Provably Safe Design of Driver-Assist Systems through Hybrid Automata with Hidden Modes

by

Cassidy Martin Palas

Submitted to the Department of Mechanical Engineering
in partial fulfillment of the requirements for the degree of

Master of Science in Mechanical Engineering

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2012

Author .....
Department of Mechanical Engineering
May 11, 2012

Certified by .....
Domitilla Del Vecchio
Associate Professor
Thesis Supervisor

Accepted by .....
David Hardt
Chairman, Department Committee on Graduate Theses

Provably Safe Design of Driver-Assist Systems through Hybrid Automata with Hidden Modes

by

Cassidy Martin Palas

Submitted to the Department of Mechanical Engineering
on May 11, 2012, in partial fulfillment of the
requirements for the degree of
Master of Science in Mechanical Engineering

Abstract

In this thesis, I consider the problem of collision avoidance between two vehicles approaching an intersection. These vehicles are human driven and one or both are equipped with an on-board driver assist system that provides warnings and can apply automatic braking/throttle when needed. This type of system will establish an intermediary step in the progression towards fully autonomous vehicles. It will allow human drivers to retain control of their vehicles while providing the guidance for drivers to apply the necessary inputs to prevent collisions before autonomous control becomes necessary. A formal approach to the design of the driver assist system is taken, employing a hybrid automaton model. This model has hidden modes, which arise from the driver making decisions about whether or not to follow the provided warnings. As a consequence, the driver assist system design is formulated as a safety control problem for a hybrid automaton with hidden modes. The solution approach is based on a mode estimator that keeps track of the possible driver decisions and, on their basis, provides warning and control inputs that ensure safety. The resulting algorithm is computationally efficient as it leverages the order preserving properties of the vehicle dynamics.

Thesis Supervisor: Domitilla Del Vecchio
Title: Associate Professor

Acknowledgments

This thesis was made possible through the support of many people, and it is these people that have made my time MIT within the Multi-Vehicle Laboratory such a rewarding experience. I would first like to thank my thesis advisor, Professor Domitilla Del Vecchio, for her guidance, support, and understanding during my time working with her.

The next people that deserve recognition are my labmates within Dr. Del Vecchio's group, especially those working along side me on the multi-vehicle control problems. They were always available to discuss new ideas as well as roadblocks throughout my time here. I would also like to thank Brianna Woeckener, who worked with me as a UROP, for helping to make the transition from theory and simulation to experimentation easier.

I would like to thank all of my friends within the MechE department and the MIT community as a whole for making my time here so awesome. Even with the all of the time and effort put into my studies, it was these friends who kept my spirits high throughout. I also want to acknowledge my family for their love and support. They have helped me not only in graduate school, but in the entire chain of events that has brought me to where I am today.

Finally, I would like to express my gratitude to the MIT school of engineering and the Wheless family for their financial support provided through the Nicholas Hobson Wheless school of engineering fellowship, as well as the NSF for for their support of my research with the Graduate Research Fellowship. This funding allowed me to pursue research topics that may not have been possible had I been burdened with the need to acquire support from other sources.

Contents

1 Introduction **11**

1.1 Overview of Vehicle Safety Systems 12

1.2 The Problem of Navigating Intersections 13

1.3 Hybrid Automata as a Framework for Solving Safety Control Problems 14

1.4 Description of the Driver-Assist System 16

2 System Model and Problem Formulation **17**

2.1 General Framework 17

2.2 Problem Formulation 18

2.2.1 Case 1 19

2.2.2 Case 2 23

3 Design Strategy for Solving Safety Control Problem **27**

3.1 Designing an Estimator System 27

3.1.1 Case 1 Estimator System 29

3.1.2 Case 2 Estimator System 32

3.2 Determining the Maximal and Minimal Signals 35

3.3 Uncontrollable Predecessor Operator and Mode Dependent Capture Set 37

4 Solution to Safety Control Problems for Case 1 **39**

4.0.1 Solution of Problem 1' 39

4.0.2 Computational Tools 41

4.0.3 Solution to Problem 2' 45

4.0.4 Simulation 47

5 Solution to Safety Control Problems for Case 2 **51**

5.0.5 Solution of Problem 1' 51

5.0.6 Computational Tools 53

5.0.7 Solution to Problem 2' 58

5.0.8 Simulation 62

6 Experimental Validation of Algorithms **65**

6.1 Lab Setup 65

6.2 Status of Experiment 66

7 Conclusions and Future Work **69**

7.1 Future Work 69

List of Figures

2-1 Pictorial representation of the problem of interest. Two vehicles approach an intersection along predetermined paths. A represents the intersection and B represents the "bad set" (a collision). 19

2-2 Automaton representation of system H for Case 1. 21

2-3 Automaton representation of system H for Case 2. The generalized warning σ_u^{wi} is used in the interest of legibility. 24

3-1 Automaton representation of system $\hat{H}$ for Case 1. 31

3-2 Automaton representation of system $\hat{H}$ for Case 2. 33

3-3 Minimized disturbance signal compared with a nominal signal. The minimized signal produces a displacement which is always behind the nominal signal. 37

4-1 Accelerations used to back propagate the lower bound of the bad set for $C(ha^2)^H$ and the resulting curve. 43

4-2 Accelerations used to back propagate the lower bound of the bad set for $C(\{ho, hd\}^2)$ and the resulting curve. 44

4-3 Accelerations used to back propagate the lower bound of the bad set for $Pre(w^2, hd^2, \tau_{RT} + T, C(ha^2)^H)$ and the resulting curve. 45

4-4 Simulation results for the two vehicle system with $0 < v_{2_{min}} < v_{1_{min}}$ and $v_{2_{max}} > v_{1_{max}}$. All the bounded regions shown are slices of the mode dependent capture sets, corresponding to the capture sets for the current vehicle speeds (v_1, v_2). 49

5-1 Simulation results for the two vehicle system with $0 < v_{1_{min}} = v_{2_{min}}$ and $v_{1_{max}} = v_{2_{max}}$. All the bounded regions shown are slices of the mode dependent capture sets, corresponding to the capture sets for the current vehicle speeds (v_1, v_2). 64

6-1 Photo of Multi-Vehicle Laboratory. 66

Chapter 1

Introduction

The invention of the modern automobile fundamentally changed the way humans travel. It allowed people to effortlessly cover long distances in less time compared to other available transportation methods. Because of this, the automobile has been widely adopted as the standard form of transportation in nearly all developed countries, with approximately 250 million passenger cars in the United States alone (Bureau of Transportation, number of vehicles and vehicle classification. Retrieved 2006-06-08). With the utility that automobiles provide, however, come inherent dangers. One such danger arises from the navigation of intersections. In order to mitigate this danger and reduce the number of collisions between vehicles at intersections, an active driver-assist system was developed.

Chapter two describes the hybrid automaton model used to represent the traffic intersection, as well as the formulation of the safety problems for single vehicle and two vehicle control systems.

Chapter three describes the strategy used to solve the control problems, and develops the tools necessary to do so.

Chapter four describes the solution to the single vehicle problem, that is, the design of a controller which will satisfy the desired safety specification. A proof of the safety under the assumed dynamics as well and the system is implemented in a simulated environment.

Chapter four describes the solution to the two vehicle problem, again providing

the proof of safety and simulation results.

Chapter five describes the implementation of the driver assist system on dynamically scaled vehicles. The purpose of this experimentation is to test the real world practicality of the proposed algorithms as well as to discover any potential implementation issues. Possible continuations of the research and ways to utilize the design strategies for other similar problems are also discussed.

1.1 Overview of Vehicle Safety Systems

Most modern day automobiles have the capability to travel at velocities in excess of one hundred miles per hour and weigh more than a ton. While laws usually prevent cars from traveling that fast, vehicles traveling on highways routinely reach speeds of seventy or eighty miles per hour. Even at lower speeds, the amount of kinetic energy stored in a moving vehicle is immense. Combining this with the fact imperfect decision making ability of the human drivers controlling the vehicle, creates a potential for dangerous crashes to occur. This becomes especially clear when considering the fact that automobile crashes are the cause of 37.5% of all accidental deaths in the United States (National Vital Statistics Report, Volume 50, Number 15, September 2002). Many technological advances have improved automobile safety, but there is still potential for many more such improvements to be made.

Vehicle safety systems can be broken down into two main categories, passive and active. Passive systems are those that improve the crash-worthiness of the vehicle, by reducing injuries to passengers during collisions. Active safety systems, on the other hand, focus on prevent collisions from ever occurring. The number of fatalities in the U.S. due to automobile accidents declined from 1972 until 1992, a time period during which many advancements were made to the passive safety systems in automobiles. Notable examples of such improvements include collapsible structures built into the vehicle to absorb energy, safety belts worn by passengers, airbags in various locations around the vehicle, and car seats for smaller passengers. There was a notable lack of reductions in crash related fatalities after the 1990's, which is evidence that there

may be a limit to the effectiveness of such passive safety systems.

Recently, there has been a shift within the automotive manufacturing industry towards focusing more on the development of active safety systems [19, 15]. Rather than trying to minimize the damages caused by a collision, active safety systems attempt to prevent collisions from happening altogether. Such systems may warn drivers about potential crashes, and or provide ways to avoid them. In conjunction with these new active safety efforts, fatality statistics have begun to drop again. Notable examples of active safety systems that have recently become more widespread are lane departure warnings, forward crash warning, and blind spot monitoring. Additional efforts have examined the use of fully autonomous vehicles, such as the automated highway systems designed during the California PATH project, to increase traffic throughput, safety, and fuel efficiency of highways [21, 27, 14, 13]. More recent studies have investigated cooperative cruise control and semi-autonomous cruise control [20, 22]. However, none of these systems handle the issue of side impacts, a major problem while navigating intersections.

1.2 The Problem of Navigating Intersections

Nearly forty percent of all vehicle accidents occur at traffic intersections (The National Motor Vehicle Crash Causation Survey, US DOT, 2008), and very few active safety systems currently assist drivers in negotiating their way through intersections. This gap in technology provides an opportunity for innovative solutions to have a profound impact on the overall safety of the driving experience. Traditionally, a set of laws, along with traffic lights and stop signs have been used to provide drivers of a safe procedure to pass through intersections. These fixed procedures are only guaranteed to work if all drivers follow them, which is occasionally is not the case, such as when a driver runs a red light. Other similar traffic flow situations such as roundabouts and or mergings between roads depend solely on the human driver's ability to determine the correct control action from his or her own evaluation of the situation.

Eventually, we may reach a point where vehicles include fully automated colli-

sion avoidance systems at intersections, such as those considered in [12, 29] or even transition to fully autonomous cars, such as those developed for the DARPA urban challenge and by Google. Before either of these realities are realized, there is a closer target, which is the development of active safety systems that interact with the human driver, provide warnings, and only if necessary issue override commands.

As an alternative approach, this thesis focuses on the development of a driver assist system that incorporates a driver model in the control strategy. Specifically, a warning is applied to one or more vehicles such that the driver may act to prevent a collision without the need for autonomous intervention. There is a rich literature in the human factors that provide detailed models of how drivers respond to warnings and various stimuli (see, for example, [10, 23, 5, 9]). In this thesis, we take a very simple model, in which a driver is assumed to have a fixed time delay in responding to a warning and makes a binary decision between following the warning or not. While not the focus of this research, another important component of human machine interactions is user interface design [16], which affects the way a driver responds to stimuli.

1.3 Hybrid Automata as a Framework for Solving Safety Control Problems

Hybrid automata are used to formally model the semi-autonomous multi-vehicle systems of interest. This is because hybrid automata provide the ideal framework for this modeling because they enable formal treatment of continuous vehicle dynamics as well as discrete human and override decision making. This strategy is useful because often times humans switch between a number of relatively simple control laws, rather than using a single more complex law to accomplish complex tasks [17, 1, 4]. Also, there are also a number of works, such as [26], [24] and [12], that develop modeling and control techniques for hybrid systems which can be utilized. I formulate the driver-assist system design as a safety control problem for hybrid automata in which modes are hidden because of unobservable and uncontrollable human decisions. Our

solution is based on constructing a mode estimator and on calculating a capture set, complement of the maximal controlled invariant set [18, 25], for each mode estimate. A dynamic feedback map is then constructed to prevent the flow of the system from entering the current relevant capture set corresponding to the mode estimate.

Safety control problems for hybrid automata with hidden modes have been addressed before [29] and have been applied for collision avoidance at traffic intersections between fully autonomous vehicles and completely human-driven vehicles [28]. Here, different from [28], we consider semi-autonomous vehicles. Furthermore, we improve on the theoretical results of [29], for the specific application under study, by providing substantially less conservative ways to determine capture sets. Specifically, different from [29], we exploit the fact that when the estimator cannot distinguish between two modes, it means that the disturbance signal is playing to keep such a mode confusion. This implicitly reveals information on the disturbance choices, which we directly account for in the calculation of the capture sets. In order to efficiently compute these capture sets, we exploit the fact that the continuous systems dynamics are order preserving [12, 3]. For such systems and when the bad set to be avoided is a box, the capture sets can be efficiently computed by backward integrating the lower and upper bounds of the bad set through minimal and maximal input (control and disturbance) signals [6].

It is important to note that the control algorithms are developed under the assumption that state information for the multi-vehicle system is available. This information could be obtained with differential GPS, from the on-board computer, or other sensors located on-board the vehicle or at the intersection [8]. Dedicated short range communications devices would be used to distribute the state information [2], and the algorithms would be executed via on-board computers, taking advantage of drive-by-wire capabilities to execute necessary override commands.

1.4 Description of the Driver-Assist System

Three driver assist systems are developed for the following two vehicle cases: (1) one vehicle contains the system and the second is human driven and (2) both vehicles contain the system. Both of these systems utilize similar modeling and design techniques and are provably safe.

From the perspective of the driver, the system works as follows. The driver approaches an intersection in the vicinity of another vehicle. If the system detects the potential for a collision to occur, an audio, visual, or tactile warning is issued advising the driver to speed up or slow down to prevent said collision from occurring. After the driver processes the warning, he or she makes a decision whether or not to follow it. The system determines the driver's action and one of 3 scenarios may occur. (i) The driver obeys the warning and safely passes through the intersection. (ii) The driver disobeys the warning, but due to conservative assumptions made to guarantee safety in all cases, they still pass through the intersection safely. (iii) The driver disobeys the warning and approaches an unsafe condition, at this point, the driver-assist system overrides unsafe driver input with an alternative safe input to prevent the collision. Also, the driver may initially obey and disobey at a later point, but this is treated identically to when the driver disobeys immediately and therefore doesn't represent a novel case.

Chapter 2

System Model and Problem Formulation

2.1 General Framework

With the end goal of designing a driver assist system, I will first define the general model employed. This will introduce the necessary notation for formulating and then solving the safety control problem of interest. A hybrid automaton model is used because of the inherent coupling of continuous dynamics from the physical plant, and discrete dynamics resulting from human decisions.

Definition 1. A *hybrid automaton* is a tuple $H = (Q, X, \Sigma_u, \Sigma_d, U, D, R, f)$ in which, Q is a finite set of system modes, with $q \in Q$; $X \subset \mathbb{R}^n$ is a set of continuous states, with the continuous state $x \in X$; Σ_u is a set of control events, with each event $\sigma_u \in \Sigma_u$; Σ_d is a set of disturbance events, with each event $\sigma_d \in \Sigma_d$; U is a set of continuous control inputs, with the control input $u(t) \in U$; D is a set of continuous disturbance inputs, with the continuous disturbance input $d \in D$; $R : X \times Q \times \Sigma_u \times \Sigma_d \to Q$ is a discrete state update map; $f : X \times Q \times U \times D \to X$ is a piecewise continuous vector field.

For a set P, we denote the set of signals with values in P by $\mathcal{S}(P)$. Signals will also be denoted with **bold** symbols. Let $\{\tau_i'\}_{i \in \mathbb{N}} \subset \mathbb{R}$ be the set of transition times

for which $(\sigma_d, \sigma_u) \neq (\emptyset, \emptyset)$ with $\tau_i' \leq \tau_{i+1}'$. Let τ_{i+1} represent the time immediately after the i^{th} mode transition, that is, $q(\tau_{i+1}) = R(x(\tau_i'), q(\tau_i'), \sigma_u(\tau_i'), \sigma_d(\tau_i'))$. For input event signals $\boldsymbol{\sigma}_u$ and $\boldsymbol{\sigma}_d$ and initial mode q_o, the discrete flow of H is denoted $\phi_q(t, q_o, \boldsymbol{\sigma}_u, \boldsymbol{\sigma}_d) := q(\sup_{\tau_i \leq t} \tau_i)$ for $t \geq 0$. We will also denote $\phi_q(t, q_o, \sigma_u, \sigma_d)$ by $q(t)$. For input signals $\mathbf{u}, \mathbf{d}, \boldsymbol{\sigma}_d$, and $\boldsymbol{\sigma}_u$ the continuous flow of H is denoted $\phi_x(t, x_o, q_o, \mathbf{u}, \mathbf{d}, \boldsymbol{\sigma}_d, \boldsymbol{\sigma}_u) := x(t)$, where $\dot{x}(t) = f(x(t), q(t), u(t), d(t))$ unless executing a mode transition in R. The state $x(t) \in X$ is measured, but the mode q is not measured. However, since q affects the evolution of $x(t)$ through f, a filtering function $\mathcal{F} : \mathcal{S}(X) \to X$ is used to determine the possible range of $\dot{x}(t)$. For a fixed $T > 0$, we define the variable: $\hat{\beta}(t) := \mathcal{F}(x([t-T, t))$, for any $t \geq T$. Based on the available signals, $\hat{\boldsymbol{\beta}}, \boldsymbol{\sigma}_u$, and $\mathbf{u}$, and the known initial condition q_o, the discrete information state $\bar{q}(t) \in 2^Q$ represents all of the possible modes which the system could occupy at time t and is defined as $\bar{q}(t) := \{q \in Q \mid \exists\ \boldsymbol{\sigma}_d,\ \mathbf{d}, \text{ s.t. } q = \phi_q(t, q_o, \boldsymbol{\sigma}_u, \boldsymbol{\sigma}_d) \text{ and } \mathcal{F}(x([\tau - T, \tau])) = \hat{\beta}(\tau),\ \forall\ T \leq \tau \leq t\}$. In order to control the system, a feedback map $\mathfrak{B} : 2^Q \times X \to U \times \Sigma_u$ is introduced. Applying this feedback map to the system produces the closed loop continuous flow $\phi_x^\pi(t, x_o, q_o, \mathbf{d}, \boldsymbol{\sigma}_d) = \phi_x(t, x_o, q_o, \mathbf{u}, \mathbf{d}, \boldsymbol{\sigma}_d, \boldsymbol{\sigma}_u)$, with $(u(t), \sigma_u(t)) = \mathfrak{B}(\bar{q}(t), x(t))$.

The safety property, $\Box F(\phi_x)$, which a controller must guarantee is defined for some bad set, $B \subset X$, as:

$$\Box F(\phi_x) := \begin{cases} \text{true} & \text{if } \forall t.\ \phi_x(t, x_o, q_o, \mathbf{u}, \mathbf{d}, \boldsymbol{\sigma}_d, \boldsymbol{\sigma}_u) \notin B \\ \text{false} & \text{otherwise,} \end{cases}$$

in which the period is a short-hand notation for "we have that".

2.2 Problem Formulation

Based on this safety property, it is possible to define the two-part safety control problem for system H as:

Determine $S := \{x_o | \forall \pi\ \exists\ \hat{\boldsymbol{\beta}} \text{ and } (\mathbf{d}, \boldsymbol{\sigma}_d) \text{ with } \mathcal{F}(x([\tau - T, \tau])) = \hat{\beta}(\tau),\ T \leq \tau \leq t \text{ s.t. } \Box F(\phi_x^\pi) = \text{false}\}$.

Determine $\pi(\bar{q}, x)$ s.t. $x_o \notin S \Rightarrow \forall t.\ \Box F(\phi_x^\pi) = \text{true}$.

S represents the set of all points in the state space for which, if no warning is issued, there is a some disturbance input sequence that will cause a collision. By finding S, and using that set to determine when a warning is needed, the system avoids applying control too soon. The solution to Problem 1 and Problem 2 for a collision avoidance problem at a traffic intersection will provide the control map for the driver assist system of interest. Specifically, we consider the two-vehicle system at an intersection depicted in Figure 2-1 and consider the safety control problem of preventing collisions in the intersection. Two cases are considered:

1) Vehicle 1 is completely human controlled, while vehicle 2 is outfitted with the driver assist system.

2) Both vehicles are outfitted with the driver assist system.

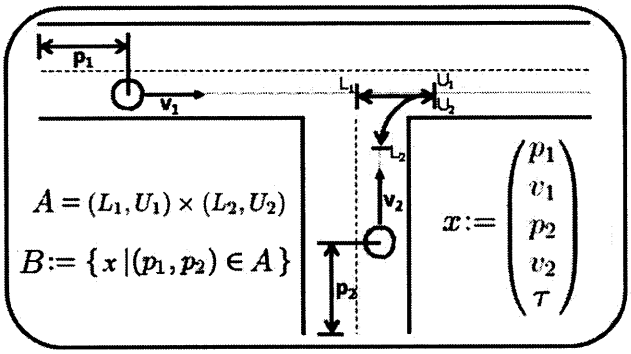


Figure 2-1: Pictorial representation of the problem of interest. Two vehicles approach an intersection along predetermined paths. A represents the intersection and B represents the "bad set" (a collision).

2.2.1 Case 1

We model this system as a hybrid automaton $H = (Q, X, \Sigma_u, \Sigma_d, U, D, R, f)$ as follows. Let $Q := \{h, w^1, w^2, ho^1, hd^1, ho^2, hd^2, ha^1, ha^2\}$ be the set of modes containing various combinations of the vehicles while human controlled and autonomously controlled. The vehicles are initially both human driven, corresponding to $q_o = h$. After one of two warnings (brake or accelerate - denoted by superscript 1 and 2, respec-

tively) is issued to vehicle 2, the mode progresses to $q \in \{w^1, w^2\}$. After a reaction time $\tau_{RT} > 0$ has elapsed, the driver chooses to obey or disobey the warning and the mode shifts to $q \in \{ho^1, hd^1, ho^1, hd^2\}$ with the "o" indicating driver obedience and the "d" indicating driver disobedience. If necessary, vehicle 2 will be overridden and controlled autonomously. If this occurs, the mode will enter $q \in \{ha^1, ha^2\}$ where ha^1 will have automated braking and ha^2 will have automated acceleration. $X := \mathbb{R}^5$ is the set of continuous states of the system with $x \in X$ given by $x = (p_1, v_1, p_2, v_2, \tau)^T$, including the position and velocities of each vehicle, and a counter variable τ, necessary to implement the τ_{RT} dwell time after a warning is issued. When referring to a single vehicle, the notation $x_i = (p_i, v_i, \tau)^T$ will be used. The initial state of the system is denoted $x = (p_{1o}, v_{1o}, p_{2o}, v_{2o}, \tau_o)^T$, with $\tau_o = 0$. $\Sigma_u := \{\sigma_u^{w1}, \sigma_u^{w2}, \sigma_u^1, \sigma_u^2\}$ is the set of control events. σ_u^{w1} and σ_u^{w2} correspond to issuing a warning for vehicle 2 to brake and accelerate, respectively. σ_u^1 is an autonomous override of a vehicle disobeying warning 1, and σ_u^2 is an autonomous override of a vehicle disobeying warning 2. $\Sigma_d := \{\sigma_d^o, \sigma_d^d\}$ is the set of disturbance events. σ_d^o indicates that the driver has obeyed the provided warning. σ_d^d indicates that the driver has disobeyed the provided warning. The continuous control input ranges within the set $U := [-\bar{u}, \bar{u}], \bar{u} > 0$. The continuous disturbance input ranges within the set $D := (D_1 \times D_2)$, $D_i = [-\bar{d}, \bar{d}], \bar{d} > 0$ with $d \in D$ given by (d_1, d_2). Physically, d_1 and d_2 represent the drivers' input via the gas and brake pedals of the vehicle.

Figure 2-2 provides a visual representation of the discrete update map, $R(\tau_q, \sigma_u, \sigma_d)$. Each mode is represented by a circle and the transitions between modes are represented by blue and red arrows. The blue arrows are control events, while the red arrows are disturbance events. As stated, the system is initialized with $q_o = h$ and progresses through the automaton as necessary. The left and right sides of the automaton correspond to two different warnings, which specify that vehicle 2 should brake or accelerate to maintain safety. Let $\tau_{RT} \geq 0$ represent the "reaction time" of the drivers, that is, the length of time required to acknowledge and act upon an issued warning.

Define two maps $\mu : Q \to \mathbb{R}$ and $\gamma : Q \to \mathbb{R}^2$, with $\gamma = (\gamma_d, \gamma_u)$. The value of

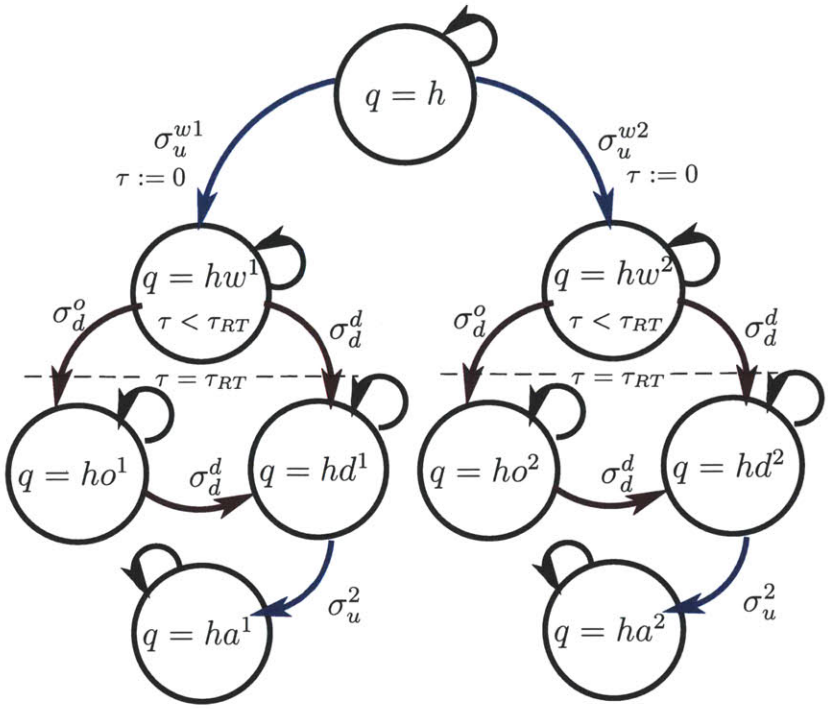


Figure 2-2: Automaton representation of system H for Case 1.

these maps modulate the effect of d and u on the system dynamics with $[d_{min}, d_{max}]$ as the range of possible driver-applied accelerations and $[u_{min}, u_{max}]$ as the range of possible control-applied accelerations. Let ϵ be some positive value, then:

$$\mu(q) := \begin{cases} \frac{d_{max}+d_{min}}{2} & \text{if } q \in \{h, hw^1, hw^2, hd^1, hd^2\} \\ d_{min} & \text{if } q = ho^1 \\ d_{max} & \text{if } q = ho^2 \\ \frac{u_{min}+d_{min}}{2} & \text{if } q = ha^1 \\ \frac{u_{max}+d_{max}}{2} & \text{if } q = ha^2, \end{cases}$$

$$\gamma_d(q) := \begin{cases} \frac{d_{max}-d_{min}}{2\tilde{d}} & \text{if } q \in \{h, hw^1, hw^2, hd^1, hd^2\} \\ \frac{\epsilon}{\tilde{d}} & \text{if } q \in \{ho^1, ho^2\} \\ 0 & \text{otherwise,} \end{cases}$$

$$\gamma_u(q) := \begin{cases} |\frac{u_{min}-d_{min}}{2\bar{u}}| & \text{if } q = ha^1 \\ |\frac{u_{max}-d_{max}}{2\bar{u}}| & \text{if } q = ha^2 \\ 0 & \text{otherwise.} \end{cases}$$

Vector field f_i provides vehicle i longitudinal dynamics along its path. Both vehicles exhibit double integrator dynamics with velocity saturation such that the velocity for vehicle i remains within $[v_{i_{min}}, v_{i_{max}}]$. It also contains the dynamics for a counter variable τ, which is initialized at $\tau = 0$ when the warning is issued, and tracks the elapsed time afterwards. We define $\alpha_1 := \frac{d_{max}-d_{min}}{2\bar{d}} d_1$ and $\alpha_2 := \mu(q) + \gamma_d(q)d_2 + \gamma_u(q)u$, then $f = (f_1, f_2)$ with:

$$f_i(x_i, q, u, d_i) := \begin{cases} v_i \\ \begin{cases} \alpha_i & \text{if } v_i \in (v_{i_{min}}, v_{i_{max}}) \vee (v_i = v_{i_{max}} \wedge \alpha_i \leq 0) \vee (v_i = v_{i_{min}} \wedge \alpha_i \geq 0) \\ 0 & \text{otherwise} \end{cases} \\ \begin{cases} 0 & \text{if } q = h \\ 1 & \text{otherwise} \end{cases} \end{cases}$$

In an effort to maintain driver confidence in the system, the choice of range for γ_u was made such that the acceleration produced by the control input is always in $[u_{min}, d_{min}]$ for warning 1 and $[d_{max}, u_{max}]$ for warning 2. Because the controller can only apply accelerations of the same sign and of greater or equal magnitude than the specified accelerations, the drivers should not be surprised by the control actions.

The safety control problem is as defined in Section 2.2, with the bad set B equal to the set of all points in the state space such that the position of both vehicles are simultaneously in the intersection, as indicated by Figure 2-1, and the initial mode is given by $q_o = \bar{q}_o = h$.

2.2.2 Case 2

Case 2 uses a similar hybrid automaton to that of Case 1, but it is complicated by the fact that both cars include the discrete decision dynamics associated with the warning system, expanding the number of possible modes. Incorporating this change, Q becomes $\{h, w^1, w^2, oo^1, oo^2, od^1, od^2, do^1, do^2, oa^1, oa^2, ao^1, ao^2, dd^1, dd^2, da^1, da^2, ad^1, ad^2, a^1, a^2\}$. Each driver assist system will progress through the same sequence or events: one of two warnings is issued, the driver obeys or not, and the system overrides if necessary. In Case 3, both cars require control and disturbance inputs, so the continuous control input ranges within the set $U := (U_1 \times U_2)$, $U_i = [-\bar{u}, \bar{u}], \bar{u} > 0$ with $u \in U$ given by (u_1, u_2), and the disturbance ranges the set $D := (D_1 \times D_2)$, $D_i = [-\bar{d}, \bar{d}], \bar{d} > 0$ with $d \in D$ given by (d_1, d_2).

Figure 2-3 provides a visual representation of the discrete update map, $R(\tau_q, \sigma_u, \sigma_d)$ for Case 2, accounting for the changes in Q. Again, each mode is represented by a circle and the transitions between modes are represented by blue and red arrows. The blue arrows are control events, while the red arrows are disturbance events. $\mu(q)$ and $\gamma(q)$ need to be adjusted to account for the changes in Q. Since the two cars will be issued opposite warning, these maps need to be individualized for each car.

$$\mu_1(q) := \begin{cases} \frac{d_{max}+d_{min}}{2} & \text{if } q \in \{h, w^1, w^2, dd^1, dd^2, do^1, do^2, da^1, da^2\} \\ d_{min} & \text{if } q \in \{oo^2, od^2, oa^2\} \\ d_{max} & \text{if } q \in \{oo^1, od^1, oa^1\} \\ \frac{u_{min}+d_{min}}{2} & \text{if } q \in \{ao^2, ad^2, a^2\} \\ \frac{u_{max}+d_{max}}{2} & \text{if } q \in \{ao^1, ad^1, a^1\}, \end{cases}$$

$$\mu_2(q) := \begin{cases} \frac{d_{max}+d_{min}}{2} & \text{if } q \in \{h, w^1, w^2, dd^1, dd^2, od^1, od^2, ad^1, ad^2\} \\ d_{min} & \text{if } q \in \{oo^1, do^1, ao^1\} \\ d_{max} & \text{if } q \in \{oo,^2, do^2, ao^2\} \\ \frac{u_{min}+d_{min}}{2} & \text{if } q \in \{oa^1, da^1, a^1\} \\ \frac{u_{max}+d_{max}}{2} & \text{if } q \in \{oa^2, da^2, a^2\}, \end{cases}$$

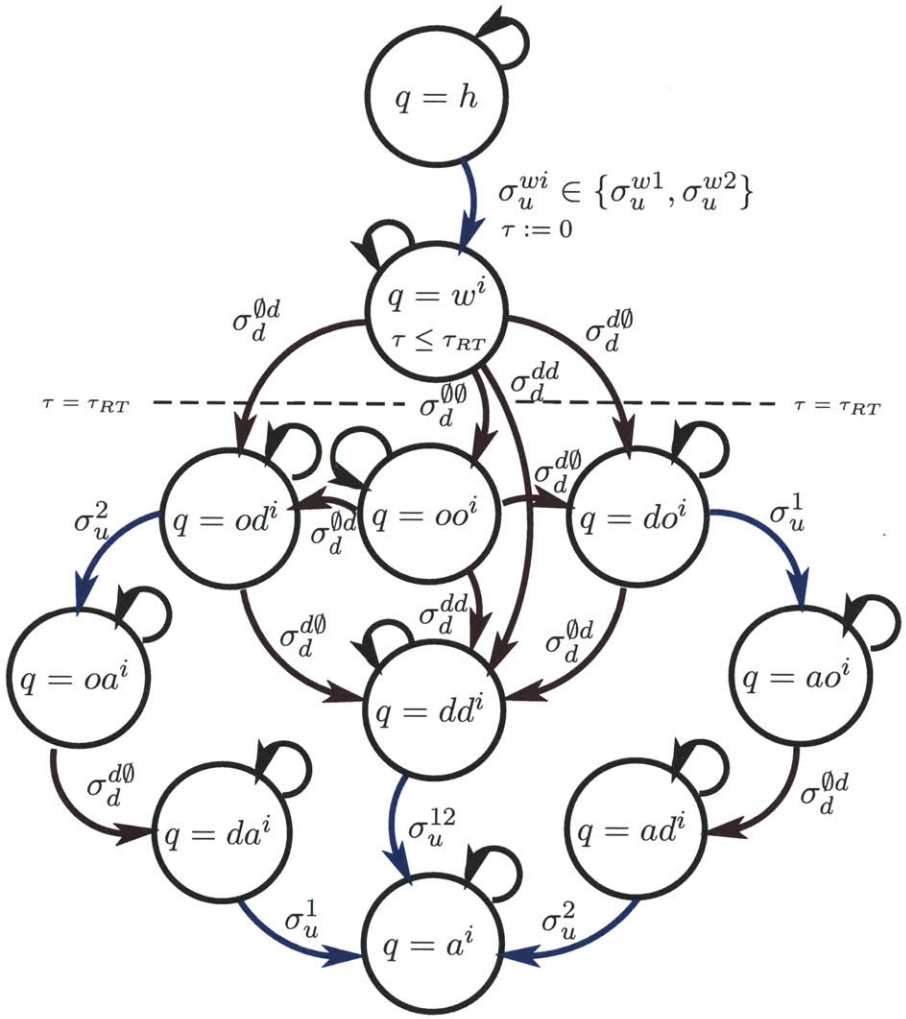


Figure 2-3: Automaton representation of system H for Case 2. The generalized warning σ_u^{wi} is used in the interest of legibility.

$$\gamma_{d1}(q) := \begin{cases} \frac{d_{max}-d_{min}}{2d} & \text{if } q \in \{h, w^1, w^2, dd^1, dd^2, do^1, do^2, da^1, da^2\} \\ \frac{\epsilon}{d} & \text{if } q \in \{oo^1, oo^2, oa^1, oa^2, od^1, od^2\} \\ 0 & \text{otherwise,} \end{cases}$$

$$\gamma_{d2}(q) := \begin{cases} \frac{d_{max}-d_{min}}{2d} & \text{if } q \in \{h, w^1, w^2, dd^1, dd^2, do^1, do^2, da^1, da^2\} \\ \frac{\epsilon}{d} & \text{if } q \in \{oo^1, oo^2, ao^1, ao^2, do^1, do^2\} \\ 0 & \text{otherwise,} \end{cases}$$

$$\gamma_{u1}(q) := \begin{cases} |\frac{u_{min}-d_{min}}{2\bar{u}}| & \text{if } q \in \{a^2, ao^2, ad^2\} \\ |\frac{u_{max}-d_{max}}{2\bar{u}}| & \text{if } q \in \{a^1, ao^1, ad^1\} \\ 0 & \text{otherwise.} \end{cases}$$

$$\gamma_{u2}(q) := \begin{cases} |\frac{u_{min}-d_{min}}{2\bar{u}}| & \text{if } q \in \{a^1, oa^1, da^1\} \\ |\frac{u_{max}-d_{max}}{2\bar{u}}| & \text{if } q \in \{a^2, oa^2, da^2\} \\ 0 & \text{otherwise.} \end{cases}$$

With these new definitions, $\alpha_1 := \mu_1(q) + \gamma_{d1}(q)d_1 + \gamma_{u1}(q)u_1$ and $\alpha_2 := \mu_2(q) + \gamma_{d2}(q)d_2 + \gamma_{u2}(q)u_2$, while f remains identical to Cases 1. So, for case 2, the safety control problem is as defined in Section 2.2, with the bad set B equal to the set of all points in the state space such that the position of both vehicles are simultaneously in the intersection, as indicated by Figure 2-1, and the initial mode is given by $q_o = \bar{q}_o = h$.

With the hybrid automaton model defined for each of the 2 cases of interest, a solution to each case will be proposed, along with a proof of its safety, and simulation results for various system evolutions.

Chapter 3

Design Strategy for Solving Safety Control Problem

Chapter two formalized the safety control problems of interest. This chapter develops the general strategy to solve both of these problems. By employing this strategy, I was able to develop suitable control maps which guarantee the safety of the system for Cases 1 and 2.

3.1 Designing an Estimator System

In order to solve the safety control problems introduced in Section 2.2, we must construct an update law for $\bar{q}(t)$. We construct such an update law in the form of a mode estimator. Here, we introduce a hybrid estimator system, $\hat{H}$, based on system H. For $\hat{H}$ we can define equivalent safety control problems, but with perfect state information, which will also guarantee safety of the original system H.

Definition 2. A *hybrid estimator system* is a tuple $\hat{H} = (\hat{Q}, X, \Sigma_u, I, U, D, \Delta, \mathcal{F}, \hat{R}, \hat{f})$, in which X, Σ_u, U, D are as defined for system H, with the continuous state now denoted by $\hat{x} \in X$; $\hat{Q} \subseteq 2^Q$ is the set of discrete system modes and we denote a mode by $\hat{q} \in \hat{Q}$; $I \subset \mathbb{R} \cup \emptyset$ is a set of continuous inputs and $\hat{\beta}(t) \in I$; $\hat{i}(t) = \emptyset$ when no mode transition occurs, otherwise $\hat{i}(t) = \hat{\beta}(t)$. $\Delta : \hat{Q} \to 2^I$ is a map that establishes for every mode $\hat{q} \in \hat{Q}$ the domain where $\mathcal{F}(\hat{x}([\tau - T, \tau]))$ is restricted

while the mode at time τ is $\hat{q}$; $\hat{R} : X \times \hat{Q} \times \Sigma_u \times I \to \hat{Q}$ is the mode update map; $\hat{f} : \hat{Q} \times X \times U \times D \to 2^X$ is a set-valued map establishing the continuous dynamics: $\dot{\hat{x}} \in \hat{f}(\hat{q}, \hat{x}, u, D) := \{f(q, \hat{x}, u, D) | q \in \hat{q}\}$ and $\mathcal{F}(\hat{x}([t-T, t])) \in \Delta(\hat{q}(t))$.

Let $\{\hat{\tau}_i'\}_{i \in \mathbb{N}} \subset \mathbb{R}$ be the set of transition times for which $\hat{i}(t) \neq \emptyset$ with $\hat{\tau}_i' \leq \hat{\tau}_{i+1}'$. Let $\hat{\tau}_{i+1}$ represent the time immediately after the i^{th} mode transition, such that, $\hat{q}(\hat{\tau}_{i+1}) = \hat{R}(\hat{x}(\tau_i'), \hat{q}(\hat{\tau}_i'), \sigma_u(\tau_i'), \hat{\boldsymbol{i}}(\tau_i'))$. For input signals $\boldsymbol{\sigma}_u, \hat{\boldsymbol{i}}$ and initial condition $\hat{q}_o$, the discrete flow of $\hat{H}$ is denoted $\phi_{\hat{q}}(t, \hat{q}_o, \boldsymbol{\sigma}_u, \hat{\boldsymbol{i}}) := \hat{q}(\sup_{\hat{\tau}_i \leq t} \hat{\tau}_i)$, for $t > 0$. We also use the notation $\hat{q}(t) = \phi_{\hat{q}}(t, \hat{q}_o, \boldsymbol{\sigma}_u, \hat{\boldsymbol{i}})$. The continuous flow of $\hat{H}$ is denoted $\phi_{\hat{x}}(t, \hat{x}_o, \hat{q}_o, \mathbf{u}, \mathbf{d}, \boldsymbol{\alpha}_\mathbf{u}, \hat{\boldsymbol{i}}) := \hat{x}(t)$, where $\dot{\hat{x}}(t) \in \hat{f}(\hat{q}(t), \hat{x}(t), u(t), d(t))$ unless executing a mode transition in $\hat{R}$. The "silent" input $i(t) = \emptyset$ denotes no mode transition taking place at time t. This is equivalent to requiring $\hat{R}(\hat{x}, q, \sigma_u, \emptyset) = q$. Consider a feedback map $\hat{\mathbf{\beta}} : \hat{Q} \times X \to U \times \Sigma_u$. The continuous flow of the system with this control map applied is $\phi_{\hat{x}}^{\hat{\pi}}(t, \hat{x}_o, \hat{q}_o, \mathbf{d}, \hat{\boldsymbol{i}}) = \phi_{\hat{x}}(t, \hat{x}_o, \hat{q}_o, \mathbf{u}, \mathbf{d}, \boldsymbol{\sigma}_u, \hat{\boldsymbol{i}})$, with $(u(t), \sigma_u(t)) = \hat{\pi}(\hat{q}(t), \hat{x}(t))$. We denote by $\phi_{\hat{x}}^{\hat{\pi}}(t, \hat{x}_o, \hat{q}_o, \mathbf{d}, \emptyset)$ the flow when $\hat{q}(t) = \hat{q}_o$ for all t.

Definition 3. We say that system $\hat{H}$ is an *exact estimator* if it has the following properties:

(a) $\hat{q}(t) = \bar{q}(t)$ for all t (it keeps track of all and only those modes compatible with the system dynamics and the measurements);

(b) Given $\hat{\beta}(t)$ and $\bar{q}(t)$, we have that $\hat{\beta}(t) \in \Delta(\bar{q}(t))$;

(c) For any $x(\cdot)$ trajectory of H and the resulting $\hat{\boldsymbol{\beta}}$, there is a trajectory $\hat{x}(\cdot)$ of $\hat{H}$ such that $\hat{x}(t) = x(t)$ for all t;

(d) Given $\hat{\boldsymbol{\beta}}$ generated by H and a resulting $\hat{x}(\cdot)$ trajectory in $\hat{H}$, there is a trajectory $x(\cdot)$ of H such that $\mathcal{F}(x([t-T, t])) = \hat{\beta}(t)$ for all $t \geq T$ and $x(t) = \hat{x}(t)$ for all $t \geq 0$.

The new safety control problem with perfect information for system $\hat{H}$ is:

Problem 1. *(Problem 1')* Determine the set $\hat{S} := \{\hat{x}_o \mid \forall\, \hat{\pi}\ \exists\, \hat{\boldsymbol{i}}$ and $\boldsymbol{d}$ *s.t.* $\Box F(\phi_{\hat{x}}^{\hat{\pi}}) =$ false$\}$.

Problem 2. *(**Problem 2'**) Determine a feedback map $\hat{\pi}$ such that $\hat{x}_o \notin \hat{S} \rightarrow \Box F(\phi_{\hat{x}}^{\hat{\pi}}) = true$.*

The following theorem ensures that solving Problems 1' and 2' is equivalent to solving the original Problems 1 and 2.

Theorem 1. *If system $\hat{H}$ is an exact estimator, then $\hat{S} = S$.*

Proof. We first show that $\hat{S} \subseteq S$. Let $x_o \in \hat{S}$, then for all $\hat{\pi}$ there is $\hat{\boldsymbol{i}}$ and $\boldsymbol{d}$ with $\mathcal{F}(\hat{x}([\tau - T, \tau])) \in \Delta(\hat{q}(t))\ \forall\ \tau \leq t$ such that $\hat{x}(t) = \phi_{\hat{x}}^{\hat{\pi}}(t, x_o, q_o, \mathbf{d}, \hat{\boldsymbol{i}}) \in B$. By property (d), for such a $\hat{\boldsymbol{i}}$ and $\hat{x}(\cdot)$ trajectory there is a trajectory $x(\cdot)$ in H such that $x(t) = \hat{x}(t)$ for all t and $\mathcal{F}(x([t-T, t])) = \hat{\beta}(t)$ for all $t \geq T$. Hence, there are $\hat{\boldsymbol{\beta}}$, $\boldsymbol{d}$, and $\boldsymbol{\sigma}_d$ such that $x(t) = \phi_x^{\hat{\pi}}(t, x_o, q_o, \boldsymbol{d}, \boldsymbol{\sigma}_d) \in B$ and $\mathcal{F}(x([t-T, t])) = \hat{\beta}(t)$. By property (a), this implies $x_o \in S$.

We show that $S \subseteq \hat{S}$. Let $x_o \in S$, then for all maps π, there are $\hat{\boldsymbol{\beta}}$ and $(\boldsymbol{\sigma}_d, \boldsymbol{d})$ with $\mathcal{F}(x([\tau - T, \tau])) = \hat{\beta}(\tau)\ \forall\ T \leq \tau \leq t$ such that $\phi_x^{\pi}(t, x_o, q_o, \boldsymbol{d}, \boldsymbol{\sigma}_d) \in B$. By properties (a)-(b), we have that such a trajectory $x(\cdot)$ is also such that $\mathcal{F}(x([t - T, t])) \in \Delta(\hat{q}(t))\ \forall\ T \leq \tau \leq t$. Using property (c), we obtain that for such a $\hat{\boldsymbol{\beta}}$ and $x(\cdot)$ there is a trajectory $\hat{x}(\cdot)$ of $\hat{H}$ such that $\hat{x}(t) = x(t)$ for all t. It follows that $x_o \in \hat{S}$.

□

With the structure of a hybrid estimator system defined, it is now possible to develop the appropriate systems for both cases of interest.

3.1.1 Case 1 Estimator System

Here I re-examine Case 1, this time with the intent of designing a hybrid estimator, $\hat{H} = (\hat{Q}, X, \Sigma_u, I, U, D, \Delta, \mathcal{F}, \hat{R}, \hat{f})$ as introduced by Definition 2. Specifically, X, Σ_u, U, and D are as defined for H in Section 2.2.1. We define $\hat{Q} := \{h, w^1, w^2, \{ho, hd\}^1, \{ho, hd\}^2, hd^1, hd^2, ha^1, ha^2\}$ as the set of mode estimates. These are subsets of the modes of system H. For example, $\hat{q} = \{ho, hd\}^1$ indicates that the estimator does not have enough information to determine whether the true mode of

the system is $q = ho^1$ or $q = hd^1$, so the system H could be in either of them. The input $\hat{\beta} \in \mathcal{S}(I)$ is given by $\hat{\beta}(t) := \frac{v_2(t)-v_2(t-T)}{T}$ for $t \geq T$.

It provides information regarding the true mode of H. Note that while $t < \tau_{RT}+T$, $\hat{\beta}(t)$ cannot be used for estimation because for $t < \tau_{RT}$ the driver has not made any obedience decision, and it takes time T for $\hat{\beta}$ to output a value once the driver has decided. This is accounted for by the structure of $\hat{R}$. Define the map $\mathcal{F}(\hat{x}([t-T,t]) := \frac{\hat{v}_2(t)-\hat{v}_2(t-T)}{T}$ for $t \geq T$, the domain of which is restricted by the map:

$$\Delta(\hat{q}) := \begin{cases} [d_{min}, d_{min} + \epsilon] & \text{if } \hat{q} = \{ho, hd\}^1 \\ [d_{max} - \epsilon, d_{max}] & \text{if } \hat{q} = \{ho, hd\}^2 \\ \text{anything} & \text{otherwise.} \end{cases}$$

$\Delta(\hat{q})$ is defined as a small range about the specified warning acceleration for two reasons. The first is that as the time parameter T approaches 0, Δ restricts α_2 directly because $\hat{\beta}(t)$ approaches $\alpha_2(t)$. This corresponds to having an "instant" estimator, and the range of Δ ensures that the disturbance is producing an acceleration α_2 close to the acceleration specified by the warning. The second reason is to ensure that the estimator has no "false negatives" in which it incorrectly estimates that the driver of vehicle 2 has disobeyed.

Figure 3-2 provides a visual representation of the discrete update map, $\hat{R}(\tau, \hat{q}, \sigma_u, \hat{i})$. Each mode estimate is represented by a circle and the transitions between modes are represented by blue and red arrows. The blue arrows are control events, while the red arrows are estimator observance events. The system is initialized with $\hat{q} = h$ and progresses through the other modes as necessary. Again, the left and right sides of the automaton correspond to the two different warnings, brake and accelerate.

Define three maps $\hat{\mu} : \hat{Q} \to \mathbb{R}$ and $\hat{\gamma} : \hat{Q} \to \mathbb{R}^2$, with $\hat{\gamma} = (\hat{\gamma}_d, \hat{\gamma}_u)$. The value of these maps modulates the effect of d and u in the system dynamics.

$$\hat{\mu}(\hat{q}) := \begin{cases} \frac{u_{min}+d_{min}}{2} & \text{if } \hat{q} = ha^1 \\ \frac{u_{max}+d_{max}}{2} & \text{if } \hat{q} = ha^2 \\ \frac{d_{max}+d_{min}}{2} & \text{otherwise.} \end{cases}$$

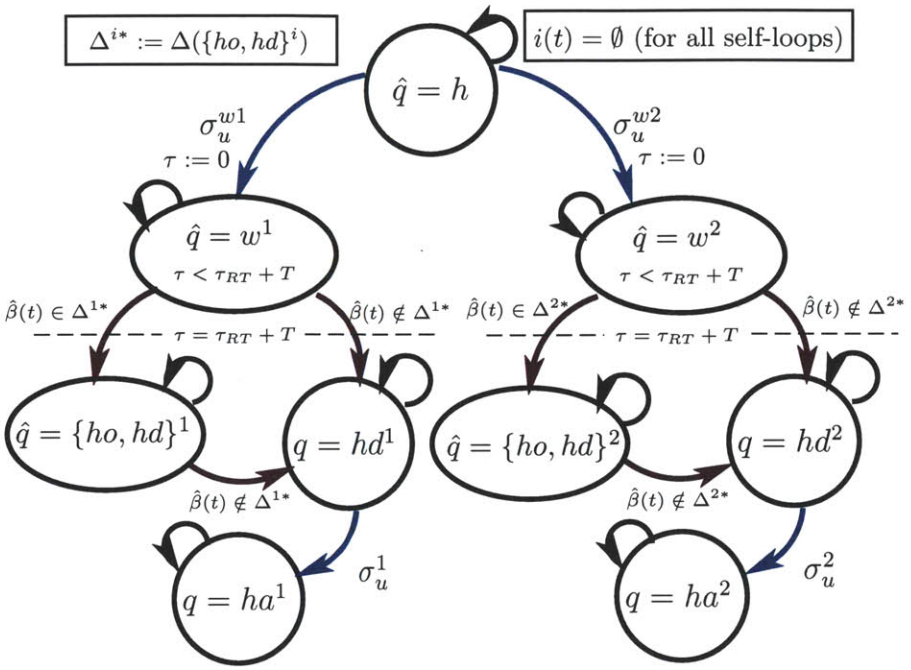


Figure 3-1: Automaton representation of system $\hat{H}$ for Case 1.

$$\hat{\gamma}_d(\hat{q}) := \begin{cases} 0 & \text{if } \hat{q} \in \{ha^1, ha^2\} \\ \frac{d_{max} - d_{min}}{2d} & \text{otherwise.} \end{cases}$$

$$\hat{\gamma}_u(\hat{q}) := \begin{cases} |\frac{u_{min} - d_{min}}{2\bar{u}}| & \text{if } \hat{q} = ha^1 \\ |\frac{u_{max} - d_{max}}{2\bar{u}}| & \text{if } \hat{q} = ha^2 \\ 0 & \text{otherwise.} \end{cases}$$

Define $\hat{\alpha}_1 = \frac{d_{max} - d_{min}}{2d} d_1$ and $\hat{\alpha}_2 = \hat{\mu}(\hat{q}) + \hat{\gamma}_d(\hat{q}) d_2 + \hat{\gamma}_u(q) u$. Define $\dot{\tau} := 0$ if $\hat{q} = h$ and $\dot{\tau} := 1$ otherwise. Then $\hat{f} = (\hat{f}_1, \hat{f}_2)$ with $\hat{f}_i(\hat{x}_i, \hat{q}, u, d_i) := (v_i, \alpha_i, \dot{\tau})^T$ if $\hat{v}_i \in (v_{i_{min}}, v_{i_{max}}) \vee (\hat{v}_i = v_{i_{max}} \wedge \hat{\alpha}_i \leq 0) \vee (\hat{v}_i = v_{i_{min}} \wedge \hat{\alpha}_i \geq 0)$ and $\hat{f}_i(\hat{x}_i, \hat{q}, u, d_i) := (v_i, 0, \dot{\tau})^T$ otherwise. By construction, $\hat{f}_i(\hat{x}_i, \hat{q}, u, D_i) = \cup_{q \in \hat{q}} f_i(\hat{x}_i, q, u, D_i)$. That is, the set of vector fields $\hat{f}_i$ provides the union of all of the possible vehicle dynamics for vehicle i based on the current mode estimate. The safety control problem for $\hat{H}$ is as defined, in Problem 1, with the bad set defined as both vehicles simultaneously occupying the intersection and with the initial mode $\hat{q} = h$. As shown in Theorem 1, these two problems are equivalent to the safety control problems for system H if $\hat{H}$ is an exact estimator. It is possible to show that $\hat{H}$ is an exact estimator and it follows by its

construction.

3.1.2 Case 2 Estimator System

We re-examine Case 2, this time with the intent of designing a hybrid estimator, $\hat{H} = (\hat{Q}, X, \Sigma_u, I, U, D, \Delta, \mathcal{F}, \hat{R}, \hat{f})$ as introduced by Definition 2. Specifically, X, Σ_u, U, and D are as defined for H in Section 2.2.2. We define $\hat{Q} := \{h, w^1, w^2, \{oo, do, od, dd\}^1, \{oo, do, od, dd\}^2, \{od, dd\}^1, \{od, dd\}^2\}, \{do, dd\}^1, \{do, dd\}^2, \{oa, da\}^1, \{oa, da\}^2, dd^1, dd^2, \{ao, ad\}^1, \{ao, ad\}^2, da^1, da^2, ad^1, ad^2, a^1, a^2\}$ as the set of mode estimates. These are subsets of the modes of system H. For example, $\hat{q} = \{od, dd\}^1$ indicates that the estimator does not have enough information to determine whether the true mode of the system is $q = od^1$ or $q = dd^1$, so the system H could be in either of them. The input $\hat{\boldsymbol{\beta}}_j \in \mathcal{S}(I)$ is given by $\hat{\beta}_j(t) := \frac{v_j(t) - v_j(t-T)}{T}$ for $t \geq T$.

It provides information regarding the true mode of H. Note that while $t < \tau_{RT} + T$, $\hat{\beta}_j(t)$ cannot be used for estimation because for $t < \tau_{RT}$ the driver has not made any obedience decision, and it takes time T for $\hat{\boldsymbol{\beta}}_j$ to output a value once the driver has decided. This is accounted for by the structure of $\hat{R}$. Define the map $\mathcal{F}(\hat{x}([t-T, t]) := \frac{\hat{v}_j(t) - \hat{v}_j(t-T)}{T}$ for $t \geq T$, the domain of which is restricted by the maps:

$$\Delta_1(\hat{q}) := \begin{cases} [d_{max} - \epsilon, d_{max}] & \text{if } \hat{q} \in \{\{oo, do, od, dd\}^1, \{od, dd\}^1, \{oa, da\}^1\} \\ [d_{min}, d_{min} + \epsilon] & \text{if } \hat{q} \in \{\{oo, do, od, dd\}^2, \{od, dd\}^2, \{oa, da\}^2\} \\ \text{anything} & \text{otherwise.} \end{cases}$$

$$\Delta_2(\hat{q}) := \begin{cases} [d_{min}, d_{min} + \epsilon] & \text{if } \hat{q} \in \{\{oo, do, od, dd\}^1, \{do, dd\}^1, \{ao, ad\}^1\} \\ [d_{max} - \epsilon, d_{max}] & \text{if } \hat{q} \in \{\{oo, do, od, dd\}^2, \{do, dd\}^2, \{ao, ad\}^2\} \\ \text{anything} & \text{otherwise.} \end{cases}$$

$\Delta_j(\hat{q})$ is defined as a small range about the specified warning acceleration for two reasons. The first is that as the time parameter T approaches 0, Δ_j restricts α_j directly because $\hat{\beta}(t)$ approaches $\alpha_j(t)$. This corresponds to having an "instant" estimator, and the range of Δ_j ensures that the disturbance is producing an acceleration α_j close

to the acceleration specified by the warning. The second reason is to ensure that the estimator has no "false negatives" in which it incorrectly estimates that a driver has disobeyed.

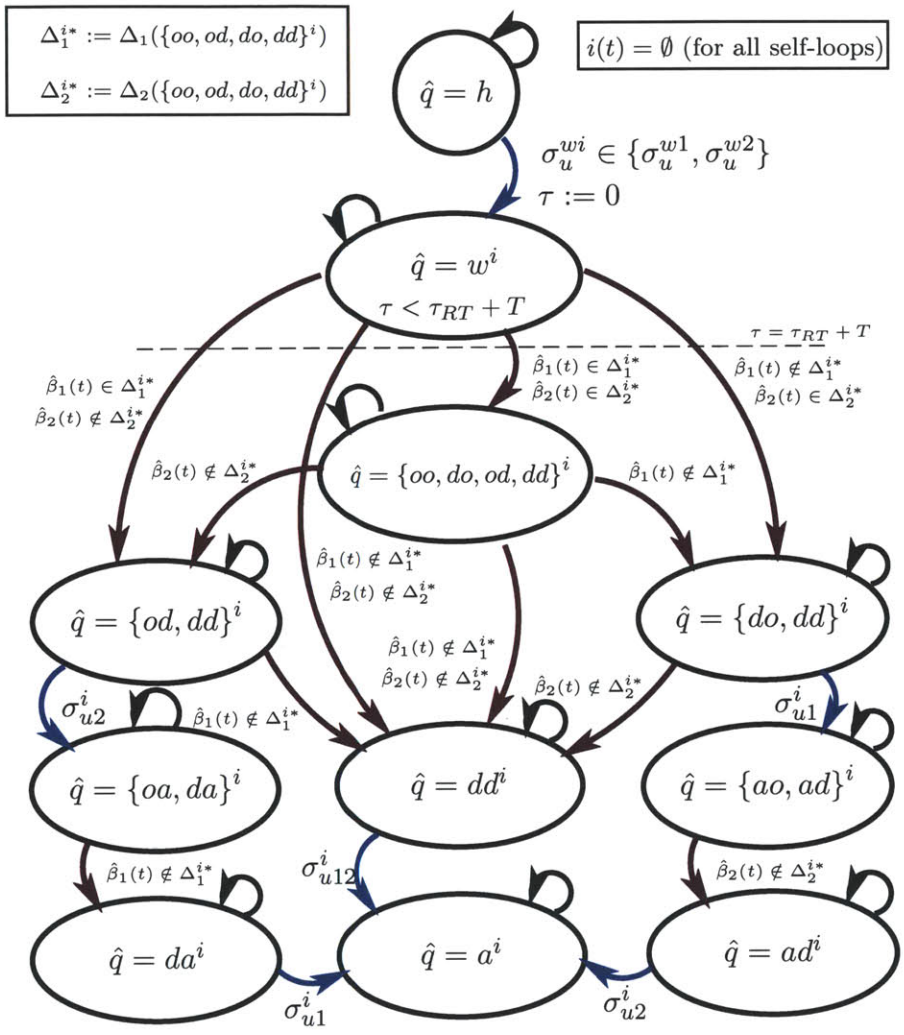


Figure 3-2: Automaton representation of system $\hat{H}$ for Case 2.

Figure 3-2 provides a visual representation of the discrete update map, $\hat{R}(\tau, \hat{q}, \sigma_u, \hat{i})$. Each mode estimate is represented by a circle and the transitions between modes are represented by blue and red arrows. The blue arrows are control events, while the red arrows are estimator observance events. The system is initialized with $\hat{q} = h$ and progresses through the other modes as necessary. The two sides have been condensed in the interest of legibility. Warning 1 corresponds to telling driver 1 to accelerate and driver 2 to brake, while warning 2 corresponds to telling driver 1 to brake and

driver 2 to accelerate. There are actually four different possible warnings, based on the combinations of the brake and accelerate for each car, but the pairs (gas, gas) and (brake, brake) are never used because they never end up being the optimal choice.

Define three maps $\hat{\mu} : \hat{Q} \to \mathbb{R}$ and $\hat{\gamma} : \hat{Q} \to \mathbb{R}^2$, with $\hat{\gamma} = (\hat{\gamma}_d, \hat{\gamma}_u)$. The value of these maps modulates the effect of d and u in the system dynamics.

$$\hat{\mu}_1(\hat{q}) := \begin{cases} \frac{u_{min}+d_{min}}{2} & \text{if } \hat{q} \in \{\{ao, ad\}^2, ad^2, a^2\} \\ \frac{u_{max}+d_{max}}{2} & \text{if } \hat{q} \in \{\{ao, ad\}^1, ad^1, a^1\} \\ \frac{d_{max}+d_{min}}{2} & \text{otherwise.} \end{cases}$$

$$\hat{\mu}_2(\hat{q}) := \begin{cases} \frac{u_{min}+d_{min}}{2} & \text{if } \hat{q} \in \{\{oa, da\}^1, da^1, a^1\} \\ \frac{u_{max}+d_{max}}{2} & \text{if } \hat{q} \in \{\{oa, da\}^2, da^2, a^2\} \\ \frac{d_{max}+d_{min}}{2} & \text{otherwise.} \end{cases}$$

$$\hat{\gamma}_{d1}(\hat{q}) := \begin{cases} 0 & \text{if } \hat{q} =\in \{\{ao, ad\}^1, \{ao, ad\}^2, ad^1, ad^2, a^1, a^2\} \\ \frac{d_{max}-d_{min}}{2\bar{d}} & \text{otherwise.} \end{cases}$$

$$\hat{\gamma}_{d2}(\hat{q}) := \begin{cases} 0 & \text{if } \hat{q} =\in \{\{oa, da\}^1, \{oa, da\}^2, da^1, da^2, a^1, a^2\} \\ \frac{d_{max}-d_{min}}{2\bar{d}} & \text{otherwise.} \end{cases}$$

$$\hat{\gamma}_{u1}(\hat{q}) := \begin{cases} |\frac{u_{min}-d_{min}}{2\bar{u}}| & \text{if } \hat{q} \in \{\{ao, ad\}^2, ad^2, a^2\} \\ |\frac{u_{max}-d_{max}}{2\bar{u}}| & \text{if } \hat{q} \in \{\{ao, ad\}^1, ad^1, a^1\} \\ 0 & \text{otherwise.} \end{cases}$$

$$\hat{\gamma}_{u2}(\hat{q}) := \begin{cases} |\frac{u_{min}-d_{min}}{2\bar{u}}| & \text{if } \hat{q} \in \{\{oa, da\}^1, da^1, a^1\} \\ |\frac{u_{max}-d_{max}}{2\bar{u}}| & \text{if } \hat{q} \in \{\{oa, da\}^2, da^2, a^2\} \\ 0 & \text{otherwise.} \end{cases}$$

Define $\hat{\alpha}_1 := \hat{\mu}_1(\hat{q}) + \hat{\gamma}_{d1}(\hat{q})d_1 + \hat{\gamma}_{u1}(\hat{q})u_1$ and $\hat{\alpha}_2 := \hat{\mu}_2(\hat{q}) + \hat{\gamma}_{d2}(\hat{q})d_2 + \hat{\gamma}_{u2}(\hat{q})u_2$. Define $\dot{\tau} := 0$ if $\hat{q} = h$ and $\dot{\tau} := 1$ otherwise. Then $\hat{f} = (\hat{f}_1, \hat{f}_2)$ with $\hat{f}_i(\hat{x}_i, \hat{q}, u, d_i) := (v_i, \alpha_i, \dot{\tau})^T$ if $\hat{v}_i \in (v_{i_{min}}, v_{i_{max}}) \vee (\hat{v}_i = v_{i_{max}} \wedge \hat{\alpha}_i \leq 0) \vee (\hat{v}_i = v_{i_{min}} \wedge \hat{\alpha}_i \geq 0)$ and

$\hat{f}_i(\hat{x}_i, \hat{q}, u, d_i) := (v_i, 0, \dot{\tau})^T$ otherwise.

By construction, $\hat{f}_i(\hat{x}_i, \hat{q}, u, D_i) = \cup_{q \in \hat{q}} f_i(\hat{x}_i, q, u, D_i)$. That is, the set of vector fields $\hat{f}_i$ provides the union of all of the possible vehicle dynamics for vehicle i based on the current mode estimate. The safety control problem for $\hat{H}$ is as defined, in Problem 1, with the bad set defined as both vehicles simultaneously occupying the intersection and with the initial mode $\hat{q} = h$. As shown in Theorem 1, these two problems are equivalent to the safety control problems for system H if $\hat{H}$ is an exact estimator. It is possible to show that $\hat{H}$ is an exact estimator and it follows by its construction.

3.2 Determining the Maximal and Minimal Signals

In order to efficiently calculate the unsafe region of the state space, it will be necessary to calculated the maximal and minimal control and disturbance signals for each mode estimate. These signals maximize or minimize the displacement of a given vehicle for a given set of initial conditions. Such signals are necessary in order to apply the results of [12] and [7]. These results hold for order preserving systems, that is, systems in which the flow preserves the ordering (usually component-wise) with respect to the initial conditions and input (disturbance and control) signals.

The longitudinal dynamics of the vehicles considered in this paper are order preserving, in which ordering in the state space is taken component-wise [11]. That is, $x^a \leq x^b$ if $p_i^a \leq p_i^b$ and $v_i^a \leq v_i^b$. Furthermore, let $p_i^a(t)$ and $p_i^b(t)$ denote the displacement of vehicle i corresponding to input signals $\mathbf{u_i^a}$, $\mathbf{d_i^a}$ and $\mathbf{u_i^b}$, $\mathbf{d_i^b}$, respectively. Let $\mathbf{d_i^a} = \mathbf{d_i^b}$, then we say that $\mathbf{u_i^a} \leq \mathbf{u_i^b}$ if $p_i^a(t) \leq p_i^b(t)$ for all $t \geq 0$. Similarly, let $\mathbf{u_i^a} = \mathbf{u_i^b}$, then we say that $\mathbf{d_i^a} \leq \mathbf{d_i^b}$ if $p_i^a(t) \leq p_i^b(t)$ for all $t \geq 0$. Basically, partial ordering on the set of input signals is defined based on displacements. The maximal input signals are those that maximize the displacement, while the minimal input signals are those that minimize the displacement, fixed the initial conditions. If

the input signals are allowed to take constant maximal and minimal values, we have that $\mathbf{u} \equiv \bar{u}$ and $\mathbf{d} \equiv \bar{d}$ will be the maximal signals, while $\mathbf{u} \equiv -\bar{u}$ and $\mathbf{d} \equiv -\bar{d}$ will be the minimal signals.

When the disturbance input d is restricted by $\mathcal{F}$, determining the maximal and minimal signals is no longer trivial. The disturbance ranges in $[-\bar{d}, \bar{d}]$, but it must be compatible with $\mathcal{F}(\hat{x}([t-T,t])) \in \Delta(\{ho, hd\}^i)$ for all $t \geq T$. In order to determine the maximal and minimal disturbance profiles compatible with this restriction, we solve the optimization problems:

$$\max_d \left(\int_0^t \int_0^\sigma \alpha_2(\tau) d\tau d\sigma \right), t \geq T, \text{ and} \tag{3.1}$$

$$\min_d \left(\int_0^t \int_0^\sigma \alpha_2(\tau) d\tau d\sigma \right), t \geq T, \text{ with} \tag{3.2}$$

$$\int_{\tau-T}^{\tau} \alpha_2(\sigma) d\sigma \in \Delta(\{ho, hd\}^i) \text{ for all } T \leq \tau \leq t.$$

For $\Delta(\{ho, hd\}^1)$, (3.2) is trivial, with solution $\mathbf{d} \equiv -\bar{d}$, but (3.1) is non-trivial. For $\Delta(\{ho, hd\}^2)$ (3.1) is trivial, with solution $\mathbf{d} \equiv \bar{d}$, but (3.2) is non-trivial. Let $\delta = \frac{\epsilon T}{d_{max} - d_{min}}$ and let $n \in \{0, 1, 2, 3...\}$. The solution to the maximization problem for $\Delta(\{ho, hd\}^1)$, is a "bang-bang" solution, with the optimal disturbance input for $t \in [nT, (n+1)T)$ given by $d_M(t) = \begin{cases} -\bar{d} & t - nT \leq \delta \\ \bar{d} & t - nT > \delta \end{cases}$. The solution to the minimization problem for $\Delta(\{ho, hd\}^2)$ is the opposite of the previous solution, for all time $t > 0$, that is, $d_m(t) = -d_M(t)$. Intuitively, δ is the maximum length of time the disturbance can remain outside of $\Delta(\{ho, hd\}^2)$ with enough time to bring the average acceleration back into the $\Delta(\{ho, hd\}^2)$ at time T. While the optimization was shown for case 1, the structure of Δ_1 and Δ_2 is such that the solution may be applied to case 2 as well.

Figure 3-3 shows the result of minimization of the disturbance signal. The green shows the nominal "obey" signal, while the red is the minimized signal. The displacement plot shows that the resultant displacement of the minimized signal remains

behind the nominal signal for all time.

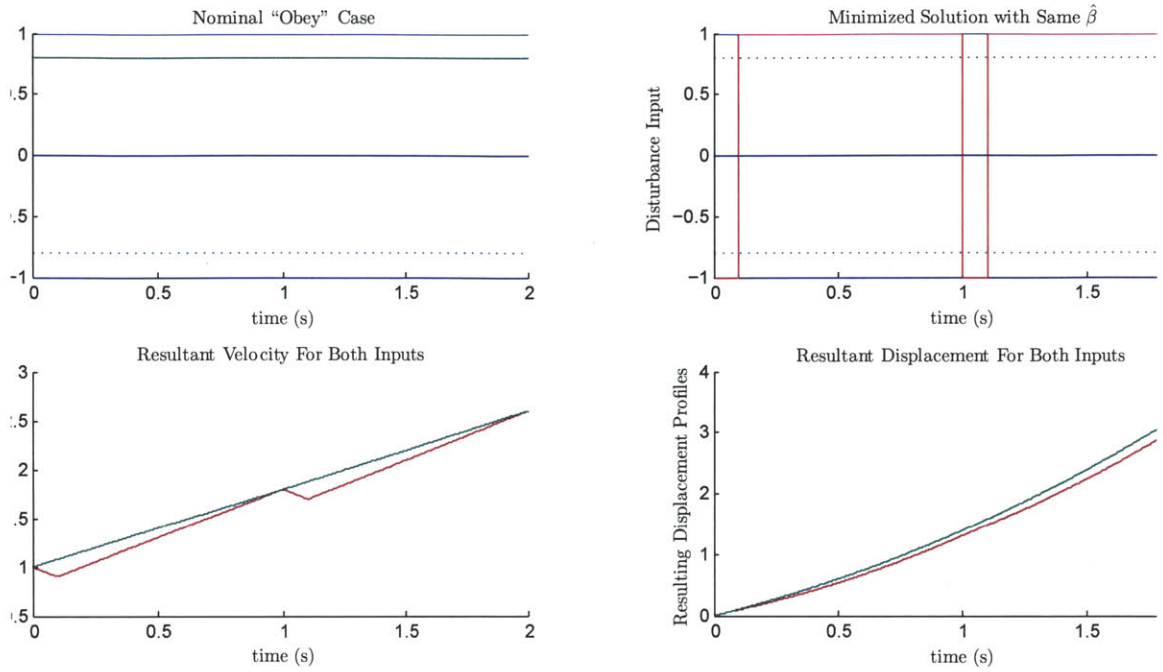


Figure 3-3: Minimized disturbance signal compared with a nominal signal. The minimized signal produces a displacement which is always behind the nominal signal.

3.3 Uncontrollable Predecessor Operator and Mode Dependent Capture Set

Two tools that will be useful for solving the proposed control problems called the uncontrollable predecessor operator and the mode dependent capture set, will be defined here. They provide convenient notation for expressing the various sets that will be utilized to solve those problems.

Definition 4. For a set $P \subseteq X$, modes $\hat{q}_i, \hat{q}_j$, and time $\tau_M > T$, we define the *uncontrollable predecessor operator*:

$$Pre(\hat{q}_i,\hat{q}_j, \tau_M, P) := \tag{3.3}$$
$$\{\hat{x}_o | \forall \hat{\pi}\ \exists\ \mathbf{d},\ t \leq \tau_M \text{ with } \mathcal{F}(\hat{x}([t-T,t])) \in \Delta(\hat{q}_j) \text{ s.t. } \phi_{\hat{x}}^{\hat{\pi}}(t, \hat{x}_o, \hat{q}_i, \mathbf{d}, \emptyset) \in P\}.$$

If no τ_M is specified, it is assumed to be equal to ∞. If no $\hat{q}_j$ is specified, there is no additional restriction on $\mathcal{F}$. Also, $\tau_M > T$. The Pre operator provides a compact way to represent the set of all points for which no control will prevent the flow from entering a given set P before τ_M under the restricted dynamics allowing for a future transition to q_j.

Definition 5. A *mode dependent capture set* for mode $\hat{q}_o \in \hat{Q}$ is defined:

$$C(\hat{q}_o) := \{\hat{x}_o | \forall \hat{\pi} \; \exists \hat{\boldsymbol{i}}, \; \mathbf{d}, \; t \text{ s.t. } \phi_{\hat{x}}^{\hat{\pi}}(t, \hat{x}_o, \hat{q}_o, \mathbf{d}, \hat{\boldsymbol{i}}) \in B\}. \tag{3.4}$$

This general definition will be applied to each mode within the hybrid estimator system, the results of which will be analyzed to determine the solution to the proposed safety control problems.

Chapter 4

Solution to Safety Control Problems for Case 1

In this chapter, I utilize the estimator system for Case 1 to solve the modified safety control problems 1' and 2'.

4.0.1 Solution of Problem 1'

Problem 1' will be solved by constructing a mode dependent capture set, $C(\hat{q})$ as defined in Definition 5 for each mode $\hat{q} \in Q$. By definition, this capture set will be the solution to Problem 1' when $\hat{q}_o = h$, but the solution relies on being able to calculate this set. To do so, $C(h)$ will be constructed iteratively, starting with $\hat{q} \in \{ha^1, ha^2\}$ and working backwards towards $\hat{q}_o = h$. As seen in the following theorem, this technique is possible because there are no loops in $\hat{R}$.

Theorem 2. *Let $i \in \{1,2\}$. Then $\hat{S} = C(h)$ where:*

(i) $C(h) = C(w^1) \cap C(w^2)$

(ii) $C(w^i) = Pre(w^i, \{ho, hd\}^i, T^*, C(\{ho, hd\}^i)) \cup Pre(w^i, hd^i, T^*, C(ha^i))$

(iii) $C(\{ho, hd\}^i) = Pre(\{ho, hd\}^i, C(ha^i))$

(iv) $C(ha^i) = Pre(ha^i, B)$.

Proof. First, apply (3.4) for $\hat{q}_o = ha^i$, producing $C(ha^i) = \{\hat{x}_o | \forall \hat{\pi}. \exists \hat{\boldsymbol{i}}, \mathbf{d}, t.$ s.t. $\phi_{\hat{x}}^{\hat{\pi}}(t, x_o, ha^i, \mathbf{d}, \hat{\boldsymbol{i}}) \in B\}$. Because there are no discrete mode transitions from $\hat{q} = ha^i$, this can be written $C(ha^i) = Pre(ha^i, B)$.

Next, apply (3.4) for $\hat{q}_o = hd^i$, producing $C(hd^i) = \{\hat{x}_o | \forall \hat{\pi}. \exists \hat{\boldsymbol{i}}, \mathbf{d}, t.$ s.t. $\phi_{\hat{x}}^{\hat{\pi}}(t, x_o, hd^i, \mathbf{d}, \hat{\boldsymbol{i}}) \in B\}$. Because the control event σ_u^i is allowable when $\hat{q} = hd^i$, and $\hat{R}(\tau, hd^i, \sigma_u^i, \hat{i}) = ha^i$, we can write this as $C(hd^i) = \{\hat{x}_o | \forall \hat{\pi}. \exists \hat{\boldsymbol{i}}, \mathbf{d}, t.$ s.t. $\phi_{\hat{x}}^{\hat{\pi}}(t, x_o, ha^i, \mathbf{d}, \hat{\boldsymbol{i}}) \in B\} = C(ha^i)$.

Now, apply (3.4) for $\hat{q}_o = \{ho, hd\}^i$, producing $C(\{ho, hd\}^i) = \{\hat{x}_o | \forall \hat{\pi}. \exists \hat{\boldsymbol{i}}, \mathbf{d}, t.$ s.t. $\phi_{\hat{x}}^{\hat{\pi}}(t, x_o, \{ho, hd\}^i, \mathbf{d}, \hat{\boldsymbol{i}}) \in B\}$. From the definition of $\hat{R}(\tau, \{ho, hd\}^1, \sigma_u, \hat{i})$, one can enter B either by flowing directly into it or by first switching modes and then flowing into it. Hence while $\hat{q} = \{ho, hd\}^i$, it is necessary to remain outside of $C(ha^i) \cup B$. Because $C(ha^i) \supset B$, we can write $C(\{ho, hd\}^i) = Pre(\{ho, hd\}^i, C(ha^i))$.

Moving backwards to $\hat{q} = w^i$ and applying (3.4) again produces $C(w^i) =: \{\hat{x}_o | \forall \hat{\pi}. \exists \hat{\boldsymbol{i}}, \mathbf{d}, t.$ s.t. $\phi_{\hat{x}}^{\hat{\pi}}(t, x_o, w^i, \mathbf{d}, \hat{\boldsymbol{i}}) \in B\}$. Writing $C(w^i)$ using the Pre operator requires the use of the τ_M argument because the mode estimate necessarily transitions to either $\hat{q} = \{ho, hd\}^i$ or $\hat{q} = hd^i$ at $\tau = \tau_{RT} + T$ based on the value of $\hat{i}$. From the definition of $\hat{R}(\tau, w^1, \sigma_u, \hat{i})$, one can enter B either by flowing directly into it or by switching modes before flowing into it. Hence, while $\mathcal{F}(\hat{x}([\tau_{RT}, \tau_{RT} + T]) \in \Delta(\{ho, hd\}^i)$, it is necessary to remain outside of $C(\{ho, hd\}^i) \cup B = C(\{ho, hd\}^i)$. If instead the dynamics are restricted by $\mathcal{F}(\hat{x}([\tau_{RT}, \tau_{RT} + T]) \notin \Delta(\{ho, hd\}^i)$, it is necessary to remain outside of $C(ha^i) \cup B = C(ha^i)$. It is important to note that there are no restrictions on $\mathcal{F}$ during $\tau \in [0, \tau_{RT})$.

Using these requirements, $C(w^i)$ can be written $C(w^i) = Pre(w^i, \{ho, hd\}^i, \tau_{RT} + T, C(\{ho, hd\}^i)) \cup Pre(w^i, hd^i, \tau_{RT} + T, C(hd^i) = C(ha^i))$. We can then step back to the initial mode $\hat{q} = h$ and apply (3.4) to produce $C(h) = \{\hat{x}_o | \forall \hat{\pi}. \exists \hat{\boldsymbol{i}}, \mathbf{d}, t.$ s.t. $\phi_{\hat{x}}^{\hat{\pi}}(t, x_o, \hat{q}_o = h, \mathbf{d}, \hat{\boldsymbol{i}}) \in B\}$. From $\hat{R}$, there are two allowable control events $\sigma_u \in \{\sigma_u^{w1}, \sigma_u^{w2}\}$ when $\hat{q} = h$ and they lead to unconnected branches of the automaton. The flow could enter B either directly, or by executing one of these transitions first. Hence, while $\hat{q} = h$, it is necessary to avoid $(C(w^1) \cap C(w^2)) \cup B = C(w^1) \cap C(w^2)$. Using this, we can write $C(h) = C(w^1) \cap C(w^2)$.

□

4.0.2 Computational Tools

Theorem 4 provides an iterative formulation for $\hat{S}$, and for the mode dependent capture sets, $C(\hat{q})$, but each set is still expressed as the uncontrollable predecessor of other capture sets, which makes it difficult to calculate them. In order to make their computation efficient, we can express them as the uncontrollable predecessor of B under restricted disturbance signals. This will allow each capture set to be calculated as a back integration of the much simpler set, B.

Proposition 1. $C(\{ho, hd\}^i) = Pre(\{ho, hd\}^i, B)$.

Proof. We first show $C(\{ho, hd\}^1) \subseteq Pre(q = \{ho, hd\}^1, B)$. Let $\hat{x} \in C(\{ho, hd\}^1)$. Then, from Theorem 1(iv), this is true if and only if $\hat{x} \in Pre(\{ho, hd\}^1, C(ha^1))$. From Theorem 1(v) this is true if and only if $\hat{x} \in Pre(\{ho, hd\}^1, Pre(ha^1, B))$. Let $A_1 := \{\hat{x}_o | \exists \hat{i}, \mathbf{d}.$ with $\mathbf{u} \equiv -\bar{\mathbf{u}},$ s.t. $\phi^{\hat{\pi}}_{\hat{x}}(t, \hat{x}_o, ha^1, \mathbf{d}, \emptyset) \in S\}$. Then $\hat{x} \in A_1$ because the control input is restricted. This implies $\hat{x} \in Pre(\{ho, hd\}^1, Pre(\{ho, hd\}^1, B))$ because $\exists \mathbf{d_2}$ s.t. $\mathcal{F} = d_{min}$. This is true if and only if $\hat{x} \in Pre(\{ho, hd\}^1, B)$ by the definition of Pre.

We show $C(\{ho, hd\}^2) \subseteq Pre(q = \{ho, hd\}^2, B)$. Let $\hat{x} \in C(\{ho, hd\}^2)$. Then, from Theorem 1(iv), this is true if and only if $\hat{x} \in Pre(\{ho, hd\}^2, C(ha^2))$. From Theorem 1(v) this is true if and only if $\hat{x} \in Pre(\{ho, hd\}^2, Pre(ha^2, B))$. Let $A_2 := \{\hat{x}_o | \exists \hat{i}, \mathbf{d}.$ with $\mathbf{u} \equiv \bar{\mathbf{u}},$ s.t. $\phi^{\hat{\pi}}_{\hat{x}}(t, \hat{x}_o, ha^2, \mathbf{d}, \emptyset) \in S\}$. Then $\hat{x} \in A_2$ because the control input is restricted. This implies $\hat{x} \in Pre(\{ho, hd\}^2, Pre(\{ho, hd\}^2, B))$ because $\exists \mathbf{d_2}$ s.t. $\mathcal{F} = d_{max}$. This is true if and only if $\hat{x} \in Pre(\{ho, hd\}^2, B)$ by the definition of Pre.

We show, $Pre(\{ho, hd\}^i, B) \subseteq C(\{ho, hd\}^i)$. Let $\hat{x} \in Pre(\{ho, hd\}^i, B)$. Then, $\hat{x} \in Pre(\{ho, hd\}^i, C(ha^1))$ because $C(ha^i) \supset B$. From Theorem 4(iii), this is true if and only if $\hat{x} \in C(\{ho, hd\}^i)$. □

Proposition 2.
$Pre(w^i, \{ho, hd\}^i, T^*, C(\{ho, hd\}^i)) = Pre(w^i, \{ho, hd\}^i, T^*, Pre(\{ho, hd\}^i, B))$.

Proof. Follows directly from Proposition 1. □

Proposition 3. $Pre(w^i, hd^i, T^*, C(ha^i)) = Pre(w^i, hd^i, T^*, Pre(ha^i, B))$.

Proof. Follows directly from Theorem 4(iv). □

Propositions 1, 2, and 3 are useful because they allow for application of the results of [12] and [7] to efficiently calculate the capture sets. In order to do this we will utilize the maximal and minimal control signals determined in Section 3.2, to back propagate the bad set for each mode dependent capture set.

To compute $C(ha^i)$, we first examine the input for vehicle 2 because it is assumed that the "control plays first" such that the disturbance will have chance to base its choice on that decision. The control input ranges in $[-\bar{u}, \bar{u}]$, and to maximize the displacement, the controller simply applies the maximum input $u(t) = \bar{u}$ for all t. To minimize the displacement, the controller applies the minimum input $u(t) = -\bar{u}$ for all t. We can then write, according to [12], [7],

$$C(ha^i) = C(ha^i)^H \cap C(ha^i)^L \tag{4.1}$$

with $C(ha^i)^H = \{\hat{x}_o | \exists \mathbf{d}, t \text{ s.t. } \phi_{\hat{x}}(t, \hat{x}_o, ha^i, \bar{u}, \mathbf{d}, \emptyset, \emptyset) \in B\}$, and $C(ha^i)^L = \{\hat{x}_o | \exists \mathbf{d}, t \text{ s.t. } \phi_{\hat{x}}(t, \hat{x}_o, ha^i, -\bar{u}, \mathbf{d}, \emptyset, \emptyset) \in B\}$. Since the input is fixed, these sets can be computed by plain back integration of the set B when the disturbance ranges in its full range $[-\bar{d}, \bar{d}]$. Since the dynamics are order preserving, this back integration can be achieved by back integrating the lower bound of B, (L_1, L_2), through the minimal disturbance $\mathbf{d} \equiv -\bar{d}$ and the upper bound of B, $U_1, U_2)$, through the maximal disturbance $\mathbf{d} \equiv \bar{d}$ [12]. In this way, the worst case in which the disturbance plays against the control input is always accounted for.

As an example of these inputs, Figure 4-1 shows a plot of the disturbance signal used to back propagate the (L_1, U_2) corner of B for $C(ha^2)^H$ and the resulting set boundary. The control input for vehicle 2 is fixed to $\bar{u}$ producing $\alpha_2 \equiv u_{max}$, while

the disturbance input for vehicle 1 is fixed to $d(t) = \bar{d}$ producing $\alpha_1 \equiv d_{max}$. The back propagation is started with the current velocity of the vehicles, and eventually saturates, which is clear from the fact that the boundary straightens out after the initial curvature.

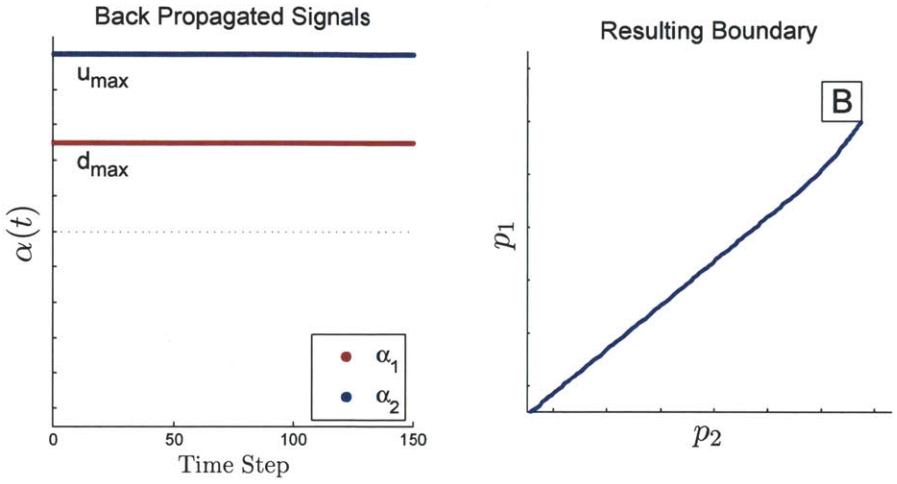


Figure 4-1: Accelerations used to back propagate the lower bound of the bad set for $C(ha^2)^H$ and the resulting curve.

By the definition of the restricted capture sets $C(ha^i)^H$ and $C(ha^i)^L$, if the restricted control input used in their definition is applied to the system when the state is outside of either set, the state will remain outside of that set.

$C(\{ho, hd\}^i)$, given Proposition 1, can be calculated similarly, but now the restrictions on $\mathcal{F}$ must be taken into account. Since there is no control input applied in the definition of $Pre(\{ho, hd\}^i, B)$, this set can be obtained by backward integration of B through all possible disturbances compatible with $\mathcal{F} \in \Delta\{ho, hd\}^i$. By virtue of the order preserving dynamics, this backward integration can be accomplished by simply back integrating the lower bound of B through the maximal disturbance d_M and the upper bound of B through the minimal disturbance d_m, as calculated in Section 3.2.

As an example of these inputs, Figure 4-2 shows a plot of the signals used to back propagate the (L_1, U_2) corner of B for $C(\{ho, hd\}^2)$ and the resulting set boundary. The disturbance input for vehicle 2 is utilizes the optimized disturbance signal $d(t) = d_M$, producing $\alpha_2(t)$ which switches between d_{min} and d_{max}, while the disturbance input for vehicle 1 is fixed to $\bar{d}$ producing $\alpha_2 \equiv d_{max}$. The back propagation is started

with the current velocity of the vehicles, and eventually saturates, which is clear from the fact that the boundary straightens out after the initial curvature. This saturation takes longer due to the fact that the acceleration of vehicle 2 is slower.

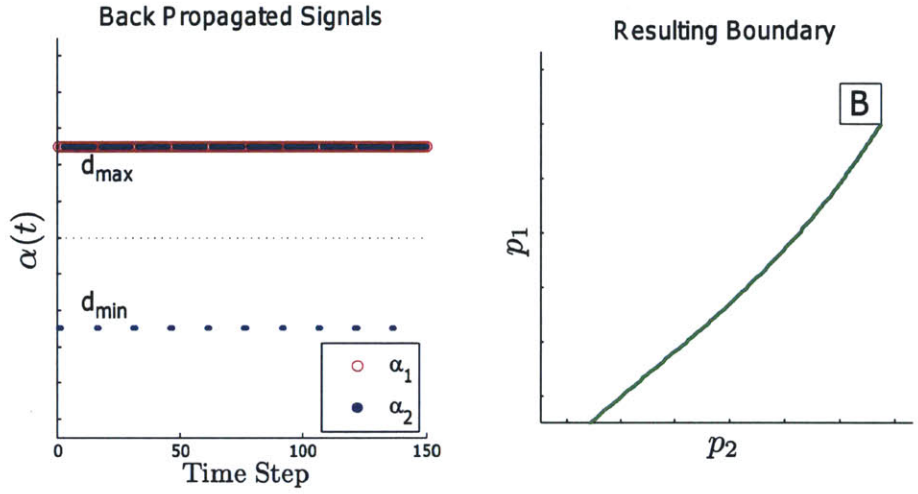


Figure 4-2: Accelerations used to back propagate the lower bound of the bad set for $C(\{ho, hd\}^2)$ and the resulting curve.

$C(w^i)$, given Theorem 4, Proposition 2, and Proposition 3, can be computed similarly by finding the maximal and minimal disturbance profiles. Specifically, we first compute $Pre(w^i, \{ho, hd\}^i, \tau_{RT} + T, Pre(\{ho, hd\}^i, B))$, by breaking up its definition into two time intervals: $t < \tau_{RT}$ and $t \geq \tau_{RT}$. During the first time interval, there are no restrictions on the disturbance signal. For the second time interval the disturbance signal follows the same restrictions as when $\hat{q} = \{ho, hd\}^1$ and therefore we can use d_M and d_m as the maximal and minimal disturbances. To compute $Pre(w^i, hd^i, \tau_{RT} + T, Pre(ha^i, B))$ we write it using the restricted capture sets from (5.1) as $Pre(w^i, hd^i, \tau_{RT} + T, C(ha^i)^L \cap C(ha^i)^H)$, and again split it into two time intervals. For $t < T^*$, there are no restrictions on the disturbance input. For $t \geq T^*$, we calculate a set $C(w^i)^H$, with $u(t) = \bar{u}$ and $C(w^i)^L$ with $u(t) = -\bar{u}$. Using the order preserving properties of the system, $C(w^i) = C(w^i)^L \cap C(w^i)^H$ using again the results of [7, 11, 12]. As shown in Theorem 4, all of the mode dependent capture sets can be expressed as combinations of $C(ha)^i, C(\{ho, hd\}^1)$, and $C(w^i)$, and as a consequence, it is possible to efficiently calculate all of the mode dependent capture sets.

As an example of the inputs used to calculate $C(w^i)$, Figure 4-3 shows a plot of the disturbance signal used to back propagate the (L_1, U_2) corner of B for $Pre(w^2, hd^2, \tau_{RT}+T, C(ha^2)^H)$ and the resulting set boundary. For the first $\frac{T^*}{\Delta t}$ timesteps, the disturbance input for vehicle 2 is fixed to $-\bar{d}$ producing $\alpha_2 \equiv d_{min}$, and for the remainder of the time steps, a control input of $\bar{u}$ is applied. The disturbance input for vehicle 1 is again fixed to $d_2(t) = \bar{d}$ producing $\alpha_1 \equiv d_{max}$. The reaction time and estimator time delays are apparent from fact that the curvature of the boundary is initially in one direction before switching. The vehicle 1 signal used for calculating $Pre(w^i, \{ho, hd\}^2, \tau_{RT}+T, Pre(\{ho, hd\}^2, B))$ is similar to the α_2 signal shown in Figure 4-3, with the disturbance $d_2(t) = -\bar{d}$ for $t < \tau_{RT}$ before switching to $d_2(t) = d_M$ for $t \geq \tau_{RT}$.

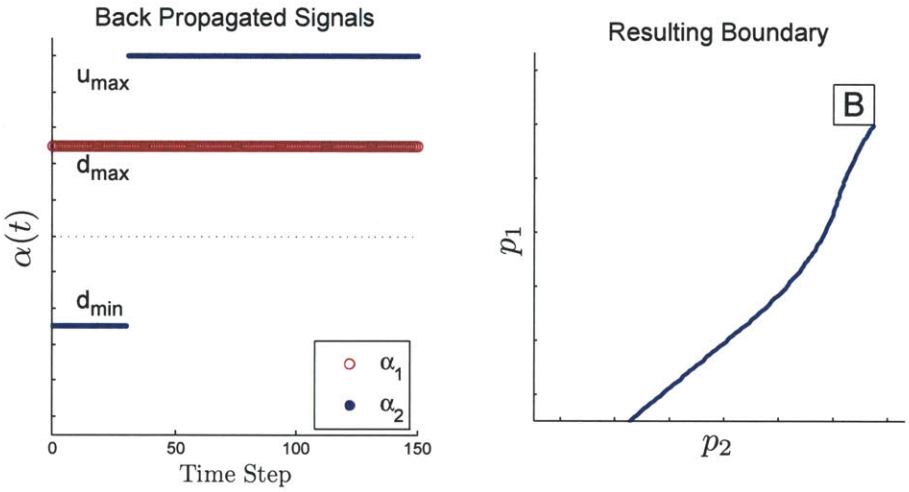


Figure 4-3: Accelerations used to back propagate the lower bound of the bad set for $Pre(w^2, hd^2, \tau_{RT} + T, C(ha^2)^H)$ and the resulting curve.

4.0.3 Solution to Problem 2'

Problem 2' is solved by constructing a control map, $\hat{\pi}(\hat{q}, \hat{x})$, using the known properties of the mode dependent capture set $C(\hat{q})$. For a set S, let ∂S denote the boundary of S. Using the known properties of the mode dependent capture set, $C(\hat{q})$, we con-

struct $\hat{\pi}$ as follows:

$$\hat{\pi}(\hat{q},\hat{x}) = \begin{cases} u = \begin{cases} -\bar{u} & \text{if } q \in \{ha^i\} \wedge x \in C(\hat{q})^H \cap \partial C(\hat{q})^L \\ \bar{u} & \text{if } q \in \{ha^i\} \wedge x \in C(\hat{q})^L \cap \partial C(\hat{q})^H \\ (\emptyset,\emptyset) & \text{else} \end{cases} \\ \sigma_u = \begin{cases} \sigma_u^1 & \text{if } \hat{q} = hd^1 \cap \partial C(ha^1) \\ \sigma_u^2 & \text{if } \hat{q} = hd^2 \cap \partial C(ha^2) \\ \sigma_u^{w1} & \text{if } \hat{q} = h \wedge x \in C(w^2) \wedge x \in \partial C(w^1) \\ \sigma_u^{w2} & \text{if } \hat{q} = h \wedge x \in C(w^1) \wedge x \in \partial C(w^2) \\ \emptyset & \text{else.} \end{cases} \end{cases}$$

This map checks the membership of the current state with respect to the mode dependent capture set $C(\hat{q})$, and uses this information to determine if control event or continuous control is required to maintain safety. It utilizes the decomposition of the capture sets into restricted capture sets in order to determine what the specified control action should be. In order for $\hat{\pi}(\hat{q},\hat{x})$ to be safe, two conditions must hold for all $\hat{q} \in \hat{Q}$. First, while in any mode $\hat{q}_i$, the flow must not enter the bad set. Second, no discrete transition from mode $\hat{q}_i$ to mode $\hat{q}_j$ can cause the continuous flow to enter the mode dependent capture set $C(\hat{q}_j)$ after the transition. Let $\tau_{\hat{q}_i}$ denote the transition time *to* the mode estimate $\hat{q} = \hat{q}_i$, and $\tau'_{\hat{q}_i}$ denote the transition time *from* that estimate. *Condition 1:* $\hat{x}(\tau_{\hat{q}_i}) \notin C\hat{q}_i \Rightarrow \forall \mathbf{d}, t \in [\tau_{q_i}, \tau'_{q_i}).\ \phi_{\hat{x}}^{\hat{\pi}}(t, \hat{x}(\tau_{\hat{q}_i}), \hat{q}_i, \mathbf{d}, \emptyset) \notin B$. *Condition 2:* $\hat{x}(\tau_{\hat{q}_i}) \notin C\hat{q}_i \Rightarrow \forall \hat{q}_j \in \cup_{\hat{i} \in I} \hat{R}(\tau, \hat{q}_i, \sigma_u, \hat{i}).\ x(\tau'_{q_i}) \notin C(\hat{q}_j)$.

Lemma 1. *Condition 1 holds for all* $\hat{q} \in \hat{Q}$.

Proof. (by cases): For $\hat{q} = h$, if $\sigma_u = \emptyset$, then $\hat{x} \notin \partial C(w^1) \cap C(w^2)$ by the definition of $\hat{\pi}$ and so $\hat{x} \notin B$. If $\sigma_u \in \{\sigma_u^{w1}, \sigma_u^{w2}\}$, for $t > \tau'_h q(t) \neq h$. Hence, $\forall t \in [\tau_h, \tau'_h)$, we have that $\phi_{\hat{x}}^{\hat{\pi}} \notin B$.

For $\hat{q} = w^i$, by the definition of $C(w^i), \hat{x}(\tau_{w^i}) \notin C(w^i) \Rightarrow \phi_{\hat{x}}^{\hat{\pi}}(\tau < \tau'_{w^i} = \tau_{w^i} + \tau_{RT} + T) \notin C(\{ho, hd\}^i) \cap C(ha^i)$. $C(\{ho, hd\}^i) \cap C(ha^i) \supset B$. Hence, $\forall t \in [\tau_{w^i}, \tau'_{w^i})$, we have that $\phi_{\hat{x}}^{\hat{\pi}} \notin B$.

For $\hat{q} = \{ho, hd\}^i$, there is no control while $\hat{q} = \{ho, hd\}^i$, so the definition

of $C(\{ho, hd\}^i)$ implies that $\hat{x}(\tau_{w^i}) \notin C(\{ho, hd\}^i) \Rightarrow \phi_{\hat{x}}^{\hat{\pi}} \notin C(ha^i)$. Hence, $\forall t \in [\tau_{\{ho,hd\}^i}, \tau'_{\{ho,hd\}^i})$, we have that $\phi_{\hat{x}}^{\hat{\pi}} \notin B$.

For $\hat{q} = hd^i$, if $\sigma_u = \emptyset$, then $\hat{x} \notin C(ha^i)$ by the definition of $\hat{\pi}$ and so $\hat{x} \notin B$. If $\sigma_u = \sigma_u^i$, for $t > \tau'_h q(t) \neq hd^i$. Hence, $\forall t \in [\tau_{hd^i}, \tau'_{hd^i})$, we have that $\phi_{\hat{x}}^{\hat{\pi}} \notin B$.

For $\hat{q} = ha^i$, as discussed in Section 5.0.6, the application of $u = -\bar{u}$ (for $\hat{q} = ha^1$) or $u = \bar{u}$ (for $\hat{q} = ha^2$) when $\hat{x} \in \partial C(ha^i)$ renders the relation $\hat{x} \notin C(ha^i)$ invariant. Hence, $\forall t \in [\tau_{ha^i}, \tau'_{ha^i})$, we have that $\phi_{\hat{x}}^{\hat{\pi}}(t) \notin B$.

□

Lemma 2. *Condition 2 holds for all $\hat{q} \in \hat{Q}$.*

Proof. (by cases): Let q_j be the mode being transitioned to. For $\hat{q}_i = h$ and $\hat{q}_j = w^i, \hat{R}(\tau, h, \sigma_u^{w1}, \hat{\beta}) = w^i$. By the definition of $\hat{\pi}$, $\sigma_u = \sigma_u^{w1}$ when $\hat{x}(\tau_{w^i}) \notin C(w^i)$. Hence, $\hat{x}(\tau'_h) \notin C(w^i)$. For $\hat{q}_i = w^i$ and $\hat{q}_j = \{ho, hd\}^i$, $\mathcal{F}(\hat{x}([\tau_{RT}, \tau_{RT} + T]) \in \Delta(\{ho, hd\}^i$. By the definition of $C(w^i), \hat{x}(\tau_{w^i}) \notin C(w^i)$ and $\mathcal{F}(x([\tau_{RT}, \tau_{RT} + T]) \in \Delta(\{ho, hd\}^i)$ implies $\hat{x}(\tau'_{w^i}) \notin C(\{ho, hd\}^i)$. Hence, $x(\tau'_{w^1}) \notin C(\{ho, hd\}^i)$. For $\hat{q}_i = w^i$ and $\hat{q}_j = hd^i$, the definition of $C(w^i)$ implies $\hat{x}(\tau_{w^i}) \notin C(w^i)$ and $\mathcal{F}(x([\tau_{RT}, \tau_{RT} + T]) \notin \Delta(\{ho, hd\}^i)$. This implies $\hat{x}(\tau'_{w^i}) \notin C(ha^i)$. Hence, $x(\tau'_{w^1}) \notin C(ha^i)$. For $\hat{q}_i = \{ho, hd\}^i$ and $\hat{q}_j = \{hd\}^i$, the definition of $C(\{ho, hd\}^i)$ implies $\hat{x}(\tau_{\{ho,hd\}^i}) \notin C(\{ho, hd\}^i)$ and $\hat{\beta}([\tau'_{\{ho,hd\}^i}, \tau'_{\{ho,hd\}^i})) \in \Delta(\{ho, hd\}^i)$ implies $\hat{x}(\tau'_{\{ho,hd\}^i}) \notin C(\{ho, hd\}^i)$. Hence, $\hat{x}(\tau'_{\{ho,hd\}^i}) \notin C(ha^i)$. For $\hat{q}_i = hd^i$ and $\hat{q}_j = ha^i$, the definition of $\hat{\pi}$ implies $\sigma_u = \sigma_u^1$ when $x \notin C(ha^i)$. Hence, $\hat{x}(\tau'_{hd}) \notin C(ha^i)$. For $\hat{q}_i = ha^1$, $\hat{i}(t) = \emptyset, \forall t$ so Condition 2 holds trivially. □

Theorem 3. *$\hat{\pi}(\hat{q}, \hat{x})$ defined in (5.2) implies $\hat{x}_o \notin \hat{S} \rightarrow \Box F(\phi_{\hat{x}}^{\hat{\pi}}) = true$.*

Proof. $\hat{\pi}(\hat{q}, \hat{x}) = (\emptyset, \emptyset)$ for $\hat{q} = h$ and $\hat{x}_o \notin S$. Also, from Lemma 3 and Lemma 4, $\hat{\pi}(\hat{q}, \hat{x})$ maintains safety for all modes in $\hat{Q}$. Hence, $\hat{\pi}(\hat{q}, \hat{x})$ solves Problem 2'. □

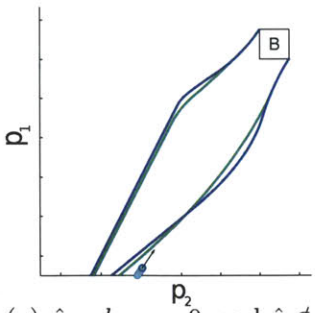
4.0.4 Simulation

Here, the results of a simulation for the driver assist system are shown. Because the capture sets are 4 dimensional objects, a 2 dimensional slice of the capture sets in

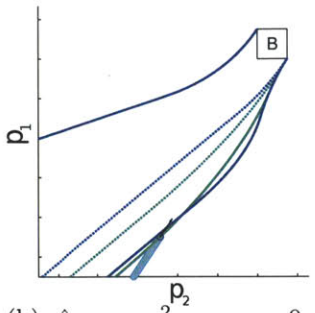
the position space of the vehicles is shown in Figure 4-4 for the current state in each snapshot. Let the coordinates of B be represented by $(L_1, U_1) \times (L_2, U_2)$, where L_i and U_i are the lower and upper coordinates of the intersection for vehicle i, respectively. To calculate the boundaries of the mode dependent capture set slices, the points (L_1, U_2) and (U_1, L_2) were back propagated as described in Section 5.0.6. $C(h)$ is shown in Figure 4-4(a) as the union of the sets bounded by the green and blue lines. The upper green and blue lines are the upper boundaries of $Pre(w^1, \{ho, hd\}^1, \tau_{RT} + T, C(\{ho, hd\}^1))$ and $Pre(w^1, hd^1, \tau_{RT} + T, C(ha^1))$, respectively. The lower green and blue lines are the lower boundaries of $Pre(w^2, \{ho, hd\}^2, \tau_{RT} + T, C(\{ho, hd\}^2))$ and $Pre(w^2, hd^2, \tau_{RT} + T, C(ha^2))$, respectively. The region between these lines forms their intersection, which from Theorem 4(ii), is equal to $C(h)$.

In Figure 4-4(b), $C(w^2)$ is the union of the region bounded by the solid green and blue lines, with the green corresponding to $Pre(w^2, \{ho, hd\}^2, \tau_{RT} + T, C(\{ho, hd\}^2))$ and the blue corresponding to $Pre(w^2, hd^2, T^*, C(ha^2))$. Also, $C(\{ho, hd\}^2)$ is represented by the region bounded by the dotted green lines, and $C(ha^2)$ is the dotted blue set. As τ approaches τ_{RT} in Fig. 4-4(c), $Pre(w^2, \{ho, hd\}^2, \tau_{RT} + T, C(\{ho, hd\}^2))$ collapses onto $C(\{ho, hd\}^2)$ because the τ_M argument of the Pre has elapsed. As τ approaches T^* in Fig. 4-4d, $Pre(w^2, hd^2, T^*, C(ha^2))$ collapses onto $C(ha^2)$ because the τ_M argument of the Pre has elapsed.

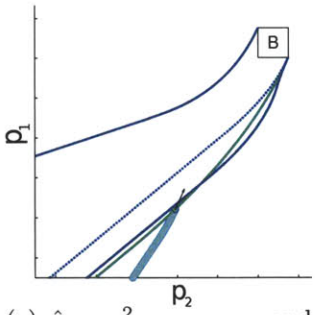
The vehicle acceleration inputs, $(\alpha_1(t), \alpha_2(t))$, and the estimator input $\hat{\beta}(t)$ are shown in Figure 4-4(g). Until the warning is issued, $d(t) = (0, 0)$, which results in $\alpha = (0, 0)$. Once the warning is issued at $t = 0.45$, $d = (-\bar{d}, \bar{d})$. At $t = 1.07$ vehicle 2 is overridden with $u(t) = \bar{u}$. The $\hat{\beta}$ plot shows that at $\hat{\beta}(1.06) \notin \Delta(\{ho, hd\}^2)$, the range denoted by the horizontal dashed lines. At this point, $\hat{q} = hd^2$ and enables the autonomous override of vehicle 2.



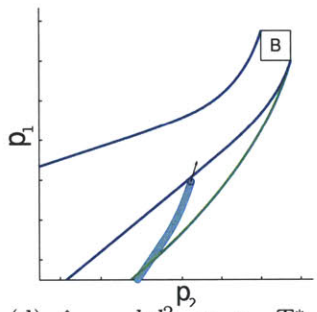
(a) $\hat{q} = h$, $\tau = 0$, and $\hat{x} \notin C(h)$. The vehicles are initially human driven with the state outside of $C(h)$.



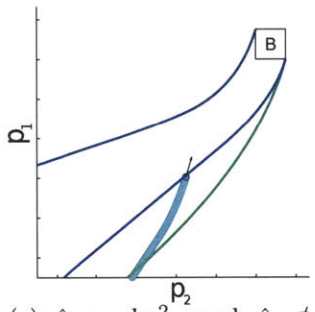
(b) $\hat{q} = w^2$, $\tau = 0$, and $\hat{x} \in \partial C(h)$ The state reaches the boundary of $C(h)$ and warning 2 is issued.



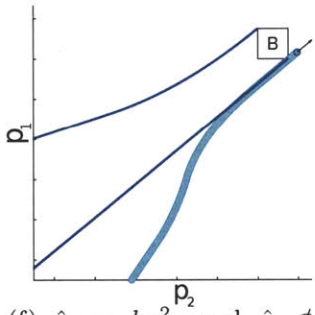
(c) $\hat{q} = w^2$, $\tau = \tau_{RT}$, and $\hat{x} \in \partial C(w^2)$. During the reaction time, the state remains outside of $C(w^2)$.



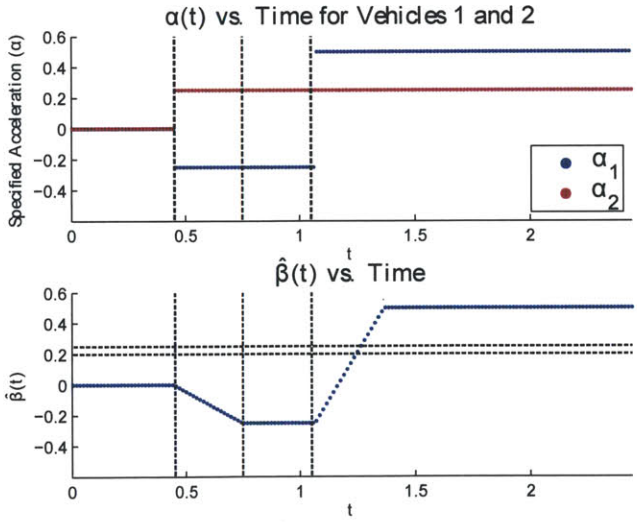
(d) $\hat{q} = hd^2$, $\tau > T^*$, and $\hat{x} \notin C(ha^2)$. The state entered $C(w^2)$, but at $\tau = T^*$ the estimator indicated vehicle 2 disobeyed the warning.



(e) $\hat{q} = ha^2$, and $\hat{x} \notin C(ha^2)$. Control event σ_u^2 triggered.



(f) $\hat{q} = ha^2$, and $\hat{x} \notin C(ha^2)$. The control keeps the state outside of B.



(g) $\alpha_1(t)$, $\alpha_2(t)$, $\hat{\beta}(t)$, shows the acceleration inputs to the vehicles and the estimator input value

Figure 4-4: Simulation results for the two vehicle system with $0 < v_{2_{min}} < v_{1_{min}}$ and $v_{2_{max}} > v_{1_{max}}$. All the bounded regions shown are slices of the mode dependent capture sets, corresponding to the capture sets for the current vehicle speeds (v_1, v_2).

Chapter 5

Solution to Safety Control Problems for Case 2

In this chapter, I utilize the estimator system for Case 2 to solve the modified safety control problems 1' and 2'.

5.0.5 Solution of Problem 1'

Problem 1' will be solved by constructing a mode dependent capture set, $C(\hat{q})$ as defined in Definition 5 for each mode $\hat{q} \in Q$. By definition, this capture set will be the solution to Problem 1' when $\hat{q}_o = h$, but again, this is only useful if there is a way to calculate this set. To do so, $C(h)$ will be constructed iteratively, starting with $\hat{q} \in \{a^1, a^2\}$ and working backwards towards $\hat{q}_o = h$. As seen in the following theorem, this technique is possible because there are no loops in $\hat{R}$.

Theorem 4. *Let $i \in \{1,2\}$. Then $\hat{S} = C(h)$ where:*

(i) $C(h) = C(w^1) \cap C(w^2)$

(ii) $C(w^i) = Pre(w^i, \{oo, do, od, dd\}^i, T^*, C(\{oo, do, od, dd\}^i)) \cup Pre(w^i, \{od, dd\}^i, T^*, C(\{od, dd\}^i)) \cup Pre(w^i, \{do, dd\}^i, T^*, C(\{do, dd\}^i)) \cup Pre(w^i, dd^i, T^*, C(a^i))$

(iii) $C(\{oo, do, od, dd\}^i) = Pre(\{oo, do, od, dd\}^i, C(\{oa, da\}^i) \cup C(\{ao, ad\}^i))$

(iv) $C(\{oa, da\}^i) = Pre(\{oa, da\}^i, C(a^i))$

(v) $C(\{ao, ad\}^i) = Pre(\{ao, ad\}^i, C(a^i))$

(vi) $C(a^i) = Pre(a^i, B)$.

Proof. First, apply (3.4) for $\hat{q}_o = a^i$, producing $C(a^i) = \{\hat{x}_o | \forall \hat{\pi}. \exists \hat{\boldsymbol{i}}, \mathbf{d}, t.$ s.t. $\phi^{\hat{\pi}}_{\hat{x}}(t, x_o, a^i, \mathbf{d}, \hat{\boldsymbol{i}}) \in B\}$. Because there are no discrete mode transitions from $\hat{q} = a^i$, this can be written $C(a^i) = Pre(a^i, B)$.

Next, apply (3.4) for $\hat{q}_o = dd^i$, producing $C(dd^i) = \{\hat{x}_o | \forall \hat{\pi}. \exists \hat{\boldsymbol{i}}, \mathbf{d}, t.$ s.t. $\phi^{\hat{\pi}}_{\hat{x}}(t, x_o, dd^i, \mathbf{d}, \hat{\boldsymbol{i}}) \in B\}$. Because the control event σ^i_u is allowable when $\hat{q} = dd^i$, and $\hat{R}(\tau, dd^i, \sigma_u 12^i, \hat{i}) = a^i$, we can write this as $C(dd^i) = \{\hat{x}_o | \forall \hat{\pi}. \exists \hat{\boldsymbol{i}}, \mathbf{d}, t.$ s.t. $\phi^{\hat{\pi}}_{\hat{x}}(t, x_o, a^i, \mathbf{d}, \hat{\boldsymbol{i}}) \in B\} = C(a^i)$. The exact same procedure can be applied for $\hat{q} \in \{da^i, ad^i\}$ to show that $C(da^i) = C(ad^i) = C(a^i)$. This procedure can be summarized as follows. Whenever a control event exists from from a given mode estimate $\hat{q}$, the mode dependent capture set is equal to that of the mode which that control event transitions too, that is, $C(q_i) = C(\hat{R}(R(\tau, \hat{q}_i, \sigma_u, \hat{i}))$.

Now, apply (3.4) for $\hat{q}_o = \{oa, da\}^i$, producing $C(\{oa, da\}^i) = \{\hat{x}_o | \forall \hat{\pi}. \exists \hat{\boldsymbol{i}}, \mathbf{d}, t.$ s.t. $\phi^{\hat{\pi}}_{\hat{x}}(t, x_o, \{oa, da\}^i, \mathbf{d}, \hat{\boldsymbol{i}}) \in B\}$. From the definition of $\hat{R}(\tau, \{oa, da\}^1, \sigma_u, \hat{i})$, one can enter B either by flowing directly into it or by first switching modes and then flowing into it. Hence while $\hat{q} = \{oa, da\}^i$, it is necessary to remain outside of $C(a^i) \cup B$. Because $C(a^i) \supset B$, we can write $C(\{oa, da\}^i) = Pre(\{oa, da\}^i, C(a^i))$. $C(\{ao, ad\}^i)$ can be written using the same logic as $C(\{ao, ad\}^i) = Pre(\{ao, ad\}^i, C(a^i))$.

Because control events exist for both $\hat{q} = \{od, dd\}^i$ and $\hat{q} = \{do, dd\}^i$, their mode dependent capture sets can be expressed as $C(\{od, dd\}^i) = C(\{oa, da\}^i)$ and $C(\{do, dd\}^i) = C(\{ao, ad\}^i)$ respectively.

Applying (3.4) to $\hat{q} = \{oo, do, od, dd\}^i$, produces $C(\{oo, do, od, dd\}^i) = \{\hat{x}_o | \forall \hat{\pi}. \exists \hat{\boldsymbol{i}}$, $\mathbf{d}, t.$ s.t. $\phi^{\hat{\pi}}_{\hat{x}}(t, x_o, \{oo, do, od, dd\}^i, \mathbf{d}, \hat{\boldsymbol{i}}) \in B\}$. From the definition of $\hat{R}(\tau, \{oo, do, od, dd\}^1, \sigma_u, \hat{i})$, one can enter B either by flowing directly into it or by first switching modes and then flowing into it. Hence while $\hat{q} = \{oo, do, od, dd\}^i$, it is necessary to remain outside of $C(\{oa, da\}^i) \cup C(\{ao, ad\}^i) \cup C(a^i) \cup B$. Because $(C(\{oa, da\}^i) \cup C(\{ao, ad\}^i)) \supset C(a^i) \supset B$, we can write $C(\{oo, do, od, dd\}^i) =$

$Pre(\{oo, do, od, dd\}, C(\{oa, da\}^i) \cup C(\{ao, ad\}^i))$.

Moving backwards to $\hat{q} = w^i$ and applying (3.4) once again produces $C(w^i) =: \{\hat{x}_o | \forall \hat{\pi}. \exists \hat{\boldsymbol{i}}, \mathbf{d}, t.$ s.t. $\phi_{\hat{x}}^{\hat{\pi}}(t, x_o, w^i, \mathbf{d}, \hat{\boldsymbol{i}}) \in B\}$. Writing $C(w^i)$ using the Pre operator requires the use of the τ_M argument because the mode estimate necessarily transitions to one of the modes $\hat{q} \in \{\{oo, do, od, dd\}^i, \{do, dd\}^i, \{od, dd\}^i, dd^i\}$ at $\tau = \tau_{RT} + T$ based on the value of $\hat{i}$. From the definition of $\hat{R}(\tau, w^1, \sigma_u, \hat{i})$, one can enter B either by flowing directly into it or by switching modes before flowing into it. Hence, while $\mathcal{F}(\hat{x}([\tau_{RT}, \tau_{RT} + T]) \in \Delta(\{oo, do, od, dd\}^i)$, it is necessary to remain outside of $C(\{oo, do, od, dd\}^i) \cup B = C(\{oo, do, od, dd\}^i)$.

If instead the dynamics are restricted by $\mathcal{F}(\hat{x}_j([\tau_{RT}, \tau_{RT}+T]) \notin \Delta_j(\{oo, do, od, dd\}^i)$, it is necessary to remain outside of the union of B with the mode dependent capture set of whichever observance transition event those dynamics would cause. It is important to note that there are no restrictions on $\mathcal{F}$ during $\tau \in [0, \tau_{RT})$.

Using these requirements, $C(w^i)$ can be written $C(w^i) = Pre(w^i, \{oo, do, od, dd\}^i, \tau_{RT} + T, C(\{oo, do, od, dd\}^i)) \cup Pre(w^i, \{do, dd\}^i, \tau_{RT} + T, C(\{do, dd\}^i)) \cup Pre(w^i, \{od, dd\}^i, \tau_{RT} + T, C(\{od, dd\}^i)) \cup Pre(w^i, dd^i, \tau_{RT} + T, C(dd^i) = C(a^i))$. We can then step back to the initial mode $\hat{q} = h$ and apply (3.4) to produce $C(h) = \{\hat{x}_o | \forall \hat{\pi}. \exists \hat{\boldsymbol{i}}, \mathbf{d}, t.$ s.t. $\phi_{\hat{x}}^{\hat{\pi}}(t, x_o, \hat{q}_o = h, \mathbf{d}, \hat{\boldsymbol{i}}) \in B\}$. From $\hat{R}$, there are two allowable control events $\sigma_u \in \{\sigma_u^{w1}, \sigma_u^{w2}\}$ when $\hat{q} = h$ and they lead to unconnected branches of the automaton. The flow could enter B either directly, or by executing one of these transitions first. Hence, while $\hat{q} = h$, it is necessary to avoid $(C(w^1) \cap C(w^2)) \cup B = C(w^1) \cap C(w^2)$. Using this, we can write $C(h) = C(w^1) \cap C(w^2)$.

□

5.0.6 Computational Tools

Theorem 4 provides an iterative formulation for $\hat{S}$, and for the mode dependent capture sets, $C(\hat{q})$, but each set is still expressed as the uncontrollable predecessor of other capture sets, which makes it difficult to calculate them. In order to make their computation efficient, we can express them as the uncontrollable predecessor of B under restricted disturbance signals. This will allow each capture set to be calculated

as a back integration of the much simpler set, B.

Proposition 4. $C(\{oa, da\}^i) = Pre(\{oa, da\}^i, B)$.

Proof. We first show $C(\{oa, da\}^1) \subseteq Pre(q = \{oa, da\}^1, B)$. Let $\hat{x} \in C(\{oa, da\}^1)$. Then, from Theorem 1(iv), this is true if and only if $\hat{x} \in Pre(\{oa, da\}^1, C(a^1))$. From Theorem 1(v) this is true if and only if $\hat{x} \in Pre(\{oa, da\}^1, Pre(a^1, B))$. Let $A_1 := \{\hat{x}_o | \exists \hat{\boldsymbol{i}}, \mathbf{d}.$ with $\mathbf{u_1} \equiv -\bar{\mathbf{u}}$, s.t. $\phi_{\hat{x}}^{\hat{\pi}}(t, \hat{x}_o, a^1, \mathbf{d}, \emptyset) \in S\}$. Then $\hat{x} \in A_1$ because the control input is restricted. This implies $\hat{x} \in Pre((\{oa, da\}^1, Pre(\{oa, da\}^1, B))$ because $\exists \mathbf{d_1}$ s.t. $\mathcal{F} = d_{min}$. This is true if and only if $\hat{x} \in Pre(\{oa, da\}^1, B)$ by the definition of Pre.

We show $C(\{oa, da\}^2) \subseteq Pre(q = \{oa, da\}^2, B)$. Let $\hat{x} \in C(\{oa, da\}^2)$. Then, from Theorem 1(iv), this is true if and only if $\hat{x} \in Pre(\{oa, da\}^2, C(a^2))$. From Theorem 1(v) this is true if and only if $\hat{x} \in Pre(\{oa, da\}^2, Pre(a^2, B))$. Let $A_2 := \{\hat{x}_o | \exists \hat{\boldsymbol{i}}, \mathbf{d}.$ with $\mathbf{u_1} \equiv \bar{\mathbf{u}}$, s.t. $\phi_{\hat{x}}^{\hat{\pi}}(t, \hat{x}_o, a^2, \mathbf{d}, \emptyset) \in S\}$. Then $\hat{x} \in A_2$ because the control input is restricted. This implies $\hat{x} \in Pre((\{oa, da\}^2, Pre((\{oa, da\}^2, B))$ because $\exists \mathbf{d_1}$ s.t. $\mathcal{F} = d_{max}$. This is true if and only if $\hat{x} \in Pre((\{oa, da\}^2, B)$ by the definition of Pre.

We show, $Pre(\{oa, da\}^i, B) \subseteq C(\{oa, da\}^i)$. Let $\hat{x} \in Pre(\{oa, da\}^i, B)$. Then, $\hat{x} \in Pre(\{oa, da\}^i, C(a^1))$ because $C(a^i) \supset B$. From Theorem 4(iv), this is true if and only if $\hat{x} \in C(\{oa, da\}^i)$. □

Proposition 5. $C(\{ao, ad\}^i) = Pre(\{ao, ad\}^i, B)$.

Proof. We first show $C(\{ao, ad\}^1) \subseteq Pre(q = \{ao, ad\}^1, B)$. Let $\hat{x} \in C(\{ao, ad\}^1)$. Then, from Theorem 1(iv), this is true if and only if $\hat{x} \in Pre(\{ao, ad\}^1, C(a^1))$. From Theorem 1(v) this is true if and only if $\hat{x} \in Pre(\{ao, ad\}^1, Pre(a^1, B))$. Let $A_1 := \{\hat{x}_o | \exists \hat{\boldsymbol{i}}, \mathbf{d}.$ with $\mathbf{u_2} \equiv \bar{\mathbf{u}}$, s.t. $\phi_{\hat{x}}^{\hat{\pi}}(t, \hat{x}_o, a^1, \mathbf{d}, \emptyset) \in S\}$. Then $\hat{x} \in A_1$ because the control input is restricted. This implies $\hat{x} \in Pre((\{ao, ad\}^1, Pre(\{ao, ad\}^1, B))$ because $\exists \mathbf{d_2}$ s.t. $\mathcal{F} = d_{max}$. This is true if and only if $\hat{x} \in Pre(\{ao, ad\}^1, B)$ by the definition of Pre.

We show $C(\{ao, ad\}^2) \subseteq Pre(q = \{ao, ad\}^2, B)$. Let $\hat{x} \in C(\{ao, ad\}^2)$. Then, from Theorem 1(iv), this is true if and only if $\hat{x} \in Pre(\{ao, ad\}^2, C(a^2))$. From

Theorem 1(v) this is true if and only if $\hat{x} \in Pre(\{ao, ad\}^2, Pre(a^2, B))$. Let $A_2 := \{\hat{x}_o | \exists \hat{\boldsymbol{i}}, \mathbf{d}.$ with $\mathbf{u_2} \equiv -\bar{\mathbf{u}}$, s.t. $\phi_{\hat{x}}^{\hat{\pi}}(t, \hat{x}_o, a^2, \mathbf{d}, \emptyset) \in S\}$. Then $\hat{x} \in A_2$ because the control input is restricted. This implies $\hat{x} \in Pre((\{ao, ad\}^2, Pre((\{ao, ad\}^2, B))$ because $\exists \mathbf{d_2}$ s.t. $\mathcal{F} = d_{min}$. This is true if and only if $\hat{x} \in Pre((\{ao, ad\}^2, B)$ by the definition of Pre.

We show, $Pre(\{ao, ad\}^i, B) \subseteq C(\{ao, ad\}^i)$. Let $\hat{x} \in Pre(\{ao, ad\}^i, B)$. Then, $\hat{x} \in Pre(\{ao, ad\}^i, C(a^1))$ because $C(a^i) \supset B$. From Theorem 4(v), this is true if and only if $\hat{x} \in C(\{ao, ad\}^i)$. □

Proposition 6. $C(\{oo, do, od, dd\}^i) = Pre(\{oo, do, od, dd\}^i, B)$.

Proof. We first show $C(\{oo, do, od, dd\}^1) \subseteq Pre(q = \{oo, do, od, dd\}^1, B)$. Let $\hat{x} \in C(\{oo, do, od, dd\}^1)$. Then, from Theorem 1(iii), this is true if and only if $\hat{x} \in Pre(\{oo, do, od, dd\}^1, C(\{oa, da\}^i) \cup C(\{ao, ad\}^i))$.

From Propositions 4 and 5 this is true if and only if $\hat{x} \in Pre(\{oo, do, od, dd\}^1, Pre(\{oa, da\}^1, B) \cup Pre(\{ao, ad\}^1))$. Let $A_1 := \{\hat{x}_o | \exists \hat{\boldsymbol{i}}, \mathbf{d}.$ with $\mathbf{u} \equiv (-\bar{\mathbf{u}}, \bar{\mathbf{u}})$, s.t. $\phi_{\hat{x}}^{\hat{\pi}}(t, \hat{x}_o, a^1, \mathbf{d}, \emptyset) \in S\}$. Then $\hat{x} \in A_1$ because the control input is restricted. This implies $\hat{x} \in Pre((\{oo, do, od, dd\}^1, Pre(\{oo, do, od, dd\}^1, B))$ because $\exists \mathbf{d}$ s.t. $\mathcal{F} = (d_{min}, d_{max})$. This is true if and only if $\hat{x} \in Pre(\{oo, do, od, dd\}^1, B)$ by the definition of Pre.

We show $C(\{oo, do, od, dd\}^2) \subseteq Pre(q = \{oo, do, od, dd\}^2, B)$. Let $\hat{x} \in C(\{oo, do, od, dd\}^2)$. Then, from Theorem 1(iv), this is true if and only if $\hat{x} \in Pre(\{oo, do, od, dd\}^2, C(a^2))$. From Theorem 1(v) this is true if and only if $\hat{x} \in Pre(\{oo, do, od, dd\}^2, Pre(a^2, B))$. Let $A_2 := \{\hat{x}_o | \exists \hat{\boldsymbol{i}}, \mathbf{d}.$ with $\mathbf{u} \equiv (\bar{\mathbf{u}}, -\bar{\mathbf{u}})$, s.t. $\phi_{\hat{x}}^{\hat{\pi}}(t, \hat{x}_o, a^2, \mathbf{d}, \emptyset) \in S\}$. Then $\hat{x} \in A_2$ because the control input is restricted. This implies $\hat{x} \in Pre((\{oo, do, od, dd\}^2, Pre((\{oo, do, od, dd\}^2, B))$ because $\exists \mathbf{d}$ s.t. $\mathcal{F} = (d_{max}, d_{min})$. This is true if and only if $\hat{x} \in Pre((\{oo, do, od, dd\}^2, B)$ by the definition of Pre.

We show, $Pre(\{oo, do, od, dd\}^i, B) \subseteq C(\{oo, do, od, dd\}^i)$. Let $\hat{x} \in Pre(\{oo, do, od, dd\}^i, B)$. Then, $\hat{x} \in Pre(\{oo, do, od, dd\}^i, Pre(\{oa, da\}^i, B) \cup Pre(\{ao, ad\}^i)$ because $(Pre(\{oa, da\}^i, B) \cup Pre(\{ao, ad\}^i) \supset B$. From Theorem 4(iv),

this is true if and only if $\hat{x} \in C(\{oo, do, od, dd\}^i)$. □

Proposition 7. $Pre(w^i, dd^i, T^*, C(a^i)) = Pre(w^i, dd^i, T^*, Pre(a^i, B))$.

Proof. Follows directly from Theorem 4(vi). □

Proposition 8.

$Pre(w^i, \{do, dd\}^i, T^*, C(a^i)) = Pre(w^i, \{do, dd\}^i, T^*, Pre(\{do, dd\}, B))$.

Proof. Follows directly from Proposition 1. □

Proposition 9.

$Pre(w^i, \{od, dd\}^i, T^*, C(a^i)) = Pre(w^i, \{od, dd\}^i, T^*, Pre(\{od, dd\}, B))$.

Proof. Follows directly from Proposition 2. □

Proposition 10.

$Pre(w^i, \{oo, do, od, dd\}^i, T^*, C(\{oo, do, od, dd\}^i)) = Pre(w^i, \{ho, hd\}\{oo, do, od, dd\}^i, T^*, Pre(\{oo, do, od, dd\}^i, B))$.

Proof. Follows directly from Proposition 3. □

Propositions 4 - 10 are useful because they allow for application of the results of [12] and [7] to efficiently calculate the capture sets. In order to do this we will utilize the maximal and minimal control signals determined in Section 3.2, to back propagate the bad set for each mode dependent capture set.

To compute $C(a^i)$, we know the control input ranges in $[-\bar{u}, \bar{u}]$, and the goal is to maximize/minimize the trajectory in the $x_1 - x_2$ plane. In order to maximize positive curvature, the controller simply applies the minimum input for vehicle 1 and the maximum input for vehicle 2, that is, $u(t) = (-\bar{u}, \bar{u})$ for all t. To minimize the trajectory, the controller applies the opposite input $u(t) = (\bar{u}, -\bar{u})$ for all t. We can then write, according to [12], [7],

$$C(ha^i) = C(ha^i)^H \cap C(ha^i)^L \tag{5.1}$$

with $C(ha^i)^H = \{\hat{x}_o | \exists \mathbf{d}, t \text{ s.t. } \phi_{\hat{x}}(t, \hat{x}_o, ha^i, (-\bar{u}, \bar{u}), \mathbf{d}, \emptyset, \emptyset) \in B\}$, and $C(ha^i)^L = \{\hat{x}_o | \exists \mathbf{d}, t \text{ s.t. } \phi_{\hat{x}}(t, \hat{x}_o, ha^i, (\bar{u}, -\bar{}), \mathbf{d}, \emptyset, \emptyset) \in B\}$. Since the input is fixed, these sets can

be computed by plain back integration of the set B under these inputs according to [12]. By the definition of the restricted capture sets $C(ha^i)^H$ and $C(ha^i)^L$, if the restricted control input used in their definition is applied to the system when the state is outside of either set, the state will remain outside of that set.

$C(\{oa, da\}^i)$, given Proposition 4, can be calculated similarly, but now the restrictions on $\mathcal{F}$ must be taken into account. For vehicle 2, the control input is again fixed to the maximum value for $C(\{oa, da\}^i)^H$, and to the minimum value for $C(\{oa, da\}^i)^L$. Each of these sets can be obtained by backward integration of B through all possible disturbances compatible with $\mathcal{F} \in \Delta\{oa, da\}^i$. By virtue of the order preserving dynamics, this backward integration can be accomplished by simply back integrating the lower bound of B through the maximal disturbance d_M and the upper bound of B through the minimal disturbance d_m, as calculated in section 3.2. Figures 4-1-4-3 show these signals for Case 1, and for Case 2 they can be build similarly, following the structure used for vehicle 2 in the Case 1 calculations.

$C(\{ao, ad\}^i)$, given Proposition 5, can also be calculated by taking into account the restrictions on $\mathcal{F}$. For vehicle 1, the control input is fixed to the minimum value for $C(\{ao, ad\}^i)^H$, and to the maximum value for $C(\{ao, ad\}^i)^L$. Each of these sets can be obtained by backward integration of B through all possible disturbances compatible with $\mathcal{F} \in \Delta\{ao, ad\}^i$. By virtue of the order preserving dynamics, this backward integration can be accomplished by simply back integrating the lower bound of B through the maximal disturbance d_M and the upper bound of B through the minimal disturbance d_m, as calculated in Section 3.2.

$C(\{oo, do, od, dd\}^i)$, given Proposition 6, again utilizes the restrictions on $\mathcal{F}$. Since there is no control input applied in the definition of $Pre(\{oo, do, od, dd\}^i, B)$, this set can be obtained by backward integration of B through all possible disturbances compatible with $\mathcal{F} \in \Delta\{oo, do, od, dd\}^i$. By virtue of the order preserving dynamics, this backward integration can be accomplished by simply back integrating the lower bound of B through the maximal disturbance d_M and the upper bound of B through the minimal disturbance d_m for each vehicle, as calculated in Section 3.2.

$C(w^i)$, given Theorem 4, Propositions 7-10, can be computed similarly by find-

ing the maximal and minimal disturbance profiles. Specifically, we first compute $Pre(w^i, \{oo, do, od, dd\}^i, \tau_{RT} + T, Pre(\{oo, do, od, dd\}^i, B))$, by breaking up its definition into two time intervals: $t < \tau_{RT}$ and $t \geq \tau_{RT}$. During the first time interval, there are no restrictions on the disturbance signal. For the second time interval the disturbance signal follows the same restrictions as when $\hat{q} = \{oo, do, od, dd\}^1$ and therefore we can use d_M and d_m as the maximal and minimal disturbances. To compute $Pre(w^i, dd^i, \tau_{RT}+T, Pre(a^i, B))$ we write it using the restricted capture sets from (5.1) as $Pre(w^i, dd^i, \tau_{RT}+T, C(a^i)^L \cap C(a^i)^H)$, and again split it into two time intervals. For $t < T^*$, there are no restrictions on the disturbance input. For $t \geq T^*$, we caculate a set $C(w^i)^H$, with $u(t) = (-\bar{u}, \bar{u})$ and $C(w^i)^L$ with $u(t) = (\bar{u}, -\bar{u})$. Using the order preserving properties of the system, $C(w^i) = C(w^i)^L \cap C(w^i)^H$ using again the results of [7, 11, 12]. The remaining two sets, $Pre(w^i, C(\{ao, ad\}^i), \tau_{RT} + T, Pre(\{do, dd\}^i, B))$ and $Pre(w^i, C(\{oa, da\}^i), \tau_{RT} + T, Pre(\{od, dd\}^i, B))$ are calculated using a similar strategy, with the autonomous vehicle utilizing the same control input as $C(a^i)$, and the human driven car using the same disturbance input as $C(\{oo, do, od, dd\}^i)$.

As shown in Theorem 4, all of the mode dependent capture sets can be expressed as combinations of $C(a)^i, C(\{oo, od, do, dd\}^i), C(\{ao, ad\}^i), C(\{oa, da\}^i)$, and $C(w^i)$, and as a consequence, it is possible to efficiently calculate all of the mode dependent capture sets.

5.0.7 Solution to Problem 2'

Problem 2' is solved by constructing a control map, $\hat{\pi}(\hat{q}, \hat{x})$, using the known properties of the mode dependent capture set $C(\hat{q})$. For a set S, let ∂S denote the boundary of S. Using the known properties of the mode dependent capture set, $C(\hat{q})$, we con-

struct $\hat{\pi}$ as follows:

$$\hat{\pi}(\hat{q},\hat{x}) = \tag{5.2}$$

$$\begin{cases} u = \begin{cases} (-\bar{u},\bar{u}) & \text{if } q \in \{a^i\} \wedge x \in C(\hat{q})^H \cap \partial C(\hat{q})^L \\ (\bar{u},-\bar{u}) & \text{if } q \in \{a^i\} \wedge x \in C(\hat{q})^L \cap \partial C(\hat{q})^H \\ (\emptyset,\bar{u}) & \text{if } q \in \{\{oa,da\}^i\} \wedge x \in C(\hat{q})^H \cap \partial C(\hat{q})^L \\ (\emptyset,-\bar{u}) & \text{if } q \in \{\{oa,da\}^i\} \wedge x \in C(\hat{q})^L \cap \partial C(\hat{q})^H \\ (-\bar{u},\emptyset) & \text{if } q \in \{\{ao,ad\}^i\} \wedge x \in C(\hat{q})^H \cap \partial C(\hat{q})^L \\ (\bar{u},\emptyset) & \text{if } q \in \{\{ao,ad\}^i\} \wedge x \in C(\hat{q})^L \cap \partial C(\hat{q})^H \\ (\emptyset,\emptyset) & \text{else} \end{cases} \\ \sigma_u = \begin{cases} \sigma^i_{u12} & \text{if } \hat{q} = dd^i \wedge x \in \partial C(a^i) \\ \sigma^i_{u1} & \text{if } (\hat{q} = \{do,dd\}^i \wedge x \in \partial C(\{ao,ad\}^i)) \vee (\hat{q} = da^i \wedge x \in \partial C(a^i)) \\ \sigma^i_{u2} & \text{if } (\hat{q} = \{od,dd\}^i \wedge x \in \partial C(\{oa,da\}^i)) \vee (\hat{q} = ad^i \wedge x \in \partial C(a^i)) \\ \sigma^{w1}_u & \text{if } \hat{q} = h \wedge x \in C(w^2) \wedge x \in \partial C(w^1) \\ \sigma^{w2}_u & \text{if } \hat{q} = h \wedge x \in C(w^1) \wedge x \in \partial C(w^2) \\ \emptyset & \text{else.} \end{cases} \end{cases}$$

This map checks the membership of the current state with respect to the mode dependent capture set $C(\hat{q})$, and uses this information to determine if control event or continuous control is required to maintain safety. It utilizes the decomposition of the capture sets into restricted capture sets in order to determine what the specified control action should be. In order for $\hat{\pi}(\hat{q},\hat{x})$ to be safe, two conditions must hold for all $\hat{q} \in \hat{Q}$. First, while in any mode $\hat{q}_i$, the flow must not enter the bad set. Second, no discrete transition from mode $\hat{q}_i$ to mode $\hat{q}_j$ can cause the continuous flow to enter the mode dependent capture set $C(\hat{q}_j)$ after the transition. Let $\tau_{\hat{q}_i}$ denote the transition time *to* the mode estimate $\hat{q} = \hat{q}_i$, and $\tau'_{\hat{q}_i}$ denote the transition time *from* that estimate.

Condition 1: $\hat{x}(\tau_{\hat{q}_i}) \notin C\hat{q}_i \Rightarrow \forall \mathbf{d}, t \in [\tau_{q_i}, \tau'_{q_i}).\ \phi^{\hat{\pi}}_{\hat{x}}(t, \hat{x}(\tau_{\hat{q}_i}), \hat{q}_i, \mathbf{d}, \emptyset) \notin B.$

Condition 2: $\hat{x}(\tau_{\hat{q}_i}) \notin C\hat{q}_i \Rightarrow \forall \hat{q}_j \in \cup_{\hat{i} \in I} \hat{R}(\tau, \hat{q}_i, \sigma_u, \hat{i}).\ x(\tau'_{q_i}) \notin C(\hat{q}_j).$

Lemma 3. *Condition 1 holds for all* $\hat{q} \in \hat{Q}$.

Proof. (by cases): For $\hat{q} = h$, if $\sigma_u = \emptyset$, then $\hat{x} \notin \partial C(w^1) \cap C(w^2)$ by the definition of $\hat{\pi}$ and so $\hat{x} \notin B$. If $\sigma_u \in \{\sigma_u^{w1}, \sigma_u^{w2}\}$, for $t > \tau_h' q(t) \neq h$. Hence, $\forall t \in [\tau_h, \tau_h')$, we have that $\phi_{\hat{x}}^{\hat{\pi}} \notin B$.

For $\hat{q} = w^i$, by the definition of $C(w^i), \hat{x}(\tau_{w^i}) \notin C(w^i) \Rightarrow \phi_{\hat{x}}^{\hat{\pi}}(\tau < \tau_{w^i}' = \tau_{w^i} + \tau_{RT} + T) \notin C(\{ho, hd\}^i) \cap C(ha^i)$. $C(\{ho, hd\}^i) \cap C(ha^i) \supset B$. Hence, $\forall t \in [\tau_{w^i}, \tau_{w^i}')$, we have that $\phi_{\hat{x}}^{\hat{\pi}} \notin B$.

For $\hat{q} = \{oo, do, od, dd\}^i$, there is no control while $\hat{q} = \{oo, do, od, dd\}^i$, so the definition of $C(\{oo, do, od, dd\}^i)$ implies that $\hat{x}(\tau_{w^i}) \notin C(\{oo, do, od, dd\}^i) \Rightarrow \phi_{\hat{x}}^{\hat{\pi}} \notin C(a^i)$. Hence, $\forall t \in [\tau_{\{oo,do,od,dd\}^i}, \tau_{\{oo,do,od,dd\}^i}')$, we have that $\phi_{\hat{x}}^{\hat{\pi}} \notin B$.

For $\hat{q} = \{od, dd\}^i$, if $\sigma_u = \emptyset$, then $\hat{x} \notin C(\{oa, da\}^i)$ by the definition of $\hat{\pi}$ and so $\hat{x} \notin B$. If $\sigma_u = \sigma_u^i$, for $t > \tau_{\{od,dd\}}' q(t) \neq \{od, dd\}^i$. Hence, $\forall t \in [\tau_{\{od,dd\}^i}, \tau_{\{od,dd\}^i}')$, we have that $\phi_{\hat{x}}^{\hat{\pi}} \notin B$.

For $\hat{q} = \{do, dd\}^i$, if $\sigma_u = \emptyset$, then $\hat{x} \notin C(\{ao, ad\}^i)$ by the definition of $\hat{\pi}$ and so $\hat{x} \notin B$. If $\sigma_u = \sigma_u^i$, for $t > \tau_{\{do,dd\}}' q(t) \neq \{do, dd\}^i$. Hence, $\forall t \in [\tau_{\{do,dd\}^i}, \tau_{\{do,dd\}^i}')$, we have that $\phi_{\hat{x}}^{\hat{\pi}} \notin B$.

For $\hat{q} = dd^i$, if $\sigma_u = \emptyset$, then $\hat{x} \notin C(a^i)$ by the definition of $\hat{\pi}$ and so $\hat{x} \notin B$. If $\sigma_u = \sigma_u^i$, for $t > \tau_{dd}' q(t) \neq dd^i$. Hence, $\forall t \in [\tau_{dd^i}, \tau_{dd^i}')$, we have that $\phi_{\hat{x}}^{\hat{\pi}} \notin B$.

For $\hat{q} = \{oa, da\}^i$, as discussed in Section 5.0.6, the application of $u = (\emptyset, -\bar{u})$ (for $\hat{q} = \{oa, da\}^1$) or $u = (\emptyset, \bar{u}$ (for $\hat{q} = \{oa, da\}^2$) when $\hat{x} \in \partial C(\{oa, da\}^i)$ renders the relation $\hat{x} \notin C(\{oa, da\}^i)$ invariant. Hence, $\forall t \in [\tau_{\{oa,da\}^i}, \tau_{\{oa,da\}^i}')$, we have that $\phi_{\hat{x}}^{\hat{\pi}}(t) \notin B$.

For $\hat{q} = \{ao, ad\}^i$, as discussed in Section 5.0.6, the application of $u = (\bar{u}, \emptyset)$ (for $\hat{q} = \{ao, ad\}^1$) or $u = (-\bar{u}, \emptyset)$ (for $\hat{q} = \{ao, ad\}^2$) when $\hat{x} \in \partial C(\{ao, ad\}^i)$ renders the relation $\hat{x} \notin C(\{ao, ad\}^i)$ invariant. Hence, $\forall t \in [\tau_{\{ao,ad\}^i}, \tau_{\{ao,ad\}^i}')$, we have that $\phi_{\hat{x}}^{\hat{\pi}}(t) \notin B$.

For $\hat{q} = da^i$, if $\sigma_u = \emptyset$, then $\hat{x} \notin C(a^i)$ by the definition of $\hat{\pi}$ and so $\hat{x} \notin B$. If $\sigma_u = \sigma_u^i$, for $t > \tau_{da}' q(t) \neq da^i$. Hence, $\forall t \in [\tau_{da^i}, \tau_{da^i}')$, we have that $\phi_{\hat{x}}^{\hat{\pi}} \notin B$.

For $\hat{q} = ad^i$, if $\sigma_u = \emptyset$, then $\hat{x} \notin C(a^i)$ by the definition of $\hat{\pi}$ and so $\hat{x} \notin B$. If $\sigma_u = \sigma_u^i$, for $t > \tau_{ad}' q(t) \neq ad^i$. Hence, $\forall t \in [\tau_{ad^i}, \tau_{ad^i}')$, we have that $\phi_{\hat{x}}^{\hat{\pi}} \notin B$.

For $\hat{q} = a^i$, as discussed in Section 5.0.6, the application of $u = (\bar{u}, -\bar{u})$ (for

$\hat{q} = ha^1$) or $u = (-\bar{u}, \bar{u}$ (for $\hat{q} = ha^2$) when $\hat{x} \in \partial C(a^i)$ renders the relation $\hat{x} \notin C(a^i)$ invariant. Hence, $\forall t \in [\tau_{a^i}, \tau'_{a^i})$, we have that $\phi^{\hat{\pi}}_{\hat{x}}(t) \notin B$. □

Lemma 4. *Condition 2 holds for all* $\hat{q} \in \hat{Q}$.

Proof. (by cases): Let q_j be the mode being transitioned to. For $\hat{q}_i = h$ and $\hat{q}_j = w^i, \hat{R}(\tau, h, \sigma^{w1}_u, \hat{\beta}) = w^i$. By the definition of $\hat{\pi}$, $\sigma_u = \sigma^{w1}_u$ when $\hat{x}(\tau_{w^i}) \notin C(w^i)$. Hence, $\hat{x}(\tau'_h) \notin C(w^i)$.

For $\hat{q}_i = w^i$ and $\hat{q}_j = \{oo, do, od, dd\}^i$, $\mathcal{F}_1(\hat{x}([\tau_{RT}, \tau_{RT} + T]) \in \Delta_1(\{oo, do, od, dd\}^i$, and $\mathcal{F}_2(\hat{x}([\tau_{RT}, \tau_{RT} + T]) \in \Delta_2(\{oo, do, od, dd\}^i$. By the definition of $C(w^i), \hat{x}(\tau_{w^i}) \notin C(w^i)$ and $\mathcal{F}_1(x([\tau_{RT}, \tau_{RT} + T]) \in \Delta_1(\{oo, do, od, dd\}^i) \wedge \mathcal{F}_2(\hat{x}([\tau_{RT}, \tau_{RT} + T]) \in \Delta_2(\{oo, do, od, dd\}^i$ and implies $\hat{x}(\tau'_{w^i}) \notin C(\{oo, do, od, dd\}^i)$. Hence, $x(\tau'_{w^1}) \notin C(\{oo, do, od, dd\}^i)$.

For $\hat{q}_i = w^i$ and $\hat{q}_j = \{od, dd\}^i$, $\mathcal{F}_1(\hat{x}([\tau_{RT}, \tau_{RT} + T]) \in \Delta_1(\{od, dd\}^i$, and $\mathcal{F}_2(\hat{x}([\tau_{RT}, \tau_{RT} + T]) \notin \Delta_2(\{od, dd\}^i$. By the definition of $C(w^i), \hat{x}(\tau_{w^i}) \notin C(w^i)$ and $\mathcal{F}_1(x([\tau_{RT}, \tau_{RT} + T]) \in \Delta_1(\{od, dd\}^i) \wedge \mathcal{F}_2(\hat{x}([\tau_{RT}, \tau_{RT} + T]) \notin \Delta_2(\{od, dd\}^i$ implies $\hat{x}(\tau'_{w^i}) \notin C(\{od, dd\}^i)$. Hence, $x(\tau'_{w^1}) \notin C(\{od, dd\}^i)$.

For $\hat{q}_i = w^i$ and $\hat{q}_j = \{do, dd\}^i$, $\mathcal{F}_1(\hat{x}([\tau_{RT}, \tau_{RT} + T]) \notin \Delta_1(\{do, dd\}^i$, and $\mathcal{F}_2(\hat{x}([\tau_{RT}, \tau_{RT} + T]) \in \Delta_2(\{do, dd\}^i$. By the definition of $C(w^i), \hat{x}(\tau_{w^i}) \notin C(w^i)$ and $\mathcal{F}_1(x([\tau_{RT}, \tau_{RT} + T]) \notin \Delta_1(\{do, dd\}^i) \wedge \mathcal{F}_2(\hat{x}([\tau_{RT}, \tau_{RT} + T]) \in \Delta_2(\{do, dd\}^i$ implies $\hat{x}(\tau'_{w^i}) \notin C(\{do, dd\}^i)$. Hence, $x(\tau'_{w^1}) \notin C(\{do, dd\}^i)$.

For $\hat{q}_i = w^i$ and $\hat{q}_j = dd^i$, the definition of $C(w^i)$ implies $\hat{x}(\tau_{w^i}) \notin C(w^i)$ and $\mathcal{F}(x([\tau_{RT}, \tau_{RT} + T]) \notin \Delta(\{ho, hd\}^i)$. This implies $\hat{x}(\tau'_{w^i}) \notin C(ha^i)$. Hence, $x(\tau'_{w^1}) \notin C(ha^i)$.

For $\hat{q}_i = \{oo, do, od, dd\}^i$ and $\hat{q}_j \in \{\{dd\}^i, \{od, dd\}^i, \{do, dd\}^i\}$, the definition of $C(\{oo, do, od, dd\}^i)$ implies $\hat{x}(\tau_{\{oo,do,od,dd\}^i}) \notin C(\{oo, do, od, dd\}^i)$ and $\hat{\beta}_1([\tau'_{\{oo,do,od,dd\}^i}, \tau'_{\{oo,do,od,dd\}^i})) \in \Delta_1(\{oo, do, od, dd\}^i) \wedge \hat{\beta}_2([\tau'_{\{oo,do,od,dd\}^i}, \tau'_{\{oo,do,od,dd\}^i})) \in \Delta_2(\{oo, do, od, dd\}^i)$ implies $\hat{x}(\tau'_{\{oo,do,od,dd\}^i}) \notin C(\{oo, do, od, dd\}^i)$. Hence, $\hat{x}(\tau'_{\{oo,do,od,dd\}^i}) \notin C(a^i) \cup C(\{oa, da\}^i) \cup C(\{ao, ad\}^i)$.

For $\hat{q}_i = dd^i$ and $\hat{q}_j = a^i$, the definition of $\hat{\pi}$ implies $\sigma_u = \sigma^i_{u12}$ when $x \notin C(a^i)$. Hence, $\hat{x}(\tau'_{dd}) \notin C(a^i)$.

For $\hat{q}_i = \{od, dd\}^i$ and $\hat{q}_j = \{oa, da\}^i$, the definition of $\hat{\pi}$ implies $\sigma_u = \sigma^i_{u2}$ when $x \notin C(\{od, da\}^i)$. Hence, $\hat{x}(\tau'_{od,dd}) \notin C(\{oa, da\}^i)$.

For $\hat{q}_i = \{do, dd\}^i$ and $\hat{q}_j = \{ao, ad\}^i$, the definition of $\hat{\pi}$ implies $\sigma_u = \sigma^i_{u1}$ when $x \notin C(\{do, ad\}^i)$. Hence, $\hat{x}(\tau'_{do,dd}) \notin C(\{ao, ad\}^i)$.

For $\hat{q}_i = \{oa, da\}^i$ and $\hat{q}_j = da^i\}$, the definition of $C(\{oa, da\}^i)$ and Lemma 3 implies $\hat{x}(\tau_{\{oa,da\}^i}) \notin C(\{oa, da\}^i)$ and $\hat{\beta}_1([\tau'_{\{oa,da\}^i}, \tau'_{\{oa,da\}^i})) \in \Delta_1(\{oa, da\}^i)$ implies $\hat{x}(\tau'_{\{oa,da\}^i}) \notin C(\{oa, da\}^i)$. Hence, $\hat{x}(\tau'_{\{oa,da\}^i}) \notin C(a^i)$.

For $\hat{q}_i = \{ao, ad\}^i$ and $\hat{q}_j = ad^i\}$, the definition of $C(\{ao, ad\}^i)$ and Lemma 3 implies $\hat{x}(\tau_{\{ao,ad\}^i}) \notin C(\{ao, ad\}^i)$ and $\hat{\beta}_2([\tau'_{\{ao,ad\}^i}, \tau'_{\{ao,ad\}^i})) \in \Delta_d(\{ao, ad\}^i)$ implies $\hat{x}(\tau'_{\{ao,ad\}^i}) \notin C(\{ao, ad\}^i)$. Hence, $\hat{x}(\tau'_{\{ao,ad\}^i}) \notin C(a^i)$.

For $\hat{q}_i = da^i$ and $\hat{q}_j = a^i$, the definition of $\hat{\pi}$ implies $\sigma_u = \sigma^i_{u1}$ when $x \notin C(a^i)$. Hence, $\hat{x}(\tau'_{da}) \notin C(a^i)$.

For $\hat{q}_i = ad^i$ and $\hat{q}_j = a^i$, the definition of $\hat{\pi}$ implies $\sigma_u = \sigma^i_{u2}$ when $x \notin C(a^i)$. Hence, $\hat{x}(\tau'_{ad}) \notin C(a^i)$.

For $\hat{q}_i = a^1$, $\hat{i}(t) = \emptyset, \forall t$ so Condition 2 holds trivially. □

Theorem 5. *$\hat{\pi}(\hat{q}, \hat{x})$ defined in (5.2) implies $\hat{x}_o \notin \hat{S} \rightarrow \Box F(\phi^{\hat{\pi}}_{\hat{x}}) = true$.*

Proof. $\hat{\pi}(\hat{q}, \hat{x}) = (\emptyset, \emptyset)$ for $\hat{q} = h$ and $\hat{x}_o \notin S$. Also, from Lemma 3 and Lemma 4, $\hat{\pi}(\hat{q}, \hat{x})$ maintains safety for all modes in $\hat{Q}$. Hence, $\hat{\pi}(\hat{q}, \hat{x})$ solves Problem 2'. □

5.0.8 Simulation

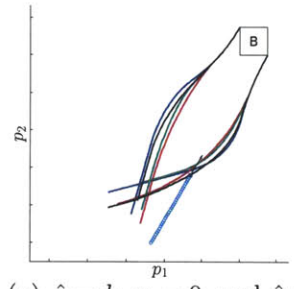
Here, the results of a simulation for the driver assist system are shown. Because the capture sets are 4 dimensional objects, a 2 dimensional slice of the capture sets in the position space of the vehicles is shown in Figure 5-1 for the current state in each snapshot. Let the coordinates of B be represented by $(L_1, U_1) \times (L_2, U_2)$, where L_i and U_i are the lower and upper coordinates of the intersection for vehicle i, respectively. To calculate the boundaries of the mode dependent capture set slices, the points (L_1, U_2) and (U_1, L_2) were back propagated as described in Section 5.0.6. $C(h)$ is shown in Figure 5-1(a) as the union of the sets bounded by the red, green, blue, and black lines. The upper lines are the upper boundaries of

$Pre(w^1, \{oo, od, do, dd\}^1, T^*, C(\{oo, od, do, dd\}^1))$, $Pre(w^1, \{do, dd\}^1, T^*, C(\{ao, ad\}^1))$, $Pre(w^1, \{do, dd\}^1, T^*, C(\{oa, da\}^1))$, and $Pre(w^1, a^1, T^*, C(a^1))$. The lower lines represent the lower boundaries of the equivalent capture sets corresponding to warning 2. The region between these lines forms their intersection, which from Theorem 4(ii), is equal to $C(h)$.

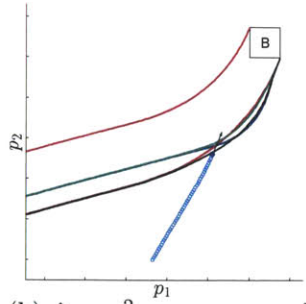
In Figure 5-1(b), warning 2 has been issued and $\tau = \tau_{RT}$. $C(w^2)$ is the union of the region bounded by the various colored lines, with the red corresponding to $Pre(w^2, \{oo, od, do, dd\}^2, T^*, C(\{oo, od, do, dd\}^2))$, the green corresponding to $Pre(w^2, \{do, dd\}^2, T^*, C(\{ao, ad\}^2))$, the black corresponding to $Pre(w^2, \{od, dd\}^2, T^*, C(\{oa, da\}^2))$, and the blue corresponding to $Pre(w^2, dd^2, T^*, C(a^2))$. In Fig. 4-4(c), $\tau = T^*$. The red set represents $C(\{oo, od, do, dd\}^2)$, the green set represents $C(\{ao, ad\}^2)$, the black set represents $C(\{oa, da\}^2)$, and the blue set represents $C(a^2)$.

The vehicle acceleration inputs, $(\alpha_1(t), \alpha_2(t))$, and the estimator input $\hat{\beta}(t)$ are shown in Figure 5-1(g). Until the warning is issued, $d(t) = (0, 0)$, which results in $\alpha = (0, 0)$. Once the warning is issued at $t = 0.7$, $d = (-\bar{d}, \bar{d})$. At $t = 1.4$ vehicle 2 is overridden with $u(t) = -\bar{u}$. The $\hat{\beta}$ plot shows that at $\hat{\beta}(1.06) \notin \Delta(\{od, dd\}^2)$, the range denoted by the red horizontal dashed line. At this point, $\hat{q} = \{od, dd\}^2$ and enables the autonomous override of vehicle 2.

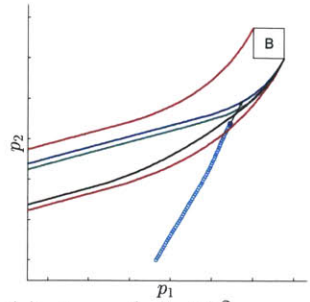
The other cases of obedience produce a similar system evolution, all resulting in safe passage through the intersection. If both cars obey, the state will always remain outside of $C(\{oo, od, do, dd\}^i)$ for the specified warning σ_u^i and no overrides will be necessary. If both cars disobey, the state will remain outside of $C(\{a^i\})$ for the specified warning σ_u^i at least until $\tau = T^*$, at which point autonomous override is allowed if necessary.



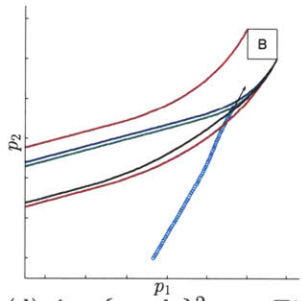
(a) $\hat{q} = h$, $\tau = 0$, and $\hat{x} \in \partial C(h)$. The state reaches the boundary of $C(h)$ and warning 2 is issued.



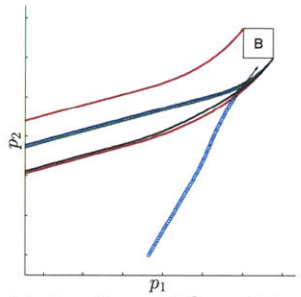
(b) $\hat{q} = w^2$, $\tau = \tau_{RT}$, and $\hat{x} \in \partial C(w^2)$. The reaction time has passed and the estimator is initialized.



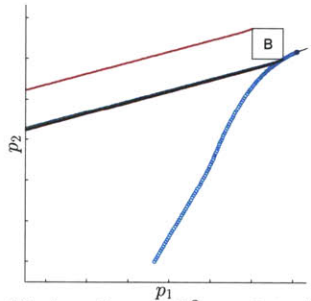
(c) $\hat{q} = \{od, dd\}^2$, $\tau = T^*$, and $\hat{x} \notin C(\{oa, da\}^2)$. The estimator determines that vehicle 2 has disobeyed.



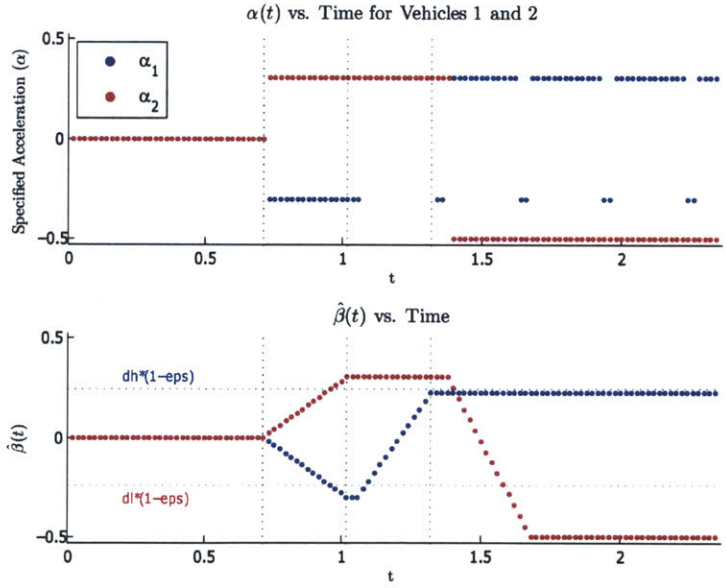
(d) $\hat{q} = \{oa, da\}^2$, $\tau > T^*$, and $\hat{x} \in \partial C(\{oa, da\}^2)$. σ_u^2 occurs, that is, vehicle 2 is overriden to gaurantee safety.



(e) $\hat{q} = \{oa, da\}^2$, and $\hat{x} \notin C(\{oa, da\}^2)$. The state



(f) $\hat{q} = \{oa, da\}^2$, and $\hat{x} \notin C(\{oa, da\}^2)$. The control keeps the state outside of B.



(g) $\alpha_1(t)$, $\alpha_2(t)$, $\hat{\beta}(t)$, shows the acceleration inputs to the vehicles and the estimator input value

Figure 5-1: Simulation results for the two vehicle system with $0 < v_{1_{min}} = v_{2_{min}}$ and $v_{1_{max}} = v_{2_{max}}$. All the bounded regions shown are slices of the mode dependent capture sets, corresponding to the capture sets for the current vehicle speeds (v_1, v_2).

Chapter 6

Experimental Validation of Algorithms

With the theory and simulations for the driver assist systems complete, the next step in the design process was experimental validation. The Multi-Vehicle Laboratory at MIT provided a platform for performing such tests. By implementing the algorithms on dynamically scaled vehicles and testing with actual human subject will expose any possible limitations or implementation issues not present in the ideal environment of a simulation code. At the time of completion of this thesis, full experimental trials have not been carried out, but the algorithm has been implemented as a proof of concept for future testing.

6.1 Lab Setup

The Multi-Vehicle Laboratory contains 6 dynamically scaled vehicles for testing control algorithms. Real time tracking of the vehicles is performed using an overhead camera system and computer vision algorithms. This positioning data from this system is then sent to the vehicles via wireless internet. A photo of the lab space can be seen in Figure 6-1. The vehicles are built on a Tamiya scaled RC car chassis. Each vehicle is contains a VIA EPIA TC6000 Mini ITX motherboard, equipped with a 600 MHz processor, 512 DDR400 RAM, and a D-Link WUA-1340 Wireless G USB

Figure 6-1: Photo of Multi-Vehicle Laboratory.

Adapter. Each on-board computer is running Fedora Core 5 Linux, and the control algorithms are executed as programs written in C. For human driven vehicles, a Logitech PlayStation 3 Driving Force GT Racing Wheel, is used to obtain the driver's steering and accelerations inputs. The Brainstem MOTO 1.0 Module is used for motor control, converting the specified control inputs output from the motherboard into PWM signals sent to the motors.

6.2 Status of Experiment

The driver assist system for the two car system for Case 1 has been implemented as a proof of concept. The paths used can be seen in Figure 6-1 with the intersection defined as the zone marked by the red tape towards the right of the image. To reduce the number of test subjects required, the car without the driver assist system is driven autonomously and programmed such that it behaves adversarially, attempting

to cause a collision. This simulates the worst case scenario if that vehicle were actually driven by a human. The warning is issued via audio signal, with a buzz representing the "slow down" warning and a ding representing the "speed up" signal.

A few additional steps remain before full experimental trials with human drivers can be carried out. Testing needs to be done to figure out what values to use for the time delay, τ_{RT}, and time parameter, T. Also, testing to find how drivers respond to each warning will be necessary to determine d_{min} and d_{max}. Once these parameters have been determined, five different drivers will be tested, each performing a minimum of ten successful intersection passes for which a warning is issued. This experiment will hopefully validate the effectiveness of the algorithms in preventing collisions while allowing drivers to maintain control of their vehicles if possible. Potential difficulties could arise from additional time delays due to latency in the data transfer between the tracking system and warning system, or due to inconsistent state information between cars if some packets are lost during transfer.

Chapter 7

Conclusions and Future Work

In this thesis, I have developed a driver assist system design that provides warnings and applies overrides if the driver does not comply to the warnings, to prevent collisions at traffic intersection. I have formulated this problem as a safety control problem for hybrid automata with hidden modes, in which the hidden modes model driver's decisions. This solution approach constructs a mode estimator and determines an unsafe region in the state space, called the mode dependent capture set, for a given system mode estimate. If the system continuous state given the current mode estimate is found in the corresponding mode dependent capture set, the vehicles are bound to collide. We found the smallest unsafe set and then developed a dynamic control map which guarantees safety for all initial states outside of that set. The solution has been validated through simulation, and has been implemented on scaled vehicles in the laboratory. Work in the laboratory is still in progress, with the goal of completing human trials to gain insight into the practical implications of the designed system.

7.1 Future Work

As stated, immediate future efforts will focus on finalizing the implementation of the described algorithms experimentally and testing them with a sampling of human subjects. Another logical progression for further efforts is to adapt the algorithm

to work cooperatively for vehicle systems containing more than two vehicles. This may require adapting the techniques used to improve their computational efficiency, because the current methods scale exponentially with then number of vehicles. More advanced models of human behavior, including a stochastic element to the reaction time and decision components of the modeling might provide further interesting insights into the problem. Additionally, there is the potential to combine the safety control techniques proposed here with optimal control techniques. This would allow for additional criteria, such as fuel efficiency, to be optimized while maintaining a given safety specification.

Bibliography

[1] T. Akita, S. Inagaki, T. Suzuki, S. Hayakawa, and N. Tsuchida. Hybrid system modeling of human driver in the vehicle following task. In *SICE, 2007 Annual Conference*, pages 1122 –1127, 2007.

[2] A. Carter. The status of vehicle-to-vehicle communication as a means of improvement crash prevention performance. In *NHTSA Tech. Rep. 05-0264*, http://www-nrd.nhtsa.dot.gov/pdf/nrd-01/esv/esv19/05-0264-W.pdf, 2005.

[3] D. Del Vecchio, M. Malisoff, and R. Verma. A separation principle for a class of hybrid automata on a partial order. In *American Control Conference*, 2009.

[4] D. Del Vecchio, R. M. Murray, and P. Perona. Decomposition of human motion into dynamics-based primitives with application to drawing tasks. *Automatica*, 39(12):2085–2098, 2003.

[5] C. Demeniuk, S. Jih, and P. Green. In-vehicle traffic signal violation warnings: A review of the human factors literature. *(technical report UMTRI-2008-10), Ann Arbor, Michigan: University of Michigan Transportation Research Institute*, 2008.

[6] R. Ghaemi and D. Del Vecchio. Safety control of piece-wise continuous order preserving systems. In *Proc. of IEEE Conference on Decision and Control*, 2011.

[7] R. Ghaemi and D. Del Vecchio. Safety control of piece-wise continuous order preserving systems. *Proc. IEEE Conf. on Decision and Control*, 2011.

[8] S. Godha and M.E. Cannon. Integration of DGPS with a low cost MEMS-based inertial measurement unit (IMU) for land vehicle navigation application. In *Proceedings of ION GNSS*, Long Beach, CA, September 2005.

[9] P. Green, J. Schweitzer, M Alter, and C. Demeniuk. Traffic signal violation warnings: Driver interface development and an initial driving simulator evaluation. *Technical Report UMTRI-2008-11*, 2008.

[10] P. A. Green, J. M. Sullivan, O. Tsimhoni, J. Oberhotzer, M. L. Buonorasa, J. Devonshire, J. Schweitzer, E. Baragar, and J. R. Sayer. Integrated vehicle-based safety systems (IVBSS): Human factors and driver-vehicle interface summary report. *(technical Report UMTRI-2007-43), Ann Arbor, MI: University of Michigan Transportation Research Institute*, 2008.

[11] M. Hafner and D. Del Vecchio. Computation of safety control for uncertain piecewise continuous systems on a partial order. In *Conference on Decision and Control*, pages 1671 –1677, 2009.

[12] Michael R. Hafner and Domitilla Del Vecchio. Computational tools for the safety control of a class of piecewise continuous systems with imperfect information on a partial order. *SIAM Journal on Control and Optimization*, 49(6):2463–2493, 2011.

[13] J. K. Hedrick, Y. Chen, and S. Mahal. Optimized vehicle control/communication interaction in an automated highway system. *California Partners for Advanced Transit and Highways (PATH). Research Reports: Paper UCB-ITS-PRR-2001-29*, 2001.

[14] R. Horowitz and P. Varaiya. Control design of an automated highway system. *Proceedings of the IEEE*, 88(7):913–925, Jul 2000.

[15] P. Koopman. Critical embedded automotive networks. *Micro, IEEE*, 22(4):14 –18, july-aug. 2002.

[16] N. Matni and M. Oishi. Reachability analysis for continuous systems under shared control: Application to user-interface design. In *Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009. Proceedings of the 48th IEEE Conference on*, pages 5929 –5934, dec. 2009.

[17] F. Mussa-Ivaldi, A. Giszter, and E. Bizzi. Linear combination of primitives in vertebrate motor control. *PNAS USA*, 91:7534–7538, 1994.

[18] M. Oishi, I. Hwang, and C. Tomlin. Immediate observability of discrete event systems with application to user-interface design. In *Conf. on Decision and Control*, pages 2665 – 2672, 2003.

[19] P. Peti, R. Obermaisser, F. Tagliabo, A. Marino, and S. Cerchio. An integrated architecture for future car generations. In *Object-Oriented Real-Time Distributed Computing, 2005. ISORC 2005. Eighth IEEE International Symposium on*, pages 2 – 13, may 2005.

[20] J. Ploeg, B.T.M. Scheepers, E. van Nunen, N. van de Wouw, and H. Nijmeijer. Design and experimental evaluation of cooperative adaptive cruise control. In *Intelligent Transportation Systems (ITSC), 2011 14th International IEEE Conference on*, pages 260 –265, oct. 2011.

[21] A. Puri and P. Varaiya. Driving safely in smart cars. In *American Control Conference*, pages 3597–3599, Seattle, WA, 1995.

[22] R. Rajamani and C. Zhu. Semi-autonomous adaptive cruise control systems. *Vehicular Technology, IEEE Transactions on*, 51(5):1186 – 1192, sep 2002.

[23] J. R. Sayer, S. E. Bogard, M. L. Buonarosa, D. J. LeBlanc, S. D. Funkhouser, S. Bao, A. D. Blankespoor, and C. B. Winkler. Integrated vehicle-based safety systems light-vehicle field operational test, key findings report. *(University of Michigan Transportation Research Institute (UMTRI), Ann Arbor, MI. Sponsored by U.S. Department of Transportation, Research and Innovative Technology Administration, ITS Joint Program Office, Washington, D.C., January 2011. DOT HS 811 416, UMTRI-2010-21*, 2011.

[24] T. Suzuki. Advanced motion as a hybrid system. In *Electronics and Communications in Japan*, volume 93, pages 35–43, 2010.

[25] C. J. 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.

[26] Claire J. Tomlin, Ian Mitchell, Alexandre M. Bayen, and Meeko Oishi. Computational techniques for the verification and control of hybrid systems. In *PROCEEDINGS OF THE IEEE*, pages 986–1001, 2003.

[27] P. Varaiya. Smart cars on smart roads. *IEEE Transactions on Automatic Control*, 38(2):195–207, Feb 1993.

[28] R. Verma and D. Del Vecchio. Semiautonomous multivehicle safety: A hybrid control approach. *IEEE Robotics and Automation Magazine*, 18(3):44–54, 2011.

[29] R. Verma and D. Del Vecchio. Safety control of hidden mode hybrid systems. *Automatic Control, IEEE Transactions on*, 57(1):62 –77, jan. 2012.