over the period of the time delay. We first make two assumptions that allow the time derivative of the two Lyapunov functions $V_p(t,x)$ and $V_q(t,x)$ to be bounded.

Assumption 1. *There exists a class $\mathscr{K}$ function $\alpha_p(||x||)$ such that*

$$-\alpha_p(||x||) \leq \frac{\partial V_p}{\partial t} + \frac{\partial V_p}{\partial x} f_p(t,x) \leq 0 \tag{5.9}$$

Assumption 2. *There exists a class $\mathscr{K}$ function $\alpha_{qp}(||x||)$ and a real constant*

$b_{qp} \in \{-1,1\}$ *such that*

$$\frac{\partial V_q}{\partial t} + \frac{\partial V_q}{\partial x} f_p(t,x) \leq b_{qp}\alpha_{qp}(||x||) \tag{5.10}$$

Note that these assumptions are not restrictive at all – for example, they will hold if the Lyapunov functions are all Lipschitz continuous (a very broad class of functions), as this will limit the magnitude of their derivatives.

Theorem 7. *Let Σ^s be the set of piecewise constant switching signals $\sigma : \mathbb{R}_+ \to \mathscr{P}$ such that (5.1) is stable. Let $\Sigma^s_{T_D}$ be the set of piecewise constant switching signals such that, for each switching instant τ, $x(\tau - T_D) \in \mathscr{S}^s(\sigma(\tau), \sigma(\tau^-), \tau)$, with*

$$\mathscr{S}^s(q,p,\tau) \quad := \quad \{x \in \mathscr{D} \,:\, V_p(\tau - T_D, x) - V_q(\tau - T_D, x) \geq \gamma^s(q,p,\tau)\} \tag{5.11}$$

the set of states for which switching from mode p to mode q is allowed for a time-varying delay buffer

$$\begin{aligned} \gamma^s(q,p,\tau) \quad = \quad & T_D \cdot [\alpha_p(\varepsilon(||x(\tau - T_D||), \tau - T_D)) \\ & + \max(0, b_{qp}) \cdot \alpha_{qp}(\varepsilon(||x(\tau - T_D||), \tau - T_D))] \end{aligned} \tag{5.12}$$

with $\varepsilon(\cdot,\cdot)$ is given as in (5.7) and $\alpha_p(\cdot)$, $\alpha_{qp}(\cdot)$, and b_{qp} satisfy Assumptions 1 and 2. Then (5.1) is stable under $\Sigma^s_{T_D}$.

Proof. From Lyapunov stability theory, a sufficient condition for a switching signal $\sigma \in \Sigma^s$ is that the piecewise continuous Lyapunov function (5.8) be non-increasing. This is equivalent to requiring that at each switching instant τ,

$$V_p(\tau, x(\tau)) - V_q(\tau, x(\tau)) \geq 0 \tag{5.13}$$

with $\sigma(\tau^-) = p$ and $\sigma(\tau) = q$. We show that $\Sigma^s_{T_D} \subseteq \Sigma^s$ by finding a lower bound for (5.13) based only on information available when the switch is triggered, i.e. $x(\tau - T_D)$, and partitioning the state space such that (5.13) holds at each switching instant, despite a switching delay T_D.

We seek to bound $V_p(t,x)$ and $V_q(t,x)$ from below and above, respectively.

$$V_p(\tau, x(\tau)) \quad = \quad V_p(\tau - T_D, x(\tau - T_D)) + \int_{\tau - T_D}^{\tau} \left(\tfrac{\partial V_p}{\partial t} + \tfrac{\partial V_p}{\partial x} f_p(t,x) \right) dt \tag{5.14}$$

Applying (5.9) we obtain

$$V_p(\tau, x(\tau)) \geq V_p(\tau - T_D, x(\tau - T_D)) - \int_{\tau - T_D}^{\tau} \alpha_p(||x(t)||)dt \tag{5.15}$$

Applying (5.2),(5.7) to bound $||x(t)||$ over $[\tau - T_D, \tau)$, the integrand becomes constant ($\alpha_p(\varepsilon(||x(\tau - T_D)||, \tau - T_D))$). Thus evaluating the integral, we obtain a lower bound for $V_p(\tau, x(\tau))$ given $x(\tau - T_D)$,

$$V_p(\tau, x(\tau)) \geq V_p(\tau - T_D, x(\tau - T_D)) - T_D \cdot \alpha_p(\varepsilon(||x(\tau - T_D)||, \tau - T_D)) \tag{5.16}$$

Similarly, to find an upper bound to $V_q(\tau, x(\tau))$,

$$\begin{aligned} V_q(\tau, x(\tau)) &= V_q(\tau - T_D, x(\tau - T_D)) + \int_{\tau - T_D}^{\tau} \left(\frac{\partial V_q}{\partial t} + \frac{\partial V_q}{\partial x} f_p(t, x) \right) dt \\ &\leq V_q(\tau - T_D, x(\tau - T_D)) + \int_{\tau - T_D}^{\tau} b_{qp} \alpha_{qp}(||x(t)||)dt \end{aligned} \tag{5.17}$$

If $b_{qp} = 1$, the integral term is positive, and we use the upper bound for $||x(t)||$ given by (5.2), (5.7) to further bound (5.15), and obtain a result similar to (5.16). However, if $b_{qp} = -1$, the integral term is negative, and we require a lower bound for $||x(t)||$ to further bound (5.15). In general, such a lower bound is unavailable, but can be conservatively approximated as 0. Combining these two cases, an upper bound for (5.17) is

$$\begin{aligned} V_q(\tau, x(\tau)) &\leq V_q(\tau - T_D, x(\tau - T_D)) \\ &+ \max(0, b_{qp}) \cdot T_D \cdot \alpha_{qp}(\varepsilon(||x(\tau - T_D)||, \tau - T_D) \end{aligned} \tag{5.18}$$

Combining (5.16), (5.18) with (5.13),

$$V_p(\tau - T_D, x(\tau - T_D)) - V_q(\tau - T_D, x(\tau - T_D)) \geq \gamma^s(q, p, \tau) \tag{5.19}$$

with γ^s given as in (5.12). Letting $\mathscr{S}^s(q, p, \tau)$ be the subset of $\mathscr{D}$ where (5.19) holds, we obtain (5.11). Thus, for any piecewise constant switching signal $\sigma \in \Sigma^s_{T_D}$, we have $\sigma \in \Sigma^s$, thus $\Sigma^s_{T_D} \subseteq \Sigma^s$. □

The sets $\mathscr{S}^s(q, p, \tau)$ thus partition the state space into regions where switching from mode p to mode q ensures (5.8) is non-increasing, guaranteeing the stabil-

ity of (5.1), despite a switching delay T_D. Computing the delay buffer γ^s given a delayed measurement $x(\tau - T_D)$ is trivial once functions α_p, α_{qp} and constant b_{qp} have been determined, and can be easily be performed online, resulting in a computationally efficient manner of verifying whether a desired switch between two modes is allowable.

Consider the following two corollaries in which we strengthen our results for US and UAS mode dynamics.

Corollary 4. *Let Σ^{us} be the set of piecewise constant switching signals $\sigma : \mathbb{R}_+ \to \mathscr{P}$ such that (5.1) is uniformly stable. Let $\Sigma^{us}_{T_D}$ be the set of piecewise constant switching signals such that, for each switching instant τ,*
$x(\tau - T_D) \in \mathscr{S}^{us}(\sigma(\tau), \sigma(\tau^-), \tau)$, with

$$\mathscr{S}^{us}(q,p,\tau) \;:=\; \{x \in \mathscr{D} \,:\, V_p(\tau - T_D, x) - V_q(\tau - T_D, x) \geq \gamma^{us}(q,p,\tau)\} \tag{5.20}$$

the set of states for which switching from mode p to mode q is allowed for a time-varying delay buffer

$$\begin{aligned} \gamma^{us}(q,p,\tau) \;=\; & T_D[\alpha_p(\bar{\alpha}_p(||x(\tau - T_D||)) \\ & + \max(0, b_{qp})\alpha_{qp}(\bar{\alpha}_p(||x(\tau - T_D||)))] \end{aligned} \tag{5.21}$$

where $\bar{\alpha}_p(\cdot)$ satisfies (5.3) and $\alpha_p(\cdot)$, $\alpha_{qp}(\cdot)$,and b_{qp} satisfy Assumptions 1 and 2.

Proof. Similar to Theorem 7: When bounding equations (5.15) and (5.17), we use $\bar{\alpha}_p(||x(\tau - T_D)||)$ as an upper bound for $||x(t)||$ over $[\tau - T_D, \tau)$ instead of (5.2), (5.7). □

Corollary 5. *Let Σ^{uas} be the set of piecewise constant switching signals $\sigma : \mathbb{R}_+ \to \mathscr{P}$ such that (5.1) is UAS. Let $\Sigma^{uas}_{T_D}$ be the set of piecewise constant switching signals such that, for each switching instant τ, $x(\tau - T_D) \in \mathscr{S}^{uas}(\sigma(\tau), \sigma(\tau^-), \tau)$, with*

$$\mathscr{S}^{uas}(q,p,\tau) \;:=\; \{x \in \mathscr{D} \,:\, V_p(\tau - T_D, x) - V_q(\tau - T_D, x) \geq \gamma^{uas}(q,p,\tau)\} \tag{5.22}$$

the set of states for which switching from mode p to mode q is allowed for a time-

varying delay buffer

$$\begin{aligned}\gamma^{uas}(q,p,\tau) &= \int_{\tau-T_D}^{\tau} \alpha_p(\beta_p(||x(\tau-T_D)||, t-(\tau-T_D)))dt \\ &\quad + \max(0,b_{qp}) \int_{\tau-T_D}^{\tau} \alpha_{qp}(\beta_p(||x(\tau-T_D)||, t-(\tau-T_D)))dt\end{aligned} \tag{5.23}$$

where $\alpha_p(\cdot)$, $\alpha_{qp}(\cdot)$, and b_{qp} satisfy Assumptions 1 and 2, and $\beta_p(\cdot)$ is the bounding function (5.4) for mode p.

Proof. Similar to Theorem 7: When bounding equations (5.15) and (5.17), we use $\beta_p(||x(\tau-T_D)||, t-(\tau-T_D))$ as an upper bound for $||x(t)||$ over $[\tau-T_D, \tau)$ instead of (5.2), (5.7). □

As in the linear case, the delay buffer γ^{uas} is time dependent, and an analogous wait-time condition applies here.

Corollary 6. *For $\sigma \in \Sigma_{T_D}^{uas}$, as $t \to \infty$, the time-varying partition $\mathscr{S}^{uas}(q,p,\tau) \to \bar{\mathscr{S}}^{uas}(q,p,\tau)$ for all $p,q \in \mathscr{P}$, where*

$$\bar{\mathscr{S}}^{uas}(q,p,\tau) := \{x \in \mathbb{R}^n : V_p(x) - V_q(x) > 0\} \tag{5.24}$$

is a delay free PLF based partitioning of the state space which guarantees UAS of (5.1).

Proof. We fix a "next mode" q and study the evolution of $\mathscr{S}^{uas}(q,\sigma(t),t)$ under a switching signal $\sigma \in \Sigma_{T_D}^{uas}$ in order to determine how these regions evolve over time. We define the functional $\gamma^{uas}(q,\cdot,\cdot) : \mathscr{P} \times \mathbb{R}_+ \to \mathbb{R}$, evolving under a switching signal $\sigma \in \Sigma_{T_D}^{uas}$, as

$$\begin{aligned}\gamma^{uas}(q,\sigma(t),t) &= \int_{t-T_D}^{t} \alpha_{\sigma(t)}(\beta_{\sigma(t)}(||x(t-T_D)||, r-(t-T_D)))dr \\ &\quad + \max(0,b_{q\sigma(t)}) \int_{t-T_D}^{t} \alpha_{q\sigma(t)}(\beta_{\sigma(t)}(||x(t-T_D)||, r-(t-T_D)))dr\end{aligned} \tag{5.25}$$

For all $\sigma \in \Sigma_{T_D}^{uas}$, (5.1) is UAS, and by Lemma 2, there exists a class $\mathscr{KL}$ function β satisfying (5.4). Hence $||x(t)|| \to 0$ as $t \to \infty$, implying that the integral terms in (5.25) asymptotically approach 0 as well. Thus the delay buffer $\gamma^{uas}(q,\sigma(t),t) \to 0$ as $t \to \infty$ for all $\sigma \in \Sigma_{T_D}^{uas}$. Letting the final active mode of σ be p, the result follows. □

The results in this section can be applied to any nonlinear switched system, including a single switched nonlinear UAV. Furthermore, although not scalable to large systems, these results could also be combined with the Lyapunov based proofs of stability of fleets of nonlinear systems found in [14], extending their applicability to smaller fleets of UAVs under distributed control.

5.3 Design and implementation issues

In general it will not be possible to obtain analytical expressions for the necessary bounding functions β_p. While Lyapunov theory guarantees the existence of such a function, it is the solution of an ordinary differential equation (ODE) (cf. Theorem 4.9, Lemma 4.4 and Appendix C.5, [41]), which may not have an analytical solution. Fortunately, the ODE is scalar, so numerical and curve fitting methods can be used to obtain conservative analytic bounds on the true β_p functions.

5.4 Examples

5.4.1 Autonomous nonlinear switched system with UAS mode dynamics

Consider a system (5.1) with $\mathscr{F} = \{f_1(x), f_2(x)\}$, $x = [x_1, x_2]^T \in \mathbb{R}^2$ and f_i

$$f_1(x) = \begin{bmatrix} -x_1 + 2x_2^3 - 2x_2^4 \\ -x_1 - x_2 + x_1 x_2 \end{bmatrix} \tag{5.26}$$

$$f_2(x) = \begin{bmatrix} -x_2 - x_1^3 \\ x_1 - 2x_2^3 \end{bmatrix} \tag{5.27}$$

restricted to $\mathscr{D} := \{x \in \mathbb{R}^2 \ : \ ||x||_2^2 \leq 1\}$, with a switching delay $T_D = .01$s.

Table 5.1 presents the Lyapunov functions, constants, class $\mathscr{K}$ functions and class $\mathscr{KL}$ functions needed to apply Corollary 5. The functions $\alpha_i(\cdot)$, $\alpha_{ji}(\cdot)$ and constants b_{ji} are all obtained by exploiting the equivalence of norms over $\mathbb{R}^n$ and the fact that $|x|^r < |x|^s$ for all $r > s$ and $|x| < 1$. The functions $\beta_i(\cdot,\cdot)$ are solved as in Theorem 4.9, Lemma 4.4 and Appendix C.5 of [41]. The resulting scalar ODE is second order, and has an analytic solution.

i	$V_i(x)$	$\alpha_i(y)$	$\alpha_{ji}(y)$	b_{ji}	$\beta_i(r,s)$
1	$x_1^2+x_2^4$	$2y^2$	$2.5y^2$	1	$\left(\frac{4r^2}{r^2s+2}\right)^{\frac{1}{4}}$
2	$\frac{1}{2}(x_1^2+x_2^2)$	$2y^2$	$3y^2$	1	$2\left(\frac{2r^2}{r^2s+2}\right)^{\frac{1}{2}}$

Table 5.1: Functions and constants necessary to apply Corollary 5 to Example 1

Figure 5.1 shows snapshots of $\mathscr{S}^{uas}(2,1,t)$ (white) evolving over time under the switching signal $\sigma(t)\equiv 1$. Initially, $\mathscr{S}^{uas}(2,1,t)$ is not very large (recal that the domain is the unit circle), but as the system evolves, the buffer delay $\gamma^{uas}(2,1,t)$ decreases, and its effect becomes less important. As can be seen, the set $\mathscr{S}(2,1,t)$ converges to the delay-free PLF based partitioning (5.24). A sample trajectory in the phase space is presented in Figure 5.2, with subsets of the trajectory evolving according to $\dot{x}=f_1(x)$ plotted in black (dark), and those evolving according to $\dot{x}=f_2(x)$ plotted in cyan (light). A switch occurs as soon as the trajectory enters a region of the state space in which switching is allowed. We note that the system initially spends a relatively long time in mode 2 because $\mathscr{S}(2,1,t)$ is relatively small (Figure 5.1). In the last snapshot of Figure 5.1, $\mathscr{S}(2,1,t)$ occupies approximately half of the unit circle. Hence, as the effect of the time delay lessens as γ decreases, switching between modes is enabled and occurs more frequently.

5.4.2 Linear switched system with time-varying UAS mode dynamics

Consider a system (5.1) with $\mathscr{F}=\{f_1(t,x),f_2(t,x)\}$,

$$f_i(x) \quad = \quad \begin{bmatrix} -x_1-g_i(t)x_2 \\ x_1-x_2 \end{bmatrix}, \tag{5.28}$$

with $x=[x_1,x_2]^T\in\mathbb{R}^2$ and $g_i:\mathbb{R}_+\to\mathbb{R}$

$$g_1(t) \quad = \quad \tfrac{3}{1+t} \tag{5.29}$$

$$g_2(t) \quad = \quad \tfrac{e^t}{(1+e^t)} \tag{5.30}$$

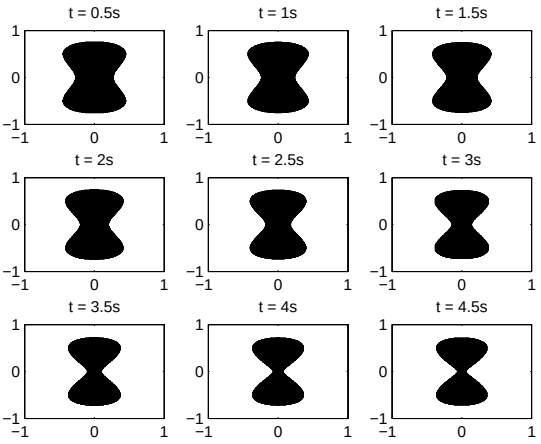

Figure 5.1: Snapshots of the partition $\mathscr{S}^{uas}(2,1,t)$ (white) evolving over time under the switching signal $\sigma(t) \equiv 1$. Notice that the black (no-switch partition) shrinks, such that $\mathscr{S}^{uas}(2,1,t)$ approaches the delay free partitioning $\bar{\mathscr{S}}^{uas}(2,1,t)$ (5.24).

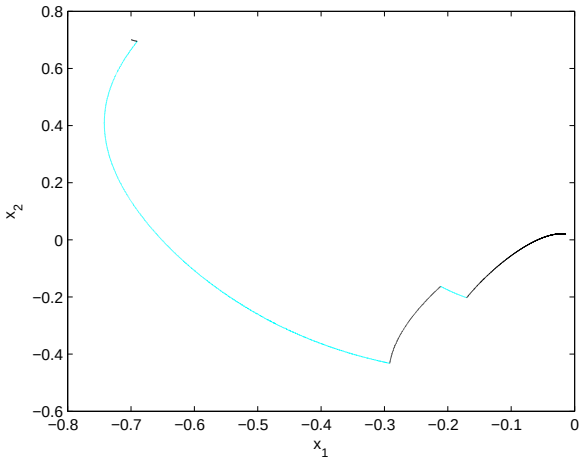

Figure 5.2: Trajectory in the phase space generated by a two mode system (5.26), (5.27). Switching obeys a signal $\sigma \in \Sigma^{uas}_{T_D}$, with subsets of the trajectory evolving according to $\dot{x} = f_1(x)$ plotted in black (dark), and those evolving according to $\dot{x} = f_2(x)$ plotted in cyan (light).

i	k_i	c_i	$V_i(x)$	$\alpha_i(y)$	$\alpha_{ji}(y)$	b_{ji}	$\beta_i(r,s)$
1	3	3	$x_1^2+(1+g_1(t))x_2^2$	$7y^2$	$2y^2$	1	$2e^{-\frac{3}{8}s}r$
2	1	0	$x_1^2+(1+g_2(t))x_2^2$	$3y^2$	$5y^2$	-1	$\sqrt{2}e^{-\frac{3}{4}s}r$

Table 5.2: Functions and constants necessary to apply Corollary 5 to Example 2

with a switching delay $T_D = .01$s.

By noting that each continuously differentiable $g_i(t)$ satisfies

$$\begin{aligned} 0 \leq g_i(t) \leq k_i \\ -c_i \leq \dot{g}(t) \leq g(t) \end{aligned} \tag{5.31}$$

for some $k_i, c_i \geq 0$, it is possible to construct the necessary Lyapunov functions, class $\mathscr{K}$ functions, and class $\mathscr{KL}$ functions. These functions and constants were solved for in a similar manner as those in the previous example, except in this case, equivalence of norms was not necessary as all terms were second order. These functions, along with the necessary constants k_i, c_i, are shown in Table 5.2. A sample trajectory in the phase space is depicted in Figure 5.2, with subsets of the trajectory evolving according to $\dot{x} = f_1(x)$ plotted in black (dark), and those evolving according to $\dot{x} = f_2(x)$ plotted in cyan (light), where a switch occurs as soon as the trajectory enters a region of the state space in which switching is allowed. We see that in this example, as opposed to Example 5.4.1, switching occurs much less frequently. This highlights the effect of both the system dynamics and Lyapunov function structures on delay buffer.

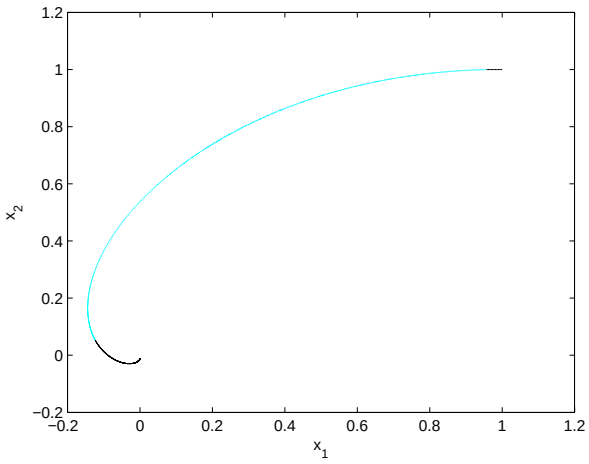

Figure 5.3: Trajectory in the phase space generated by Example 5.4.2. Switching obeys a signal $\sigma \in \Sigma_{T_D}^{uas}$, with subsets of the trajectory evolving according to $\dot{x} = f_1(x)$ plotted in black (dark), and those evolving according to $\dot{x} = f_2(x)$ plotted in cyan (light).

Chapter 6

Safety in human-automation systems under shared control

The partitions of the state space developed in Chapters 4 and 5 can be used to inform the design of a user interface indicating to the user which modes (if any) can safely be switched to given the current delayed measurement. Of course, here, "safety" is interpreted in the sense of theoretical stability, as given in Definitions 4 and 1 and Lemma 2. When performance and safety requirements go beyond stability (e.g. aerodynamic envelope protection in A/C) additional analysis and design methods are required.

Computational techniques for verification can create new levels of confidence and reliability in safety-critical systems such as as aircraft autopilots, by predicting where failures might occur, and how human operators can avoid them[7, 15, 39, 65]. Verification of human-automation systems introduces further complexity because it involves not only the automation, but also the way in which the user interacts with the automation [6]. The user-interface both provides information to the user about the underlying automation, and allows the user to issue input commands to the system. Formal methods have been used to verify user-interfaces modeled as discrete event systems [11, 15, 19, 34, 39]. Estimation has been used to anticipate the human's actions [45] through particle filters. We consider continuous systems that have inputs from both the human and the automation, and extend reachability analysis and controller synthesis [45, 54, 65] to human-automation systems under

continuous shared control. Since we cannot guarantee what actions the human will take, we focus on guarantees that the correct information has been provided to the human, in order to achieve a desired task. While *how* this information is displayed is vitally important to effective human-automation interaction, we restrict ourselves to the portion of this problem we can quantify: *what* information is displayed.

We begin with a description of the continuous system under shared control to be studied in this chapter. We then introduce reachability techniques applied to verification and develop an algorithm for generating provably correct user-interfaces. The chapter concludes with an example: a civil jet aircraft operating in "manual mode."

6.1 Modeling

Consider a continuous system under shared control

$$\dot{x} = f(x, u_c, u_h) \tag{6.1}$$

with states $x \in \mathscr{X} \subseteq \mathbb{R}^n$, automation-controlled continuous input $u_c \in \mathscr{U}_c = [\underline{u}_c, \overline{u}_c]$, human-controlled continuous input $u_h \in \mathscr{U}_h = [\underline{u}_h, \overline{u}_h]$, with $\underline{u}_h < 0, \overline{u}_h > 0$. We assume that the automation input $u_c = u_c(x)$ is strictly a function of the state, whereas the human input $u_h = u_h(r)$ is a function of a human-controlled reference input $r \in \mathscr{R} = [r_{\min}, r_{\max}]$. Consider the following motivating example.

Example 2. *Consider the double integrator system*

$$\begin{aligned} \dot{x} &= Ax + B(u_c(x) + u_h(r)) \\ A &= \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \end{bmatrix}^T \\ u_c(x) &= -3 \cdot \text{sign}(x_2), \quad u_h(r) = r \end{aligned} \tag{6.2}$$

with state $x \in \mathscr{X} \subseteq \mathbb{R}^2$, automatic control input $u_c \in [-3,3]$, human control input $u_h \in [-3,3]$ and constraint set $\mathscr{C} = [-5,5] \times [-5,5]$.

Consider trajectories starting from $x(0) = [4,3]^T \in \mathscr{C}$ under different human inputs (Figure 6.1). 1) The human input $r = -\frac{2}{3}u_c(x)$ drives the state out of the

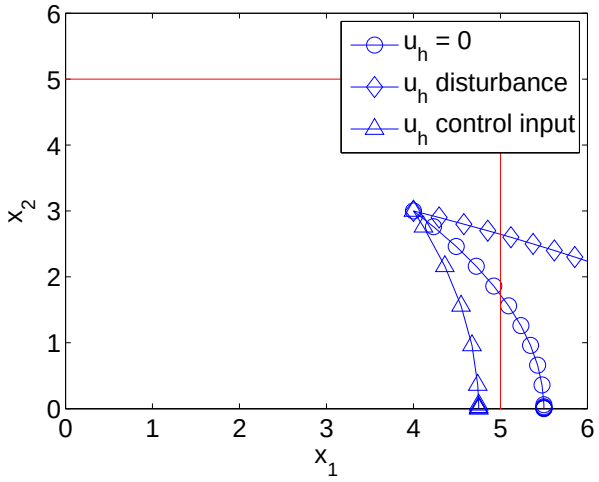

Figure 6.1: Trajectories for Example 2 starting from $x(0) = [4,3]^T$ for which: 1) ($\diamond$) the user acts as a disturbance 2) ($\circ$) the user is "hands-off" and 3) ($\triangle$) the user acts as a control input. The constraint set $\mathscr{C}$ is drawn with a solid red line.

constraint set ($\diamond$), effectively acting as a disturbance, leading to safety failure. 2) When the human is "hands off" the controls ($r = 0$), the resulting trajectory ($\circ$) also exits the constraint set $\mathscr{C}$. If system safety is to be preserved the human *must* assist the automation. 3) When the human input $r = u_c(x)$ co-operates with the automation. The resulting trajectory ($\triangle$) remains within the constraint set $\mathscr{C}$, preserving system safety.

6.2 Invariance under shared control

In order to accomodate a system under shared continuous control, we take into account how interactions between the human input and the automation input affect system safety. Our approach is to broadly classify the human's input as: 1) a disturbance, driving the system to unsafety, 2) neutral ("hands-off"), implying $u_h(r) = 0$, or 3) a controlled input, assisting the automation in preserving safety. Consider the following three types of invariant sets.

Definition 5. *For a set $\mathscr{W}_I \subseteq \mathscr{X}$ to be* invariant *with respect to a constraint set $\mathscr{C}$,*

all trajectories $x(t)$ which start in $\mathscr{W}_I$ must remain within $\mathscr{C}$ for all $t \geq 0$ for all continuous human input $u_h \in \mathscr{U}_h$.

$$\mathscr{W}_I = \{x(0) \in \mathscr{C} \mid \forall u_h \in \mathscr{U}_h \; \exists u_c \in \mathscr{U}_c \text{ such that } x(t) \in \mathscr{C} \; \forall t \geq 0\} \tag{6.3}$$

Definition 6. *For a set $\mathscr{W}_{UI} \subseteq \mathscr{X}$ to be* user-invariant *with respect to a constraint set $\mathscr{C}$, all trajectories $x(t)$ which start in $\mathscr{W}_{UI}$ must remain within $\mathscr{C}$ for all $t \geq 0$ for all $u_h \in \mathscr{U}_{UI} \subseteq \mathscr{U}_h$.*

$$\mathscr{W}_{UI} = \{x(0) \in \mathscr{C} \mid \forall u_h \in \mathscr{U}_{UI} \; \exists u_c \in \mathscr{U}_c \text{ such that } x(t) \in \mathscr{C} \; \forall t \geq 0\} \tag{6.4}$$

Definition 7. *For a set $\mathscr{W}_{UAI} \subseteq \mathscr{X}$ to be* user-assisted-invariant *with respect to a constraint set $\mathscr{C}$, there must exist a control input pair $(u_h, u_c) \in \mathscr{U}_{UAI} \times \mathscr{U}_c$ such that all trajectories $x(t)$ which start in $\mathscr{W}_{UI}$ will remain within $\mathscr{C}$ for all $t \geq 0$. Here, $\mathscr{U}_{UAI} \subseteq \mathscr{U}_h$.*

$$\mathscr{W}_{UAI} = \{x(0) \in \mathscr{C} \mid \exists (u_h, u_c) \in \mathscr{U}_{UAI} \times \mathscr{U}_c \text{ such that } x(t) \in \mathscr{C} \;\; \forall t \geq 0\} \tag{6.5}$$

Invariant sets are computed by effectively treating the human input as a disturbance input. Often, this very conservative assumption leads to $\mathscr{W}_I = \{\emptyset\}$, and in many systems, treating the operator as a disturbance is not realistic or necessary. By bounding the control authority given to the user when they are acting as a disturbance, a less conservative and possibly more useful result can be obtained.

User-invariant sets are effectively computed by ignoring the human input (assuming $u_h = 0$), hence some human inputs (outside the allowable range) may cause the state to exit the constraint set. The guarantee of safety is weaker than for invariant sets.

A user-assisted-invariant set represents the portion of the state space in which it is possible for the human to apply a prescribed input which maintains system safety.

The important distinction between user-invariant and user-assisted-invariant sets is that there are portions of user-assisted-invariant sets in which the human *must* apply an input to preserve system safety, as the automation is unable to prevent failure on its own. By contrast, in a user-invariant set, the human *may* apply

an input to assist the automation to keep the system safe, but does not have to. In user-invariant sets, bounds on the human input can be interpreted as a recommendation – remaining within these bounds guarantees safety, but exceeding them will not cause failure. In user-assisted-invariant sets, the constraints are much stricter – an input must be applied to preserve system safety, and failing to do so will eventually lead to a violation of the safety constraints. The relationship between these sets will be described in Section 6.3.

6.2.1 Using invariant sets to create a user-interface

The algorithm in [54] for user-interface design for supervisory hybrid systems to preserve system safety involves three steps: 1) separation of the hybrid system into subsystems which contain no human-initiated discrete inputs, 2) calculation of the reachable set (to be defined formally in the next section) for each subsystem, and 3) abstraction to a discrete event system based on the reachability result. The reachability result partitions the state-space into intersections of "safe" or "unsafe" regions in each subsystem. *Our aim is to abstract (6.1) to a discrete event system that conveys the safety information of multiple invariant, user-invariant and user-assisted-invariant sets, $\mathscr{W}_i$, $i \in \{1,...,n\}$, to the user. Having this information allows the user to determine if the current state is in an invariant, user-invariant or user-assisted-invariant subset of the state space, and consequently, whether or not there are safety restrictions on the human input.* To accomplish this, 1) compute the invariant, user-invariant and user-assisted-invariant sets of (6.1) with respect to the constraint set $\mathscr{C}$, and 2) abstract the computed invariant, user-invariant and user-assisted-invariant sets to a DES. This DES conveys the safety information contained in these sets to the user.

6.3 Calculating reachable sets

Computing the reachable set involves representing all of the states which have a path to a target set. As in [64], for $\dot{x} = f(x,u,d)$, with control input $u \in \mathscr{U}$, disturbance input $d \in \mathscr{D}$, and constraint set $\mathscr{C}$, the "target" is encoded implicitly as a level set function $\overline{\mathscr{W}}_0 = \mathscr{C}^c = \{x \in \mathscr{X} \mid J_0(x) < 0\}$, $J_0 : \mathscr{X} \to \mathbb{R}$. The boundary of the target set is propagated backwards in time according to the system dynamics.

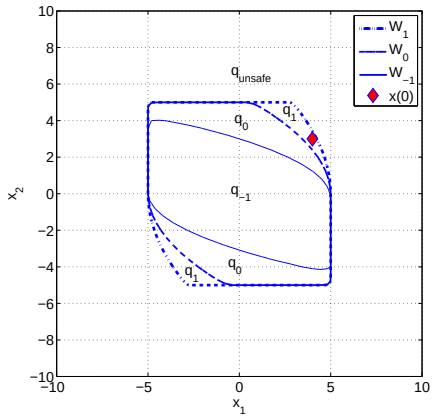

Figure 6.2: The safe, marginally safe and recoverably safe sets $\mathscr{W}_{-1}$, $\mathscr{W}_0$ and $\mathscr{W}_1$ (Example 2), computed by treating the user as a disturbance, "hands off" and as a controlled input, respectively.

Finding the backwards reachable set $\overline{\mathscr{W}}(t)$ requires solving the terminal value time-dependent modified Hamilton-Jacobi partial differential equation

$$\begin{aligned} 0 &= \frac{\partial J(x,t)}{\partial t} + \min\left[0, H\left(x, \frac{\partial J(x,t)}{\partial x}\right)\right] \\ H\left(x, \frac{\partial J(x,t)}{\partial x}\right) &= \max_{u\in\mathscr{U}} \min_{d\in\mathscr{D}} \frac{\partial J(x,t)}{\partial x}^T f(x,u,d) \end{aligned} \tag{6.6}$$

with $J(x,0) = J_0(x)$ for $t = 0$ such that the invariant set is $\mathscr{W}(t) = \{x \in \mathscr{X} \mid J(x,t) \geq 0\}$.

Although the user typically acts to preserve system safety, it is extremely difficult and often non-generalizable to explicitly model a user's control actions. Instead, we compute an arbitrary number of reachable sets that encompass the full range of possible user behaviors. Define the set $\mathscr{U}_i \subseteq \mathscr{U}_h$ as a reduced set of inputs

$$\mathscr{U}_i = \alpha_i \mathscr{U}_h, \alpha_i \in [0,1],\ i \in \{-N, ..., 0, ...M\} \tag{6.7}$$

where N and M are the arbitrarily chosen number of safe sets and recoverably safe sets, respectively.

6.3.1 Safe sets

Let $i = -N, ..., -1$, with N the number of *safe sets* $\mathscr{W}_i$ to be calculated by solving (6.6) with the Hamiltonian

$$H_i\left(x, \frac{\partial J(x,t)}{\partial x}\right) = \max_{u_c \in \mathscr{U}_c} \min_{u_h \in \mathscr{U}_i} \frac{\partial J(x,t)}{\partial x}^T f(x, u_c, u_h) \tag{6.8}$$

and $\mathscr{U}_i = \alpha_i \mathscr{U}_h$, $\alpha_i \in (0,1]$ $\alpha_{i+1} < \alpha_i$ such that $\mathscr{U}_{i+1} \subset \mathscr{U}_i$. Note that the following property holds [16]:

$$\mathscr{W}_{-N} \subset \mathscr{W}_{-N+1} \subset \ldots \subset \mathscr{W}_{-1} \tag{6.9}$$

The sets $\mathscr{W}_i$, $i \in \{-N, ..., -1\}$ are "safe" because they represent portions of the state-space in which the user can apply any input $u_h \in \mathscr{U}_i$ without violating the constraints for safety. The invariance preserving control law is *not* enforced along the boundaries of the sets, allowing the user to transition between sets by choosing inputs $u_h \notin \mathscr{U}_i$.

Example 2: The safe set $\mathscr{W}_{-1}$, calculated with

$$\begin{aligned} H_{-1}\left(x, \frac{\partial J(x,t)}{\partial x}\right) &= \max_{u_c \in \mathscr{U}_c} \min_{u_h \in \mathscr{U}_{-1}} \frac{\partial J(x,t)}{\partial x}^T f(x, u_c, u_h) \\ &= \frac{\partial J(x,t)}{\partial x_1} x_2 + \left|\frac{\partial J(x,t)}{\partial x_2}\right| \end{aligned} \tag{6.10}$$

and $\mathscr{U}_{-1} = \frac{2}{3}\mathscr{U}_h$ is shown in Figure 6.2. As expected, the initial condition $x(0) = [4,3]^T$, lies outside of $\mathscr{W}_{-1}$.

6.3.2 Marginally safe sets

Let $i = 0$, and $\mathscr{U}_0 = 0$ to calculate the *marginally safe set* $\mathscr{W}_0$ by solving (6.6) with Hamiltonian

$$H_0\left(x, \frac{\partial J(x,t)}{\partial x}\right) = \max_{u_c \in \mathscr{U}_c} \frac{\partial J(x,t)}{\partial x}^T f(x, u_c, 0) \tag{6.11}$$

The set $\mathscr{W}_0$ is "marginally safe" because it represents the portion of the state-space in which the automation is capable of maintaining system safety without user interference or assistance. As long as the user remains neutral, or "hands-off" the controls, safety is guaranteed.

Example 2: $\mathscr{W}_0$ (shown in Figure 6.2) is calculated with

$$\begin{aligned} H_0\left(x, \tfrac{\partial J(x,t)}{\partial x}\right) &= \max_{u_c \in \mathscr{U}_c} \tfrac{\partial J(x,t)}{\partial x}^T f(x, u_c, 0) \\ &= \tfrac{\partial J(x,t)}{\partial x_1} x_2 + 3|\tfrac{\partial J(x,t)}{\partial x_2}| \end{aligned} \tag{6.12}$$

As expected, $x(0) = [4,3]^T \notin \mathscr{W}_0$.

Lemma 3. *Safe sets and marginally safe sets are user-invariant.*

Proof. By construction: For $\mathscr{W}_i,\ i \in \{-N, ..., -1\}$ computed with $u_h \in \mathscr{U}_i \subseteq \mathscr{U}_h$, for all $x(0) \in \mathscr{W}_i$, $x(t) \in C$ for all $t \geq 0$ as long as $u_h \in \mathscr{U}_i$. Thus $\mathscr{W}_i,\ i \in \{-N, ..., -1\}$ are user-invariant by definition. Similarly, for $\mathscr{W}_0$ computed with $u_h \in \mathscr{U}_0 = 0 \subset \mathscr{U}_h$, for all $x(0) \in \mathscr{W}_i$, $x(t) \in C$ for all $t \geq 0$ as long as $u_h \in \mathscr{U}_0$. Thus $\mathscr{W}_0$ is user-invariant. □

6.3.3 Recoverably safe sets

Let $i = 1, ..., M$, with M the number of *recoverably safe sets* $\mathscr{W}_i$ to be calculated by solving (6.6) with the Hamiltonian

$$H_i\left(x, \tfrac{\partial J(x,t)}{\partial x}\right) = \max_{u_c \in \mathscr{U}_c} \max_{u_h \in \mathscr{U}_i} \tfrac{\partial J(x,t)}{\partial x}^T f(x, u_c, u_h) \tag{6.13}$$

with $\mathscr{U}_i = \alpha_i \mathscr{U}_h$, $\alpha_i \in (0,1]$ and $\alpha_i < \alpha_{i+1}$ such that $\mathscr{U}_i \subset \mathscr{U}_{i+1}$. Note that the following property holds [16]:

$$\mathscr{W}_1 \subset \mathscr{W}_2 \subset ... \subset \mathscr{W}_M \tag{6.14}$$

The sets $\mathscr{W}_i, i \in \{1, ..., M\}$ are "recoverably safe" because they contain portions of the state space in which there always exists a control pair $(u_h, u_c) \in \mathscr{U}_i \times \mathscr{U}_c$ which maintains system safety. As with safe sets, the invariance preserving control law is *not* enforced along the boundaries of the sets. The recoverably safe sets provide information about what the user *must* do in order to preserve system safety, in case a disturbance input (external or user-applied) pushes the system into a configuration that the automation is unable to recover from on its own (i.e. states outside of $\mathscr{W}_0$).

Example 2: The recoverably safe set $\mathscr{W}_1$ is calculated with

$$\begin{aligned} H_1\left(x, \tfrac{\partial J(x,t)}{\partial x}\right) &= \max_{u_c \in \mathscr{U}_c} \max_{u_h \in \mathscr{U}_1} \tfrac{\partial J(x,t)}{\partial x}^T f(x, u_c, u_h) \\ &= \tfrac{\partial J(x,t)}{\partial x_1} x_2 + 6 \left| \tfrac{\partial J(x,t)}{\partial x_2} \right| \end{aligned} \tag{6.15}$$

and $\mathscr{U}_1 = \mathscr{U}_h$. Since $x(0) = [4,3]^T \in \mathscr{W}_1$, with appropriate user assistance, a trajectory starting at $x(0)$ will remain safe.

Lemma 4. *Recoverably safe sets are user-assisted-invariant.*

Proof. By construction: For $\mathscr{W}_i,\ i \in \{1,...,M\}$ computed with $u_h \in \mathscr{U}_i \subseteq \mathscr{U}_h$, for all $x(0) \in \mathscr{W}_i$, there exists a control pair $(u_h, u_c) \in \mathscr{U}_i \times \mathscr{U}_c$ such that $x(t) \in \mathscr{C}$ for all $t \geq 0$. Thus $\mathscr{W}_i,\ i \in \{1,...,M\}$ are user-assisted-invariant by definition. □

To summarize, we constructed $N+M+1$ sets to encompass all possible human input. Combining (6.9) and (6.14),

$$\mathscr{W}_{-N} \subset \mathscr{W}_{-N+1} \subset ... \subset \mathscr{W}_0 \subset \mathscr{W}_1 \subset ... \subset \mathscr{W}_M \tag{6.16}$$

The set $\mathscr{W}_0$ acts as a reference – if the system is in a state outside of $\mathscr{W}_0$, a human input *must* be applied to prevent failure, as the automation is unable to preserve safety unassisted. The set $\mathscr{W}_M$ corresponds to the standard "safe" invariant set [54]; its complement $\overline{\mathscr{W}}_M$ corresponds to the unsafe subset of the state-space. A controller could be synthesized to ensure that the set $\mathscr{W}_M$ is never exited and safety is preserved.

6.4 Abstraction to a DES

Definition 8. *Let the index i denote the safety level of the invariant set $\mathscr{W}_i$, where safety level decreases as i increases. Let the safety level of a point $x \in \mathscr{X} \subseteq \mathbb{R}^n$ be given by the smallest i such that $x \in \mathscr{W}_i$. A region of the state space $\mathscr{M} \subseteq \mathscr{C}$ has a* homogeneous safety level *i if all $x \in \mathscr{M}$ have the same safety level i.*

Definition 9. *A DES abstraction of a continuous system under shared control (6.1) is considered* safety informative *if 1) each mode corresponds to a region of the*

state space which has homogeneous safety level and 2) the DES conveys whether the system is in a user-invariant or user-assisted-invariant subset of the state space.

6.4.1 Generation of modes

Let $i = -N, \ldots, 0, \ldots, M$, where N is the number of safe sets, and M is the number of recoverably safe sets. Define a map from the continuous state-space to the discrete state-space, based on a partition that divides $\mathscr{X}$ into $N+M+2$ disjoint regions q_i as follows:

1. $\mathscr{W}_{-N} \rightarrow q_{-N}$
2. $\mathscr{W}_i \cap \overline{\mathscr{W}}_{i-1} \rightarrow q_i$, for $i = -N+1, ..., 0, ..., M$,
3. $\overline{\mathscr{W}}_M \rightarrow q_{unsafe}$

Lemma 5. *Modes defined by the above mapping represent cells of the state-space with homogeneous safety level.*

Proof. By construction: For $\mathscr{W}_{-N} \rightarrow q_{-N}$, the cell defined by $\mathscr{W}_{-N}$ is of homogeneous safety level $-N$. For modes $\mathscr{W}_i \cap \overline{\mathscr{W}}_{i-1} \rightarrow q_i$, $i \in \{-N+1, ..., 0, ..., M\}$, recall that by (6.16), $\mathscr{W}_{i-1} \subset \mathscr{W}_i$. Therefore the cells $\mathscr{W}_i \cap \overline{\mathscr{W}}_{i-1}$ are by definition of homogeneous safety level i. Thus the modes q_i, $i \in \{-N, \ldots, 0, \ldots, M\}$ correspond to cells of the state-space that have homogeneous safety level. □

Example 2: The cells in Figure 6.2 map to modes q_{-1}, q_0, q_1 and q_{unsafe}, as shown in Figure 6.4.

6.4.2 Transition function

Define the set of events $\Sigma = \{\sigma_{up}, \sigma_{down}\}$, corresponding to an increase or decrease in safety level, respectively. These events are state-based transitions that occur when the state crosses into a neighboring cell:

$$\begin{aligned} \sigma_{up}: &\quad x(t^-) \in \mathscr{W}_i \cap \overline{\mathscr{W}}_{i-1} \rightarrow x(t^+) \in \mathscr{W}_{i-1} \\ \sigma_{down}: &\quad x(t^-) \in \mathscr{W}_{i-1} \cap \overline{\mathscr{W}}_i \rightarrow x(t^+) \in \overline{\mathscr{W}}_{i-1} \cap \mathscr{W}_i \end{aligned} \tag{6.17}$$

An important consequence of (6.16) for this mapping is that transitions can only occur between neighboring modes. Hence the transition function R is defined as

$$\begin{aligned} R(q_i, \sigma_{up}) &= q_{i-1}, \quad i \in \{-N+1, ..., 0, ..., M\} \\ R(q_i, \sigma_{down}) &= q_{i+1}, \quad i \in \{-N, ..., 0, ..., M-1\} \\ R(q_M, \sigma_{down}) &= q_{unsafe} \end{aligned} \tag{6.18}$$

Note that in general, σ_{up} may not exist.

6.4.3 Construction of the DES

The discrete event system $G = (Q, \Sigma, R)$ is constructed as illustrated in Figure 6.3. Since the designer decides how many modes to generate, G is of minimal mode cardinality. Details of the abstraction (and proof of its determinism) are presented in [54].

Lemma 6. *The discrete event system $G = (Q, \Sigma, R)$ as defined in Figure 6.3 is safety informative.*

Proof. The first condition is satisfied by Lemma 5. The second condition is satisfied by construction: modes $q_i,\ i \in \{-N, ..., 0\}$ correspond to user-invariant subsets of the state-space by Lemma 3, and modes $q_i,\ i \in \{1, ..., M\}$ correspond to user-assisted-invariant subsets of the state-space by Lemma 4. The transition $R(q_0, \sigma_{down}) = q_1$ from (6.18) corresponds to a transition from a user-invariant to a user-assisted-invariant subset of the state-space. □

The main advantage is that this abstraction provides the user with a warning that their actions may lead to unsafety. When in a user-invariant mode (i.e. $q_i,\ i \in \{-N, ..., 0\}$), the user is informed of safety restrictions on their input, but also free to violate these restrictions if they choose to. Is the user input violates safety restrictions, the system simply transitions to a user-assisted-invariant mode (i.e. $q_i,\ i \in \{1, ..., M\}$), indicating what input the user *must* apply in order to maintain system safety. Essentially, the user-assisted-invariant modes act as a buffer, allowing the user to "recover" to a higher safety level before the system enters the unsafe region of the state-space. Having multiple user-assistant-invariant modes provides more opportunities for correction. As the mode index i increases, so does

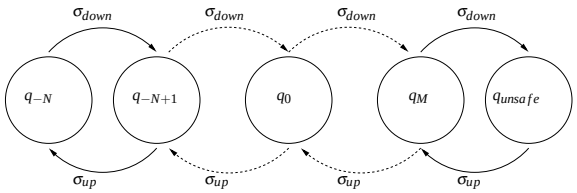

Figure 6.3: DES $G = (Q, \Sigma, R)$, an abstraction of (6.1), constructed using (6.16) and reachability calculated with Hamiltonians (6.8), (6.11) and (6.13). The dashed transitions indicate a repeated pattern of transitions for a generic system with $N + M + 1$ modes, eventually passing through q_0.

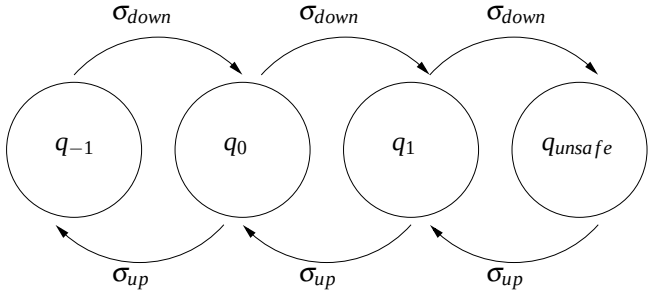

Figure 6.4: DES $G = (Q, \Sigma, R)$ for Example 2. Note that q_{-1} represents a region in the continuous state-space that is safe, q_0 represents a region that is marginally safe, q_1 represents a region that is recoverably safe, and q_{unsafe} represents a region that is unsafe.

the necessity for control action - a designer may choose to have increasing levels of alerts corresponding to increasing level of unsafety.

For Example 2, this algorithm results in the DES in Figure 6.4. In q_{-1}, the user is free to apply any input $|r| \leq 2$ without risking transitioning to a lower safety level. If the user violates these constraints, the system may transition into q_0. In this case, if the user is "hands-off" the controls ($r = 0$), the automation will still be able to maintain system safety. Once again, the user is free to apply inputs that drive the system to a lower safety level. However, once in q_1, the user *must* apply an input $r = 3 \cdot \text{sign}(x_2)$ to maintain that safety.

6.5 Example: aircraft in manual mode

Consider manual control mode of the aircraft longitudinal dynamics introduced in [48], in which the flight crew sets the reference flight path angle, while the automation performs low level control tasks. Using the short period approximation, the state $x = [\alpha, \dot{\theta}, \gamma]$ consists of angle of attack α, pitch rate $\dot{\theta}$, and flight path angle γ [49]. The reference input $r \in \mathscr{R}$ consists of the reference flight path angle for γ. Elevator deflection δ_e is used to implement a static full-state feedback controller, yielding the closed loop dynamics [48]:

$$\begin{aligned} f_{\text{MAN}}(x,r) &= Ax + B(u_c(x) + u_h(r)) \\ &= A_{cl}x + B_{cl}r \end{aligned} \tag{6.19}$$

with $u_c(x) = -Kx$, $u_h(r) = N_r r$ and

$$\begin{aligned} A_{cl} &= \begin{bmatrix} -0.6486 & 0.9376 & -0.0963 \\ -2.6226 & -3.0477 & -3.0803 \\ 0.6486 & 0.0624 & 0.0963 \end{bmatrix} \\ B_{cl} &= -2.3 \begin{bmatrix} -0.0418 & -1.3391 & 0.0418 \end{bmatrix}^T \end{aligned} \tag{6.20}$$

where K is a state feedback matrix such that A_{cl} has eigenvalues at $-1.2, -1.2 \pm 0.12j$, and $N_r = -2.3$.

State constraints (due to the flight envelope) and control constraints (due to feedback under saturation) define

$$\begin{aligned} J_0(x) &= \min_x\{J_0^{\text{state}}(x), J_0^{\text{sat}}(x)\}, \text{ with} \\ J_0^{\text{state}}(x) &= \min_x\{x - x_{\min}, x_{\max} - x\} \\ J_0^{\text{sat}}(x) &= \min_x\{u_{\max} - \max_{r\in\mathscr{R}} \delta_e(x,r), \\ &\qquad \min_{r\in\mathscr{R}} \delta_e(x,r) - u_{\max}\} \end{aligned} \tag{6.21}$$

with state bounds $x_{\min} \le x \le x_{\max}$, $x_{\min} = [-11.5^\circ, -15^\circ, -13.3^\circ]$, $x_{\max} = -x_{\min}$, $u_{\max} = 50^\circ$, and $r \in \mathscr{R} = [-13.3^\circ, 13.3^\circ]$.

Choosing $N = M = 1$, invariant sets $\mathscr{W}_{-1}$,$\mathscr{W}_0$ and $\mathscr{W}_1$ are calculated as shown in Figure 6.5 (dark green solid, light yellow transparent, and red mesh, respectively). Safe set $\mathscr{W}_{-1}$ is computed by bounding the pilot's input to 25% of $\mathscr{R}$, a reasonable

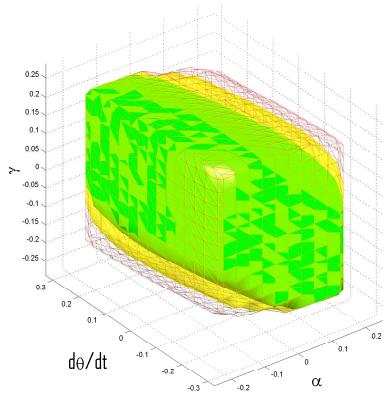

Figure 6.5: The solid green (dark), transparent yellow (light) and red mesh sets represent, respectively, safe set $\mathscr{W}_{-1}$, marginally safe set $\mathscr{W}_0$, and recoverably safe set $\mathscr{W}_1$. $\mathscr{W}_{-1}$ is user-invariant (the user can apply any input $u_h \in \mathscr{U}_{-1}$ without affecting system safety). $\mathscr{W}_0$, although also user-invariant, is computed assuming $u_h(r) = 0$ (the automation can preserve safety without interference or assistance from the user). $\mathscr{W}_1$ is user-assisted-invariant – for states within this set but not contained in $\mathscr{W}_0$, the user *must* apply an input to preserve system safety.

estimate of pilot behavior under normal operating conditions, with $\alpha_{-1} = \frac{.25|N|r_{max}}{u_{max}}$, $\mathscr{U}_{-1} = \alpha_{-1}\mathscr{U}_h$, and Hamiltonian as defined in (6.8). Marginally safe set $\mathscr{W}_0$ is calculated as in (6.11). Recoverably safe set $\mathscr{W}_1$ is calculated with $\alpha_1 = \frac{|N|(r_{max})}{u_{max}} = \frac{(2.3)(13.3^\circ)}{50^\circ}$, and $\mathscr{U}_1 = \alpha_1\mathscr{U}_h$ – we assume the pilot has full control authority, as per (6.13).

The state space is partitioned into four disjoint regions: $\mathscr{W}_{-1} \rightarrow q_{-1}$, $\mathscr{W}_0 \cap \overline{\mathscr{W}}_{-1} \rightarrow q_0$, $\mathscr{W}_1 \cap \overline{\mathscr{W}}_0 \rightarrow q_1$, and $\overline{\mathscr{W}}_1 \rightarrow q_{unsafe}$. The transition function R and DES G are shown in Figure 6.4 (the same DES as in Example 2, although the events σ_{up} and σ_{down} correspond to state-based transitions defined in Figure 6.5).

The DES can be used as a user-interface, whose main benefit is that the flight crew knows at all times 1) what inputs can be applied without affecting system safety, 2) what inputs can be applied that reduce system system safety without causing failure and 3) what inputs must be applied to preserve system safety.

Chapter 7

Conclusions

7.1 Summary

Unmanned aerial vehicles, both as individiual aircraft and as fleets, have a wide range of applications – beyond traditional military uses, they can be used for such diverse tasks as surveillance and reconnaissance, search and rescue, and scientific data collection. These versatile aircraft remove highly trained pilots and operators from potentially dangerous situations, and allow for extended operation periods. However, like most aircraft, UAVs are fundamentally hybrid systems, which when combined with remote operation, introduces new challenges to their design and analysis.

The work presented in this thesis contributes towards extending and combining hybrid and distributed systems theory, such that the resulting systems are scalable and robust to switching delays. For fleets of identical switched linear systems under distribtued control, I showed how to prove GUAS under arbitrary switching in a scalable and computationally efficient manner. For systems not shown to be stable under arbitrary switching, I introduced a delay buffer to traditional state constraint based switching schemes such that stability is preserved desptied a bounded switching delay. This has applications to a remote supervisory controller triggering mode switches over a communication channel that introduces delays. These results generalize to linear switched systems, as well as to certain classes of nonlinear switched systems. In all cases, the delay buffer and its effect on system stability

was computed by bounding the derivative of each mode's Lyapunov function over the time delay period, essentially examining a worst case scenario. However, I also showed that for UAS systems, the delay buffer approaches zero, establishing a wait-time condition, since the effect of the time delay on state based switching becomes negligible by waiting long enough. With wireless communication becoming more and more reliable, and unmanned vehicles becoming more complex and autonomous, our theory provides a step forward in allowing the benefits of switched systems to be safely incorporated.

I conclude with results in interface design for systems under shared continuous control based on formal verification techniques, motivated by applications to pilot-automation interaction. I developed an algorithm for generating a provably correct user interface that accomodates all possible user intent. In doing so, I do not limit the user's actions, but rather provide the information necessary for them to ascertain the effects of their actions on system safety. I conclude with an example based on a model of an actual incident in which faulty pilot-automation interaction led to catastrophic failure of a civil jet aircraft.

7.2 Future work

Avenues for future work include, but are by no means limited to, extending these results to input to state stability of distributed hybrid systems, using our results to extend optimal control of switched linear systems to be robust to a switching delay, as well as dealing with quantized and corrupted state measurements.

In Chapter 3, a key restriction is that all subsystems switch modes simultaneously. I aim to address this, as in real-world applications this may prove to be an unrealistic assumption. A first step in this direction would be to show that for systems with slower dynamics, if there is a relatively short period of heterogeneity amongst the vehicles during switching, then this period can be neglected without significant consequence to system stability or performance.

In Chapters 4 and 5, I assume that all modes are stable. It is important to extend these results to systems in which modes are unstable, such that stabilizing switching schemes robust to switching delays can be developed. Many high performance systems (e.g. fighter planes) require switching to unstable modes to

achieve necessary behavior. Furthermore, the work presented in these two chapters is certainly conservative, as the bounds used in obtaining the results are not tight, and improvements in this area would certainly add to their usefulness. Finally, the investigation of heuristics for choosing the various Lyapunov functions such that the safe switching regions are maximized would prove useful as well.

Chapter 6 limits analysis to continuous time systems. Although an informal merging of these results with hybrid system verification is presented in [48], a complete theory of user-interface design will necessitate a formal combination of the two results into general definitions, theorems and algorithms. How the concepts of safe, marginally safe and recoverably safe subsets generalize to a hybrid space needs to be investigated. Furthermore, it is important to note that only discrete information is presented to the user as of yet. The inclusion of continuous time information, such as time remaining in the current mode given the present state/input configuration, could prove beneficial.

Finally, our approach of exploiting the block upper-triangular structure of many distributed systems under cooperative control agrees well with recent techniques used to reduce the complexity of reachability computations [40]. If our results can be combined with these recent advances, the result will be large distributed systems that are provably safe, despite bounded control authority.

Bibliography

[1] R. Agaev and P. Chebotarev. On the spectra of nonsymmetric laplacian matrices. *Linear Algebra and its Applications*, 399:157 – 168, 2005. ISSN 0024-3795. doi:DOI:10.1016/j.laa.2004.09.003. Special Issue devoted to papers presented at the International Meeting on Matrix Analysis and Applications, Ft. Lauderdale, FL, 14-16 December 2003. → pages 9

[2] A. A. Agrachev and D. Liberzon. Lie-algebraic stability criteria for switched systems. *SIAM Journal on Control and Optimization*, 40(1):253–269, 2001. doi:10.1137/S0363012999365704. → pages 2, 14

[3] W. N. Anderson, Jr, and T. D. Morley. Eigenvalues of the Laplacian of a graph. *Linear and Multylinear Algebra*, 18:141–145, 1985. → pages 9

[4] J. Aubin. *Viability Theory*. Birkhauser, 1991. → pages 30

[5] F. Blanchini, S. Miani, and F. Mesquine. A separation principle for linear switching systems and parametrization of all stabilizing controllers. *IEEE Transactions on Automatic Control*, 54(2):279 –292, feb. 2009. ISSN 0018-9286. doi:10.1109/TAC.2008.2010896. → pages 3

[6] J. Bowen and S. Reeves. Formal models of informal GUI designs. In *Proceedings of the 1st Int'l Conf. on Software Formal Methods for Interactive Systems*, Electronic notes in theoretical computer science, pages 57–72. Elsevier Science, July 2007. → pages 4, 47

[7] R. Boyatt and J. Sinclair. A lightweight formal methods perspective on investigating aspects of interactive systems. In *Proceedings of the 1st Int'l Workshop on Formal Methods for Interactive Systems (FMIS)*, UK, September 2007. Elsevier. → pages 47

[8] M. Branicky. *Control of Hybrid Systems*. PhD thesis, Department of Electrical Engineering and Computer Sciences, Massachusetts Institute of Technology, 1994. → pages 8

[9] M. Branicky. Multiple lyapunov functions and other analysis tools for switched and hybrid systems. *Automatic Control, IEEE Transactions on*, 43 (4):475 –482, apr. 1998. ISSN 0018-9286. doi:10.1109/9.664150. → pages 3, 8, 9, 23, 26

[10] S. Campbell. Stability of a class of linear switching systems with time delay. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 53(2): 384–393, Feb. 2006. ISSN 1057-7122. doi:10.1109/TCSI.2005.856666. URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1593944. → pages 3

[11] A. Cerone, P. Lindsay, and S. Connelly. Formal analysis of human-computer interaction using model-checking. In *Proceedings of the 3rd IEEE Int'l Conf. on Software Engineering and Formal Methods*, pages 352–361. IEEE, September 2005. → pages 4, 47

[12] P. Chandler, M. Pachter, and S. Rasmussen. Uav cooperative control. In *American Control Conference, 2001. Proceedings of the 2001*, volume 1, pages 50 –55 vol.1, 2001. doi:10.1109/ACC.2001.945512. → pages 1

[13] J. Cortes, S. Martinez, T. Karatas, and F. Bullo. Coverage control for mobile sensing networks. *IEEE Transactions on Robotics and Automation*, 20(2): 243 – 255, apr. 2004. ISSN 1042-296X. doi:10.1109/TRA.2004.824698. → pages 2

[14] L. Cremean and R. Murray. Stability analysis of interconnected nonlinear systems under matrix feedback. volume 3, pages 3078 – 3083 Vol.3, dec. 2003. doi:10.1109/CDC.2003.1273096. → pages 2, 17, 42

[15] J. Crow, D. Javaux, and J. Rushby. Models and mechanized methods that integrate human factors into automation design. In *International Conference on Human-Computer Interaction in Aeronautics*, pages 163–168, Toulouse, France, September 2000. → pages 4, 47

[16] E. Cruck and P. Saint-Pierre. Nonlinear impulse target problems under state constraint: A numerical analysis based on viability theory. *Set-Valued Analysis*, 12(4):383–416, December 2004. → pages 53, 54

[17] W. Dayawansa and C. Martin. A converse lyapunov theorem for a class of dynamical systems which undergo switching. *IEEE Transactions on Automatic Control*, 44(4):751 –760, april 1999. ISSN 0018-9286. doi:10.1109/9.754812. → pages 2

[18] R. DeCarlo, M. Branicky, S. Pettersson, and B. Lennartson. Perspectives and results on the stability and stabilizability of hybrid systems. *Proceedings of the IEEE*, 88(7):1069–1082, July 2000. → pages 8

[19] A. Degani and M. Heymann. Formal verification of human-automation interaction. *Human Factors*, 44(1):28–43, 2002. → pages 4, 47

[20] M. Di Benetto and A. Sangiovanni-Vincentelli, editors. *Hybrid Systems: Computation and Control*, volume 2034 of *Lecture Notes in Computer Science*. Springer-Verlag, Rome, Italy, March 2001. → pages 8

[21] R. Diestel. *Graph Theory*. Springer, Berlin, 2006. ISBN 9783540261834. → pages 9

[22] W. Dunbar. Distributed receding horizon control of cost coupled systems. pages 2510 –2515, dec. 2007. doi:10.1109/CDC.2007.4434033. → pages 2, 17

[23] T. Erneux. *Applied Delay Differential Equations*. Springer, Berlin, 2009. ISBN 9780387743714. → pages 3

[24] J. Fax. *Optimal and cooperative control of vehicle formations*. PhD thesis, California Inst. of Technology, Pasadena, CA., 2002. → pages 2, 21

[25] J. Fax and R. Murray. Information flow and cooperative control of vehicle formations. *Automatic Control, IEEE Transactions on*, 49(9):1465 – 1476, sep. 2004. ISSN 0018-9286. doi:10.1109/TAC.2004.834433. → pages 2, 10, 11, 14

[26] F. Gao, S. Zhong, and X. Gao. Delay-dependent stability of a type of linear switching systems with discrete and distributed time delays. *Applied Mathematics and Computation*, 196(1):24–39, 2008. ISSN 00963003. doi:10.1016/j.amc.2007.05.053. URL http://linkinghub.elsevier.com/retrieve/pii/S0096300307006248. → pages 3

[27] V. Gupta, D. Spanos, B. Hassibi, and R. Murray. On lqg control across a stochastic packet-dropping link. pages 360 – 365, jun. 2005. → pages 2

[28] V. Gupta, C. Langbort, and R. Murray. On the robustness of distributed algorithms. pages 3473 –3478, dec. 2006. doi:10.1109/CDC.2006.377451. → pages

[29] V. Gupta, A. Dana, J. Hespanha, R. Murray, and B. Hassibi. Data transmission over networks for estimation and control. *IEEE Transactions*

on Automatic Control, 54(8):1807 –1819, aug. 2009. ISSN 0018-9286. doi:10.1109/TAC.2009.2024567. → pages 2

[30] A. Gusrialdi, T. Hatanaka, and M. Fujita. Coverage control for mobile networks with limited-range anisotropic sensors. pages 4263–4268, Dec. 2008. → pages 2

[31] J. Hespanha and A. Morse. Stability of switched systems with average dwell-time. volume 3, pages 2655 –2660 vol.3, 1999. doi:10.1109/CDC.1999.831330. → pages 3, 16, 29

[32] J. P. Hespanha and A. S. Morse. Towards the high performance control of uncertain processes via supervision. In *Proceedings of the Conference on Information Sciences and Systems*, volume 1, pages 405–410, Mar. 1996. → pages 2

[33] J. P. Hespanha and A. S. Morse. Switching between stabilizing controllers. *Automatica*, 38(11):1905 – 1917, 2002. ISSN 0005-1098. doi:DOI:10.1016/S0005-1098(02)00139-5. → pages 3

[34] W. Hussak and S. Yang. Formal development of remote interfaces for large scale real-time systems. In *IEEE Int'l Conference on Systems, Man, and Cybernetics*, pages 124–129, 2004. → pages 47

[35] I. Hussein and D. Stipanovic. Effective coverage control for mobile sensor networks with guaranteed collision avoidance. *IEEE Transactions on Control Systems Technology*, 15(4):642 –657, jul. 2007. ISSN 1063-6536. doi:10.1109/TCST.2007.899155. → pages 2

[36] A. Jadbabaie, J. Lin, and A. Morse. Coordination of groups of mobile autonomous agents using nearest neighbor rules. *IEEE Transactions on Automatic Control*, 48(6):988 – 1001, jun. 2003. ISSN 0018-9286. doi:10.1109/TAC.2003.812781. → pages 2

[37] Z. Ji, X. Guo, S. Xu, and L. Wang. Stabilization of switched linear systems with time-varying delay in switching occurrence detection. *Circuits, Systems, and Signal Processing*, 26(3):361–377, June 2007. ISSN 0278-081X (Print) 1531-5878 (Online). doi:10.1007/s00034-006-0414-x. URL http://www.springerlink.com/content/03LG619618326617. → pages 3

[38] M. Johansson and A. Rantzer. Computation of piecewise quadratic lyapunov functions for hybrid systems. *Automatic Control, IEEE Transactions on*, 43 (4):555 –559, apr 1998. ISSN 0018-9286. doi:10.1109/9.664157. → pages 2, 3

[39] A. Joshi, S. P. Miller, and M. P. Heimdahl. Mode confusion analysis of a flight guidance system using formal methods. In *22nd IEEE Digital Avionics Systems Conference (DASC 2003)*, pages 2D.1–21–12 vol.1, October 2003. → pages 47

[40] S. Kaynama and M. Oishi. Schur-based decomposition for reachability analysis of linear time-invariant systems. In *Proceedings of the IEEE Conference on Decision and Control and the Chinese Control Conference*, pages 69 –74, dec. 2009. → pages 63

[41] H. Khalil. *Nonlinear Systems*. Gareth Stevens Pub, Milwaukee, 2002. ISBN 9780130673893. → pages 36, 37, 42

[42] S. Kim, S. A. Campbell, and X. Liu. Stability of a class of linear switching systems with time delay. *IEEE Trans. Circuits Syst. - Regular Papers*, 53(2): 384–393, 2006. → pages 3

[43] A. Kurzhanskiy and P. Varaiya. Ellipsoidal techniques for reachability analysis of discrete-time linear systems. *IEEE Transactions on Automatic Control*, 52(1):26 –38, jan. 2007. ISSN 0018-9286. doi:10.1109/TAC.2006.887900. → pages 30

[44] P. Ladkin and H. Sogame. Aircraft accident investigation report 96-5. http://sunnyday.mit.edu/accidents/nag-contents.html, July 1996. → pages 5, 6

[45] C. Lesire and C. Tessier. Estimation and conflict detection in human controlled systems. In J. Hespanha and A. Tiwari, editors, *Hybrid Systems: Computation and Control*, LNCS 3927, pages 407–420. Springer Verlag, March 2006. → pages 4, 47

[46] D. Liberzon. *Switching in Systems and Control*. Birkhauser, Boston, MA, Jun 2003. Volume in series Systems and Control: Foundations and Applications. → pages 2, 3, 9, 13, 14

[47] D. Liberzon, J. P. Hespanha, and A. S. Morse. Stability of switched systems: a lie-algebraic condition. *Systems & Control Letters*, 37(3):117 – 122, 1999. ISSN 0167-6911. doi:DOI:10.1016/S0167-6911(99)00012-2. → pages 2, 14

[48] N. Matni and M. Oishi. Reachability-based abstraction for an aircraft landing under shared control. In *Proceedings of the American Control Conference*, pages 2278–2284, Seattle, WA, June 2008. → pages 59, 63

[49] D. McRuer, I. Ashkenas, and D. Graham. *Aircraft dynamics and automatic control*. Princeton University Press, 1973. → pages 59

[50] R. Merris. Laplacian Matrices of Graphs: A Survey. *Linear Algebra and its Applications*, 10010:143–176, 1994. → pages 9

[51] I. M. Mitchell. A toolbox of level set methods. Technical report TR-2007-11, UBC Department of Computer Science, June 2007. → pages 30

[52] Y. Mori, T. Mori, and Y. Kuroe. A solution to the common lyapunov function problem for continuous-time systems. volume 4, pages 3530 –3531 vol.4, dec. 1997. doi:10.1109/CDC.1997.652397. → pages 2, 14

[53] R. M. Murray. Recent research in cooperative control of multivehicle systems. *Journal of Dynamic Systems, Measurement, and Control*, 129(5): 571–583, 2007. doi:10.1115/1.2766721. URL http://dx.doi.org/10.1115/1.2766721. → pages 2

[54] M. Oishi, I. Mitchell, A. M. Bayen, and C. J. Tomlin. Invariance-preserving abstractions of hybrid systems: Application to user interface design. *IEEE Transactions on Control System Technology*, 16(2):229–244, March 2008. → pages 4, 47, 51, 55, 57

[55] R. Olfati-Saber. Flocking for multi-agent dynamic systems: algorithms and theory. *Automatic Control, IEEE Transactions on*, 51(3):401 – 420, mar. 2006. ISSN 0018-9286. doi:10.1109/TAC.2005.864190. → pages 2

[56] R. Olfati-Saber and R. Murray. Consensus problems in networks of agents with switching topology and time-delays. *IEEE Transactions on Automatic Control*, 49(9):1520 – 1533, sep. 2004. ISSN 0018-9286. doi:10.1109/TAC.2004.834113. → pages 2

[57] P. Peleties and R. DeCarlo. Asymptotic stability of m-switched systems using lyapunov-like functions. In *Proceedings of the American Control Conference*, pages 1679 –1684, 26-28 1991. → pages 3

[58] M. Rotkowitz and S. Lall. A characterization of convex problems in decentralized control. *IEEE Transactions on Automatic Control*, 50(12): 1984 – 1996, dec. 2005. ISSN 0018-9286. doi:10.1109/TAC.2005.860365. → pages 2

[59] S. Sastry. *Nonlinear System*. Springer, Berlin, 1999. ISBN 9780387985138. → pages 17

[60] L. Sherry and R. Feary. Task design and verification testing for certification of avionics equipment. In *Proceedings of the AIAA/IEEE Digital Avionics Systems Conference*, pages 10.A.3–10.A.10, September 2004. → pages 4

[61] A. Suzuki, T. Ushio, and M. Adachi. Detection of automation surprisees in discrete event systems operated by multiple users. In *SICE-ICASE International Joint Conference*, pages 1115–1119, Korea, October 2006. → pages 4

[62] C. Tomlin. *Hybrid Control of Air Traffic Management Systems*. PhD thesis, University of California, Berkeley, CA, September 1998. → pages 8

[63] C. Tomlin, J. Lygeros, and S. Sastry. A game theoretic approach to controller design for hybrid systems. *Proceedings of the IEEE*, 88(7): 949–970, 2000. → pages 30

[64] C. Tomlin, I. Mitchell, A. Bayen, and M. Oishi. Computational techniques for the verification of hybrid systems. *Proceedings of the IEEE*, 91(7): 986–1001, 2003. → pages 51

[65] S. Umeno and N. Lynch. Safety verification of an aircraft landing protocol: A refinement approach. In A. Bemporad, A. Bicci, and G. Buttazzo, editors, *Hybrid Systems: Computation and Control*, LNCS 4416, pages 557–572. Springer Verlag, April 2007. → pages 4, 47

[66] K. Valavanis. *Advances in Unmanned Aerial Vehicles: State of the Art and the Road to Autonomy*. Springer, Berlin, 2007. ISBN 9781402061134. → pages 1

[67] L. Vu and K. Morgansen. Stability of feedback switched systems with state and switching delays. In *Proceedings of the American Control Conference*, pages 1754 –1759, 10-12 2009. doi:10.1109/ACC.2009.5160070. → pages 3, 29

[68] A. Williams, G. Lafferriere, and J. Veerman. Stable motions of vehicle formations. In *Proceedings of the IEEE Conference on Decision and Control and the European Control Conference*, pages 72–77, Dec. 2005. → pages 2, 10, 11

[69] G. Xie and L. Wang. Stabilization of switched linear systems with time-delay in detection of switching signal. *Journal of Mathematical Analysis and Applications*, 305(1):277 – 290, 2005. ISSN 0022-247X. doi:DOI:10.1016/j.jmaa.2004.11.043. → pages 3

[70] L. Zhang and H. Gao. Asynchronously switched control of switched linear systems with average dwell time. *Automatica*, 46(5):953 – 958, 2010. ISSN 0005-1098. doi:DOI:10.1016/j.automatica.2010.02.021. → pages 3