UC Berkeley

Research Reports

Title

A Verified Hybrid Controller For Automated Vehicles

Permalink

<https://escholarship.org/uc/item/0345c547>

Authors

Lygeros, J.
Godbole, D. N.
Sastry, S.

Publication Date

1997

CALIFORNIA PATH PROGRAM
INSTITUTE OF TRANSPORTATION STUDIES
UNIVERSITY OF CALIFORNIA, BERKELEY

A Verified Hybrid Controller for Automated Vehicles

John Lygeros
Datta N. Godbole
Shankar Sastry

California PATH Research Report
UCB-ITS-PRR-97-9

This work was performed as part of the California PATH Program of the University of California, in cooperation with the State of California Business, Transportation, and Housing Agency, Department of Transportation; and the United States Department of Transportation, Federal Highway Administration.

The contents of this report reflect the views of the authors who are responsible for the facts and the accuracy of the data presented herein. The contents do not necessarily reflect the official views or policies of the State of California. This report does not constitute a standard, specification, or regulation.

February 1997

ISSN 1055-1425

A Verified Hybrid Controller for Automated Vehicles *

John Lygeros, Datta N. Godbole and Shankar Sastry

Intelligent Machines and Robotics Laboratory
University of California, Berkeley
Berkeley, CA 94720
lygeros, godbole, sastry@eecs.berkeley.edu

Abstract

In this paper, we design safe and efficient hybrid controller for an Automated Highway System (AHS) architecture based on platooning. AHS is an example of a large scale, multiagent, complex dynamical system which is ideally suited for design of a hierarchical hybrid controller. The objective of an AHS design is to increase the safety and throughput of highways by full or partial automation of the traffic. In an architecture developed by researchers of the California PATH project, a full automation scheme is proposed based on the concept of platooning. Here we apply the game theoretic design techniques developed in [1] to obtain hybrid controllers that guarantee safe and efficient operation thereby eliminating the need for verification. Even though the final theorems are specialized to the platooning concept the details of the calculations are general enough to apply to any vehicle control problem.

Keywords: Automated Highway Systems, Hybrid Systems, Safety, Verification, Optimal Control

*Research supported by the California PATH program, Institute of Transportation Studies, University of California, Berkeley, under MOU-238.

Executive Summary

The goal of MOU 238 is to develop analytical methods for design, analysis and verification of switched controllers for Automated Highway Systems. Because of the size and complexity of the AHS design task, hierarchical, hybrid controllers are needed; conventional continuous controllers to take care of the regulation of individual vehicles at a low level and discrete supervisors to provide coordination between vehicles at a higher level¹. In this report, we present a hybrid control scheme for low level regulation of automated vehicles. Our design makes use of the techniques introduced in [1]. In particular game theory is used to design continuous controllers and establish bounds on their performance. These bounds are then used as abstractions of the operation of the low level closed loop system in the design of the discrete switching scheme. This approach produces an overall control scheme that is by design guaranteed to be safe. The design process also provides considerable insight into the limitations of the physical system thereby allowing the designer to establish bounds on the expected performance and investigate other design alternatives.

In this report, we consider the AHS platooning architecture introduced in [2]. Considerable research has been carried out in terms of designing controllers for all levels of this hierarchy. We concentrate on the on-board control design problem for an automated vehicle. Each vehicle is equipped with a two layer on-board controller. The regulation (lower) layer is responsible for trajectory tracking and regulation of each vehicle. The coordination (higher) layer is responsible for the communication and coordination between agents. A design for the coordination layer is given in detail in [7]. The logical correctness of this design is verified in [7] under simplifying assumptions on the continuous dynamics of the vehicles and the regulation layer controllers. Here we apply the design methodology developed in [1] to complete the on-board controller design. We produce a regulation layer controller that guarantees safe, comfortable and efficient operation under minimal assumptions on the coordination layer. These assumptions that naturally emerge from the calculations are used as guidelines for forming an interface between the two layers and for tuning the coordination layer design.

According to this architecture of [2], traffic on the AHS is organized in platoons of close-following automated vehicles. Five maneuvers are needed to do this, namely, join, split, lane change, entry and exit. Decisions to initiate and abort maneuvers is taken by the coordination layer of the leader of each platoon. Such decisions are based on the commands received from the roadside controllers trying to maximize AHS throughput. We present methodology to design regulation layer controllers for each maneuver. We assume that the highway operates in normal mode, and that the lateral and platoon follower controllers operate perfectly. The design process also produces necessary conditions that if satisfied by the coordination layer before switching to a new maneuver guarantee safe operation. The individual controllers for each maneuver are combined together to produce a safe hybrid controller for platooning operation. The results we obtain depend only on the physical limitations of the vehicles and can therefore easily be extended to non-platooning AHS architectures as well.

¹Even at the low levels, switching controllers may be used [16] to satisfy multiple objectives such as safety, efficiency, passenger comfort, etc.

Contents

1	Introduction	1
2	The AHS control problem	1
2.1	The Platooning Concept	2
2.2	A Platooning Control Architecture	2
2.3	Overview of the AHS Research Effort	3
2.4	Mathematical Preliminaries	5
2.4.1	Game Theory	5
2.4.2	Optimal Control:	7
2.4.3	Hybrid Automata:	8
3	Problem Formulation	8
3.1	Discrete Level Abstraction	8
3.2	Hybrid Vehicle Model	9
3.2.1	Control Objectives	11
3.2.2	The “Leader” Mode	11
3.2.3	The “Follower” Mode	15
3.3	Design Requirements	16
3.4	Assumptions	17
4	Single Lane Safety Theorem	20
4.1	Background Lemmas	20
4.2	Safety Theorem	21
5	Multi Lane Safety Theorem	23
5.1	Background Lemmas	24
5.2	Safety Theorem	25
6	The Leader Control Law	26
6.1	Design for safety	26
6.1.1	Safe Set of Initial Conditions	30
6.1.2	The Class of Safe Controls	31
6.2	Design for comfort	32
6.3	Design for efficiency	33
6.4	Proof of the Leader Safety Lemma	33
7	The Join Control Law	34
7.1	Design for Safety	36
7.2	Numerical Investigation	39
7.3	Completing the Design	41
7.4	The Split Design	41
8	The Lane Change Laws	42

9	Key Points and Discussion	43
A	Simulation Plots	52

List of Figures

1	PATH Architecture	4
2	Automated Vehicle Operation	10
3	Vehicle Following	10
4	Hybrid Automaton for the Platoon Leader	14
5	Lane Change	24
6	Interface Design	27
7	Safe set of initial conditions for $x_3^0 = 20, 30$ and 40 meters	30
8	Controller Hybrid Automaton	34
9	Boundary of the safe set for $x_1^0 = 20ms^{-1}$	35
10	Minimum front sensor ranges for safe operation	47
11	State trajectory under maximum braking	52
12	Maximum braking by vehicle A, worst case d	53
13	State trajectory under the inputs of Figure 12	53
14	Saddle solution (u_0^*, d_0^*)	54
15	State trajectory under (u_0^*, d_0^*)	54

1 Introduction

Automated Highway Systems (AHS) have recently attracted attention as a possible solution to highway congestion problems. The goal of an AHS is to increase the throughput of an existing highway by fully or partially automating the operation of the vehicles.

Automated highways pose a very interesting and difficult control problem. Because of the size and complexity of the system, hierarchical, hybrid control schemes are needed, with conventional continuous controllers taking care of the regulation of individual vehicles at a low level and discrete supervisors providing coordination between vehicles at a higher level. In this paper we present a possible hybrid control scheme for low level regulation of automated vehicles. Our design makes use of the techniques introduced in [1]. In particular game theory is used to design continuous controllers and establish bounds on their performance. These bounds are then used as abstractions of the operation of the low level closed loop system in the design of the discrete switching scheme. The advantage of this approach is that the overall control scheme is by design guaranteed to be safe² under minimal assumptions on the physical plant. Another advantage is that the design process provides considerable insight into the limitations of the physical system. This allows the designer to establish bounds on the expected performance (that can be used as an abstraction of the low level controllers in throughput calculations) and investigate other design alternatives.

The paper is arranged in nine sections. In Section 2 we give a brief overview of the AHS control problem. We highlight the concept of platooning which forms the backbone of the control architecture [2] on which our work is based. We specify the role which the work presented here plays within this concept and give an overview of related work found in the literature. We also briefly introduce the mathematical tools used in the analysis. In Section 3 the problem that this paper addresses is formally posed. We describe the hybrid models used for the vehicles, formulate the design requirements and state the underlying assumptions. In Section 4 we state and prove the main safety theorem for a single lane highway. The theorem is extended to the multi-lane case in Section 5. Both safety theorems are based on a series of lemmas that establish the properties of the continuous controllers needed by the automated vehicles. These lemmas are proved in Sections 6, 7 and 8. In Section 9 we summarize the key points of our design and discuss possible design alternatives and modifications and their effect on the system performance.

2 The AHS control problem

Highway travel has become an indispensable part of everyday life. The current highway system is being pushed to the limit however, as the ever increasing congestion and the consequent delays testify. Studies indicate that this trend is unlikely to be reversed in the near future. Building new highways does not seem like a viable, long term solution to the problem, because of the prohibitively large cost of construction (especially in and near urban areas where real estate is expensive). One alternative is to improve the efficiency of current highways by automating their operation. The goal of such an automated highway system is to funnel more vehicles over the same piece of real estate.

²Also comfortable and efficient whenever safety is not at stake.

An underlying constraint in this process is safety. One would like to achieve increased throughput with at least the level of safety of current highways (in terms of accidents, injuries and vehicle damage per vehicle-mile traveled). At a first glance the demands for throughput and safety seem contradictory: enhanced safety requires large spacings and low speeds³, so that if needed the vehicles have enough time to stop before they collide, while enhanced throughput requires exactly the opposite, tight spacing and high speed. Clearly any acceptable AHS design should seek a compromise between these two opposing trends.

2.1 The Platooning Concept

The concept of platooning [3] offers such a compromise. Key to this concept is the observation that collisions are not dangerous (in terms of passenger injuries and hardware damage) unless there is a large velocity differential between the colliding vehicles [4]. A simple calculation shows that, in the presence of actuation and sensing delays, differences in deceleration capabilities etc., low relative velocity collisions can be guaranteed in two situations:

- If the vehicles are initially far apart, in which case they can come to a stop before they collide.
- If the vehicles are initially very close, in which case the collision happens almost instantaneously (and therefore the relative velocity is low).

The platooning concept is based on this observation. The vehicles travel in platoons, following each other very closely, with spacings of the order of 1 meter. Platoons are separated by large spacings, of the order of 60 meters. In addition to safety this large spacing guarantees that disturbances are attenuated as they propagate down a long string of platoons. This property of **string stability** is achieved within the platoon by communicating the state information of the first vehicle to all the vehicles in the platoon [5].

In terms of capacity, platooning clearly leads to an enormous improvement. “Static” calculations [6] indicate that, with reasonable size platoons, a fourfold increase in throughput can be expected over a manual driving scheme with the same level of safety. In practice the improvement will probably be less, due to the transient effects of forming and dissipating platoons, but it is still likely to be substantial. Unfortunately, human drivers are not fast and reliable enough to produce the steering, throttle and braking inputs required for such close following. Therefore fully automated vehicle operation is needed if the platooning concept is to be implemented.

2.2 A Platooning Control Architecture

Macroscopically, a fully automated highway is a control problem of gigantic proportions, with many thousands of interacting agents (vehicles) competing for the scarce highway space-time resource. The optimum policy for each agent (driving fast and weaving through traffic) does not coincide with the systemwide objective of increasing the productivity of the entire highway system. Although a centralized controller is capable of producing an optimal solution for the

³The safest highway is an empty highway.

highway system, it is clearly infeasible given the size and dynamically changing nature (vehicles entering and leaving the highway) of the system. Moreover, the calculations presented here will indicate that completely autonomous operation can not provide the guarantees necessary for safe formation of platoons. The problem is therefore ideally suited for a semiautonomous agent design. Such a design was proposed in [2]. Each vehicle is equipped with a two layer controller. The lower layer, called the **regulation layer** is responsible for trajectory tracking and regulation of each agent. The higher level, called the **coordination layer** is responsible for the communication and cooperation between the agents. A design for the coordination layer is given in detail in [7]. The logical correctness of the coordination layer design was verified in [7] under simplifying assumptions on the continuous dynamics of the vehicle and the regulation layer controllers. We will apply the design methodology developed in [1] to come up with a controller for the regulation layer that can guarantee safe, comfortable and efficient operation under minimal assumptions on the coordination layer. These assumptions that naturally emerge from the calculations will be used as guidelines for forming an interface between the two layers and tuning the coordination layer.

Our design methodology is primarily geared towards addressing the issue of safety. Even though the calculations can be used to quantify the tradeoff between safety and throughput, the throughput of the resulting highway system will not be investigated. Throughput maximization is a macroscopic issue, an emergent behavior of our design, and is difficult to quantify at the microscopic vehicle level considered here. In the control architecture proposed in [2], throughput maximization is the goal of two additional levels, called the **network layer** and the **link layer**. The overall control hierarchy is shown in Figure 1. The top two layers reside on the roadside, monitor the flow of traffic in entire sections of highway and broadcast commands to all the vehicles in the section. A number of designs have been proposed for the roadside controller, especially for the link layer. They make use of “fluid” flow models [8, 9], the concept of highway work [10] or the concept of highway space-time [11] to model the traffic. The coordination design of [7] takes into account the demands made by the higher layers, assuming they have been filtered by a suitable interface.

Summarizing, the controller presented here does not address the parsing of the requirements for increased throughput down the network, link and coordination layers. We will be concerned more with the impact of the throughput requirements on the regulation layer, the safety constraints that the latter imposes and the effect of these constraints on the coordination layer. The impact of these safety constraints on throughput is the topic of ongoing research.

2.3 Overview of the AHS Research Effort

The possibility of automating highway traffic has attracted attention for many years. A number of solutions have been proposed for this problem, involving various degrees of automation [12, 13, 2, 14, 15]. The platooning architecture considered here was introduced in [12, 2]. Since then, considerable research has been carried out for all the levels of the hierarchical controller. In the link and network layers controllers have been designed based on traffic flow models [8, 9], vehicle activity models [11] and highway work models [10]. At the coordination layer, a controller based on finite state machine communication protocols was designed and verified in [7]. Finally, at the regulation layer, controllers based on continuous vehicle models have

Figure 1: PATH Architecture

been designed to regulate the longitudinal motion both for the platoon leaders [13, 16, 14, 17] and for the platoon followers [5, 18, 19, 20]. For lateral vehicle motion controllers have been designed both for maintaining position in a lane [21] and for changing lanes [22]. Work at the physical layer on sensors [23, 24], actuators [25] and communication devices [26] has allowed researchers to investigate the performance of some of these controllers in experiments [5, 27].

The main concern in the design of most of these controllers has been safety. Here we focus on the safety issue from the point of view of the platoon leader. In particular we are concerned with safety problems that might arise by the hybrid interaction between the coordination and regulation layers. In [28], Godbole et.al. highlighted examples of such problems. The discussion in [28] was based on controllers designed in [16] for the various actions of the leader. These controllers were based on a third order, feedback linearizable model for the vehicle and were observed to perform well when simulated individually. However, when they were interfaced [29] with the coordination layer design of [7] and simulated in the SmartPath micro simulator [30] unsafe, high relative velocity collisions were observed under extreme traffic conditions. To remedy the situation, Frankel et.al. proposed leader mode controllers that explicitly incorporate safety considerations [31]. These controllers were based on a linear, second order vehicle model with actuation delay. Under the underlying assumption that the worst possible action of the preceding vehicle is to decelerate as fast as possible, it was shown that these controllers can guarantee low relative velocity collisions. In [32], Puri-Varaiya proposed to use optimal control to determine the worst possible action of the preceding

platoon, once a controller for the trailing platoon has been designed. The feasibility of the approach was illustrated by determining conditions under which the safety of some of the control laws designed in [16] can be guaranteed.

In [33], Lygeros et.al. introduced ideas from game theory to show that maximum deceleration by both leading and trailing vehicles is indeed a saddle solution, when the objective of the trailing vehicle is to avoid collision altogether⁴. The results of [33] were based on the third order model used in [16] and made no assumptions about the relative deceleration capabilities of the vehicles. The calculations were used to determine “safe” sets of initial conditions and classify the “safe” controllers. Using the second order with delay model, Li et.al. were able to show that maximum deceleration by both leading and trailing vehicles is also a saddle solution when the objective of the trailing vehicle is to minimize the relative velocity at impact [17]. The calculations were based on the assumption that the deceleration capability of all vehicles is uniform. In [17] complete control schemes were designed based on these results and their performance in terms of stability and safety was proved. In [34] the assumption that all vehicles have uniform deceleration capability was relaxed. For the third order vehicle model it was shown that maximum deceleration by both leading and trailing vehicles is not necessarily a saddle solution in this case; in fact the saddle solution may initially involve maximum acceleration of both the leading and the trailing vehicles.

Finally, in [35], the effect of collisions as a discrete disturbance to the system was introduced. Even though low relative velocity collisions were allowed by previous designs, their effect on the system dynamics was never investigated. While this omission is insignificant in the case of two vehicles, it may lead to catastrophic results in general, as it allows the relative velocity of collisions to increase geometrically down a long string of vehicles.

The work presented here is based on the results of [33, 34, 35]. The various elements are brought together and conditions on both the regulation and coordination layers are given under which safe operation of the AHS can be guaranteed. The analysis provides considerable insight into the physical restrictions of the system and suggests design modifications that can be used to improve the closed loop system performance.

2.4 Mathematical Preliminaries

The analysis presented in this paper will require concepts from the areas of game theory, optimal control and hybrid automata. Here we briefly introduce the necessary notions. We will also need some very basic concepts from dynamical systems and topology: invariant sets, interior and boundary of a set, induced topology of a subset, etc. These concepts are covered in any of the standard textbooks (e.g. [36, 37]).

2.4.1 Game Theory

We will be dealing the following type of two player, zero sum games:

Definition 1 *A two player, zero sum dynamic game involves:*

1. A time interval $[0, T]$.

⁴The design algorithm presented in [1] was also originally introduced in [33].

2. A trajectory space, $\mathcal{X}$ with some topological structure. The elements of $\mathcal{X}$, denoted $\{x(t), 0 \leq t \leq T\}$, are the permissible state trajectories of the game.
3. An input space, $\mathcal{U}$, with some topological structure. The elements of $\mathcal{U}$, denoted $\{u(t), 0 \leq t \leq T\}$, are the permissible inputs of player 1.
4. A disturbance space, $\mathcal{D}$, with some topological structure. The elements of $\mathcal{D}$, denoted $\{d(t), 0 \leq t \leq T\}$, are the permissible inputs of player 2.
5. A differential equation:

$$\dot{x}(t) = f(t, x(t), u(t), d(t)) \quad (1)$$

$$x(0) = x^0 \quad (2)$$

whose solution determines the state trajectory for a given selection of u and d .

6. A cost function:

$$J : \mathcal{X} \times \mathcal{U} \times \mathcal{D} \longrightarrow \mathbb{R}^+ \quad (3)$$

To be consistent with the notation we develop for the multiagent models we will give the following interpretation: the “reward” of player 1 for a given play is $-J(x, u, d)$ while the reward of player 2 is $J(x, u, d)$ (hence a zero sum game). In other words, player 1 is trying to minimize J while player 2 is trying to maximize it.

For our games we will assume the so called **closed-loop, perfect state** information structure. This means that, when called upon to decide their strategy at time t , both players have access to the entire state $\{x(s), 0 \leq s \leq t\}$ up to that point. For our purposes we will assume that $x(t) \in X \subset \mathbb{R}^n$, $u(t) \in U \subset \mathbb{R}^{n_i}$ and $d(t) \in D \subset \mathbb{R}^{n_d}$ for all $t \in [0, T]$ and some n, n_i and n_d . We will also assume that $\mathcal{X}$ will be a subset of the set of piecewise differentiable and $\mathcal{U}$ and $\mathcal{D}$ subsets of the set of piecewise continuous functions of t . Note that, if the differential equation 1 defines a unique state trajectory for a given choice of u and d , we can write the cost function as a function of the initial condition, rather than the whole state trajectory, i.e.

$$\begin{aligned} J : X \times \mathcal{U} \times \mathcal{D} &\longrightarrow R \\ (x^0, u, d) &\longmapsto J(x^0, u, d) \end{aligned}$$

We will be interested in saddle solutions to these games:

Definition 2 A **saddle solution** to the two player, zero sum game is a pair of input trajectories $(u^*, d^*) \in \mathcal{U} \times \mathcal{D}$ such that for any $u \in \mathcal{U}$ and any $d \in \mathcal{D}$:

$$J(x^0, u^*, d) \leq J(x^0, u^*, d^*) \leq J(x^0, u, d^*)$$

In other words, a saddle solution will be such that any unilateral deviation from it will leave the player who decided to deviate worse off. The games considered in this paper will turn out to have unique saddle solutions. Existence and uniqueness of solutions can not be guaranteed for general games, however. For results in this direction the reader is referred to [38, 39, 40].

2.4.2 Optimal Control:

Our analysis also makes use of the **Maximum Principle**. The following statement comes from [41], with a slight modification in notation. Given the dynamical system:

$$\dot{x} = f(x, u)$$

Consider the problem of steering it, using a piecewise continuous $u(t)$, from the point P at time t_1 to the point Q at time t_2 along a trajectory that minimizes:

$$J(x_0, u) = \int_{t_1}^{t_2} L(x, u) dt$$

Theorem 1 ⁵ *A necessary condition for a trajectory $x(t)$ and the corresponding control $u(t)$, $0 \leq t \leq T$ to be optimal is that there exist a constant $p_0 \leq 0$ and a vector valued, piecewise continuously differentiable function $p(t)$ such that:*

1. $p(t)$ and p_0 not both 0 for any t
2. At $(t, x(t), p(t), p_0)$, the function of u :

$$\tilde{H}(x, p, p_0, u) = p_0 L + p' f$$

assumes its maximum, $H(t, x, p, p_0)$, for $u = u(t)$.

3. For the arguments $t, x(t), p(t), p_0, u(t)$ the Euler equations hold:

$$\dot{x} = \frac{\partial \tilde{H}}{\partial p} \quad \dot{p} = -\frac{\partial \tilde{H}}{\partial x}$$

4. The end points satisfy the transversality condition:

$$[p \delta x - H \delta t]_P^Q = 0$$

In our vehicle problem, the initial point $P = x^0$ and time $t_1 = 0$ are fixed. The final point and time can vary, but are restricted to correspond to the first collision. In other words, $x(t_2) \in \Pi$ where Π is the hyperplane corresponding to $x_3 = 0$. In this setting the last condition of the theorem becomes:

$$H = 0 \text{ at time } T \tag{4}$$

$$p(t_2) \perp \Pi \tag{5}$$

⁵In fact the theorem holds under more general conditions (e.g. time varying dynamics) but this version is sufficient for our problem.

2.4.3 Hybrid Automata:

We will only need an informal treatment of hybrid automata. For precise definitions the reader is referred to [42, 43]. For a formalism customized to automated highway systems see [44].

A hybrid automaton, H , will be a dynamical system, with a set of states and relations that determine the transitions between them. We will follow the hybrid automaton model described in [1]. The state of a hybrid automaton is a tuple $(q, x) \in Q_H \times \mathbb{R}^{n_H}$, where Q_H is a finite set of discrete states and x a set of continuous state variables. In each discrete state the continuous state evolves according to a set of differential equations⁶. The discrete state evolves according to a transition graph defined by a finite state machine. An edge between discrete states is labeled by an *event*, a *guard* and a *reset*. A guard is a boolean expression on predicates defined on the continuous variables $x(t)$. An edge may be taken only if the guard is true. Upon execution of the edge, the continuous state is reinitialized using the reset action, which assigns a new value to the state as a function of x at the time of transition. The events can be used for synchronization. When two hybrid automata share an event the corresponding edges must be executed synchronously (provided they are both enabled). Roughly speaking, the parallel composition of a collection of hybrid automata, $\{H_i\}_{i=1}^N$, will be a new automaton with state space:

$$Q_{H_1} \times \dots \times Q_{H_N} \times \mathbb{R}^{n_{H_1}} \times \dots \times \mathbb{R}^{n_{H_N}}$$

and the appropriate edges synchronized.

To simplify the figures somewhat we will occasionally omit events, guards or resets from the transitions. The interpretation is that a missing guard is always true and a missing reset is the identity.

3 Problem Formulation

3.1 Discrete Level Abstraction

In the platooning concept a vehicle on the automated highway operates either as a *leader* of a platoon, a *follower* within a platoon or a *free agent* (one vehicle platoon). The discussion of Section 2.1 indicates that two distinct modes of operation can be distinguished: the **follower mode** and the **leader mode** (a free agent is a special case of a leader). These two modes differ in their set points (small vs. large spacing) and the information available for feedback control (sensory data as well as information propagated through communication vs. only sensory information). In particular, in the leader mode, we assume that a vehicle is equipped with sensors to measure its own velocity and acceleration, as well as the relative position and velocity with respect to the vehicle ahead. The follower mode, on the other hand, assumes that infrared communication devices are used to provide measurements of the acceleration of the preceding vehicle and the state of the leader of the platoon (if other than the preceding vehicle), in addition to the information provided by the sensors. The two modes can be thought of as a form of “discrete” state of the automated vehicle. Another discrete aspect of the vehicle state is the lane it is in. Assume that the automated lanes are indexed by numbers, increasing from right to left, with 1 representing the right most lane and let lane number 0 denote the

⁶Or, more generally differential inclusions.

situation where the vehicle is off the AHS. Then the discrete state of an automated vehicle can be summarized at any time by a pair:

$$(\text{mode}, \text{lane})$$

with $\text{mode} \in \{\text{leader}, \text{follower}\}$ and $\text{lane} = 0, 1, \dots$ ⁷. This is a somewhat coarse description of the discrete state of the vehicle (for example we do not keep track of the exact position of a vehicle in the platoon), it will however be sufficient for our purposes.

Transitions between the discrete states are achieved by means of five maneuvers: **join**, **split**, **lane change**, **entry** and **exit**. The join maneuver is used to join two platoons in the single lane to form a bigger platoon. The trailing platoon accelerates to catch up with the leading platoon. The split maneuver is used to break a platoon into two smaller platoons. The trailing platoon decelerates to safe inter-platoon distance. The lane change maneuver is used to move a vehicle from one lane to another. The entry and exit maneuvers can be considered as a special case of lane change maneuver that allow the vehicle to get on/off the automated highway. In [7] communication protocols were designed to implement these maneuvers. Some assumptions were made to simplify the design process: a platoon can only be engaged in one maneuver at a time⁸ (in particular all maneuvers are coordinated by the leader) and only free agents can change lane, enter and exit. The logical correctness of the proposed protocols (i.e. their effectiveness as transitions between the discrete states) was verified in [7] using automatic verification tools. The verification was based on simplifying assumptions about the behavior of the continuous state of the vehicles. Here we refine these assumptions and determine if and how they can be met.

The evolution of the discrete state of an automated vehicle can be represented by the automaton of Figure 2. Our goal here is to design control laws for tracking the set points and for executing the maneuvers such that the overall AHS is safe.

3.2 Hybrid Vehicle Model

Consider three vehicles (labeled A, B and C) moving along a single lane highway (Figure 3)⁹. We will primarily be interested in the interaction between vehicles A and B, vehicle C will be used only in certain cases, to isolate the system A-B from the rest of the highway. Assume that vehicles A and B have lengths L_A and L_B and let x_A and x_B denote their positions with respect to a fixed reference on the road. Assume that vehicle B is leading while vehicle C comes last, i.e. $x_B > x_A > x_C > 0$. The problem we are interested in is the vehicle following problem: we assume no control over vehicle B and try to control vehicle A.

The dynamics of the trailing vehicle will be approximated by a third order ordinary differential equation:

$$\ddot{x}_A = b_A(\dot{x}_A, \ddot{x}_A) + a_A(\dot{x}_A)v_A$$

⁷Even though this is in theory an infinite state space, in practice there are a finite number of discrete states as the number of lanes is finite.

⁸By definition all cooperating platoons are engaged in the maneuver. For example while one platoon joins another they are both engaged in a join maneuver. Similarly a lane change may involve (in addition to the vehicle changing lane) vehicles in the target lane, as well as two lanes away.

⁹Under the assumptions of Sections 3.4, A, B and C can in fact be entire platoons.

Figure 2: Automated Vehicle Operation

Figure 3: Vehicle Following

a_A and b_A are complicated nonlinear functions of the state with $a_A(\dot{x}_A) \neq 0$. The first two derivatives on x_A arise from the laws of motion. The third has to do with the operation of the brakes and engine, which can be modeled by the throttle and brake angles acting through an integrator on some nonlinear dynamics (involving engine time constants, aerodynamic drag, etc.) [5, 25]. For our purposes the details of the nonlinear functions b_A and a_A are not important. Following the design of [16], we will assume that feedback linearization has already been carried out, i.e. input:

$$v_A(t) = \frac{-b_A(\dot{x}_A, \ddot{x}_A) + u}{a_A(\dot{x}_A)} \quad (6)$$

$$(7)$$

has been applied to yield:

$$\ddot{\ddot{x}}_A = u \quad (8)$$

We will design controllers for the resulting linear dynamics. We assume that the dynamics are constrained by the engine, tire and road conditions. More specifically it is required that:

$$\dot{x}_A \in [v_{min}^A, v_{max}^A]$$

$$\begin{aligned}\ddot{x}_A &\in [a_{min}^A, a_{max}^A] \\ u(t) &\in [j_{min}, j_{max}]\end{aligned}$$

For highway operation it is assumed that vehicles will not be allowed to go backwards, therefore $v_{min}^A = 0$ will be used. v_{max}^A is imposed by engine limitations. One of the objectives of the controllers we design will be fuel efficiency. As a consequence the engine will not have to be pushed to its limits for maximum speed and therefore v_{max}^A will not feature in the safety calculations. We will assume $v_{max}^A = \infty$ to simplify the analysis. Typical values of a_{min}^A , etc. can be found in [35].

3.2.1 Control Objectives

The objective is to design a controller for vehicle A. The requirements we impose on the design are safety, passenger comfort and efficiency. It is assumed that safety takes precedence over the other two requirements. Comfort will be assumed to be more important than efficiency. Quantitative definitions of these design requirements will be given in Section 3.3.

3.2.2 The “Leader” Mode

In the leader mode we can abstract the behavior of vehicle B by treating its (unmeasured) acceleration as a disturbance. Both the design specifications and the system dynamics are independent of the absolute vehicle position. To remove the absolute position from the problem we introduce a new variable to measure the spacing between vehicles A and B:

$$D = x_B - x_A - L_B$$

All pertinent information can now be encoded by the state vector:

$$x = \begin{bmatrix} \dot{x}_A \\ \ddot{x}_A \\ D \\ \dot{D} \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \in \mathbb{R}^4$$

From Section 3.2 the state dynamics are:

$$\begin{aligned}\dot{x} &= \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 \end{bmatrix} x + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} u + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \ddot{x}_B \\ &= Ax + Bu + D\ddot{x}_B \\ x(0) &= x^0\end{aligned}\tag{9}$$

For the vehicle following problem we are interested in regulating the spacing and relative velocity to a desired fixed point. In addition, whenever possible, a vehicle may be required to track a certain velocity, v_H , calculated by the roadside controllers in order to maximize

throughput. These requirements can be encoded by means of three outputs:

$$\begin{aligned} y &= \begin{bmatrix} D \\ \dot{D} \\ \dot{x}_A \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} x \\ &= Cx \end{aligned}$$

Note that the assumed sensor arrangement can provide full state measurements.

To complete the picture we also need to encode the constraints in the new coordinates. From the discussion in Section 3.2 it is required that, for all t :

$$\begin{aligned} x(t) \in \mathbf{X}_C &= \{x \in \mathbb{R}^4 | x_1 \in [v_{min}^A, v_{max}^A], x_2 \in [a_{min}^A, a_{max}^A], x_4 + x_1 \in [v_{min}^B, v_{max}^B]\} \\ u(t) \in \mathbf{U} &= [j_{min}, j_{max}] \\ \ddot{x}_B(t) \in \mathbf{D} &= [a_{min}^B, a_{max}^B] \end{aligned}$$

The analysis can be greatly simplified if the input constraints are modified somewhat to guarantee that the state constraints are satisfied. We will assume that:

$$u(t) \in [u_{min}(x(t)), u_{max}(x(t))] = \begin{cases} [j_{min}, j_{max}] & \text{if } x_2(t) \in (a_{min}^A, a_{max}^A) \\ [0, j_{max}] & \text{if } x_2(t) = a_{min}^A \\ [j_{min}, 0] & \text{if } x_2(t) = a_{max}^A \end{cases} \quad (10)$$

$$\ddot{x}_B(t) \in [d_{min}(x(t)), d_{max}(x(t))] = \begin{cases} [a_{min}^B, a_{max}^B] & \text{if } x_4(t) + x_1(t) \in (v_{min}^B, v_{max}^B) \\ [0, a_{max}^B] & \text{if } x_4(t) + x_1(t) = v_{min}^B \\ [a_{min}^B, 0] & \text{if } x_4(t) + x_1(t) = v_{max}^B \end{cases} \quad (11)$$

This will ensure that the constraints on x_2 and $x_1 + x_4$ will never be violated if $x^0 \in \mathbf{X}_C$.

The only state constraint that we have to worry about is $x_1 \in [v_{min}^A, v_{max}^A]$. For the reasons discussed above we will not be concerned with the upper bound too much. We can work around the lower bound by assuming that $\ddot{x}_A = x_2$ becomes zero when $x_1 = v_{min}^A$ is reached (note that when x_1 reaches v_{min}^A , $x_2 \leq 0$). This modification will not have a drastic effect on our analysis. The reason is that, what happens after x_1 reaches $v_{min}^A = 0$ is not very important, at least from the safety point of view. Recall that the constraint (11) guarantees that $x_B \geq v_{min}^B = 0$. Therefore, if no collision occurs until $x_1 = 0$, none is going to occur from then on, unless vehicle A starts accelerating again.

There are four kinds of exogenous inputs that influence the system evolution:

1. the jerk input of vehicle A, $u(t)$,
2. the trajectory of $\ddot{x}_B(t)$,
3. collisions of vehicle B with its preceding vehicle (that affect $\dot{x}_B(t)$ and hence x_4),
4. collisions of vehicle A with vehicle C (that affect x_1 and hence x_4).

$u(t)$ is assumed to be under the control of the designer. The remaining inputs, however, will have to be treated as disturbances to be guarded against. The acceleration disturbance $\ddot{x}_B(t)$ can be modeled as a piecewise continuous function of time:

$$\ddot{x}_B : [0, \infty) \longrightarrow [d_{min}, d_{max}]$$

In the hybrid automaton terminology this is a *continuous disturbance*. The collision disturbances on the other hand can be modeled by an instantaneous jump in the state of the system. Assuming that the vehicle collisions are elastic, a collision of vehicle B with the vehicle in front of it at time T_B with relative velocity δv_B will result in a reset of the state:

$$x_4(T'_B) := x_4(T_B) + \delta v_B$$

Similarly an elastic collision between vehicles A and C at time T_C and with relative velocity δv_C will result in a reset of the state¹⁰:

$$\begin{aligned} x_1(T'_C) &:= x_1(T_C) - \delta v_C \\ x_4(T'_C) &:= x_4(T_C) + \delta v_C \end{aligned}$$

This model will be quite accurate if the relative velocity at impact is low, in which case the collision is more or less elastic [45]. We will assume that the relative velocity of all collisions is bounded in an interval $[v_a, 0]$. In hybrid system terminology the collisions are *discrete disturbances*.

To model the general situation assume that vehicle B experiences n_B collisions and that the i^{th} collision takes place at T_{B_i} with relative velocity δv_{B_i} (similarly for vehicle C). Then the overall disturbance experienced by vehicle A can be encoded by:

$$d = \{\ddot{x}_B, \{T_{B_i}, \delta v_{B_i}\}_{i=1}^{n_B} \{T_{C_i}, \delta v_{C_i}\}_{i=1}^{n_C}\} \quad (12)$$

Physical considerations restrict the set of allowable disturbances. In particular:

$$\begin{aligned} d \in \mathcal{D} = \{d \mid & \ddot{x}_B(t) \in [d_{min}, d_{max}], \\ & 0 \leq T_{B_1} \leq T_{B_2} \leq \dots, \\ & \delta v_{B_i} \in [v_a, 0] \text{ for all } i, \\ & 0 \leq T_{C_1} \leq T_{C_2} \leq \dots, \\ & \delta v_{C_i} \in [v_a, 0] \text{ for all } i\} \end{aligned}$$

In the ensuing discussion we will be interested in situations where vehicle B and vehicle C can experience at most one collision ($n_C = n_B = 1$). To remove some of the indices we will use T_B and T_C to denote the collision times in this case. The requirement that vehicle B does not go backward after the collision can be encoded by restricting the set of allowable disturbances:

$$\begin{aligned} \mathcal{D} = \{d \mid & \ddot{x}_B(t) \in [d_{min}, d_{max}], \\ & 0 \leq T_B, \delta v_B \in [\max\{v_a, x_4(T_B) + x_1(T_B)\}, 0] \\ & 0 \leq T_C, \delta v_C \in [v_a, 0]\} \end{aligned} \quad (13)$$

Collisions between vehicles C and A can not lead to a violation of the state constraints, since we assume $v_{max}^A = \infty$. By abuse of notation we will use the same representation when vehicles B and C experience no collision. We will simply assume that $\delta v_B = \delta v_C = 0$.

¹⁰Note that in the coordinate system defined above, the collisions imply that $\delta v_B \leq 0$ and $\delta v_C \leq 0$.

Figure 4: Hybrid Automaton for the Platoon Leader

Under these assumptions, the leader evolution is determined by a hybrid dynamical system. It is shown pictorially in Figure 4. The discrete state can take one of five values, *00*, *01*, *10*, *11* and *CRASH*. The first four keep track of whether vehicles B and C have experienced a collision (1) or not (0). The discrete state *CRASH* is introduced to model the situation where vehicle A crashes into vehicle B. It will be used to translate the safety problem into a reachability question on hybrid automata. There are six continuous states, two keeping track of when the collision occurred and four keeping track of the state of vehicle A. The initial conditions, node invariants, transition guards, events and reset maps should be obvious from the figure. The automaton runs can be obtained using the variation of constants formula [46]. Define the step function:

$$1_T(t) = \begin{cases} 0 & \text{if } t < T \\ 1 & \text{if } t \geq T \end{cases}$$

Then:

$$\begin{aligned}
x(t) = e^{At}x^0 &+ \int_0^t e^{A(t-\tau)}Bu(\tau)d\tau + \int_0^t e^{A(t-\tau)}D\ddot{x}_B(\tau)d\tau \\
&+ \begin{bmatrix} 0 \\ 0 \\ t - T_B \\ 1 \end{bmatrix} 1_{T_B}(t)\delta v_B + \begin{bmatrix} -1 \\ 0 \\ t - T_C \\ 1 \end{bmatrix} 1_{T_C}(t)\delta v_C
\end{aligned}$$

Using the fact that A is nilpotent ($A^3 = 0$) we obtain:

$$e^{At} = \begin{bmatrix} 1 & t & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -t^2/2 & 1 & t \\ 0 & -t & 0 & 1 \end{bmatrix}$$

This leads to:

$$\begin{aligned}
x(t) = & \begin{bmatrix} x_1^0 + tx_2^0 \\ x_2^0 \\ -t^2x_2^0/2 + x_3^0 + tx_4^0 \\ -tx_2^0 + x_4^0 \end{bmatrix} + \int_0^t \begin{bmatrix} t - \tau \\ 1 \\ -(t - \tau)^2/2 \\ -t + \tau \end{bmatrix} u(\tau)d\tau \\
& + \int_0^t \begin{bmatrix} 0 \\ 0 \\ t - \tau \\ 1 \end{bmatrix} \ddot{x}_B(\tau)d\tau + \begin{bmatrix} 0 \\ 0 \\ t - T_B \\ 1 \end{bmatrix} 1_{T_B}(t)\delta v_B + \begin{bmatrix} -1 \\ 0 \\ t - T_C \\ 1 \end{bmatrix} 1_{T_C}(t)\delta v_C
\end{aligned}$$

3.2.3 The “Follower” Mode

The objective of the followers of a platoon is to maintain a small constant separation (independent of vehicle speed) from the preceding vehicle. The design of feedback control laws for safe follower operation has received considerable attention in recent years [5, 47]. There are three problems that make the design particularly challenging. The more obvious one is regulating to the follower fixed spacing (typically 1 meter) without crashing into the preceding vehicle. In [5] it was shown that, in order to achieve this objective, the vehicle controller needs information about the acceleration of the preceding vehicle. Unlike the spacing and relative velocity information, preceding vehicle acceleration is not readily available through sensors and will have to be obtained through intervehicle communications. Because of the tight spacings communication between adjacent followers can easily be established by a point-to-point infrared link.

The second problem associated with follower operation is attenuation of disturbances along the platoon. Unless special care is taken during the design, a small disturbance of the platoon leader (e.g. a transient change in velocity) may get amplified as it propagates from one follower to the next, possibly resulting in collisions down the string. In [5] it was shown that, in order to avoid this “slinky effect”, followers need information about the state of the platoon leader in addition to the information about the vehicle immediately ahead of them. Because the accumulated delays caused by point-to-point communication increase with the

size of the platoon, the leader information may have to be broadcast by the leader (using a radio link for example).

Finally, in [5] it was also shown that, under the information structure dictated by the previous observations, the control law will invariably result in amplification of the control effort exerted by followers further down the platoon. This fact imposes restrictions on the operation of the leader. For example, assume that the braking force is amplified by at most a factor of $\gamma \geq 1$, in a platoon of identical vehicles with deceleration capability a_{min} . Then the maximum deceleration of the lead vehicle should be $\frac{a_{min}}{\gamma}$ in order to avoid actuator saturation and the possibility of collisions within the platoon. This figure should be used as a deceleration constraint on the leader of the platoon, rather than a_{min} itself.

The above discussion indicates that the information structure required for safe operation within a platoon is very different from the one for the platoon leader. Here we will concentrate primarily on the leader operation. We will avoid dealing with the complications of the follower design by introducing the assumption that the follower operation is always safe (Assumption 7). The ensuing discussion will provide some justification for this assumption. For more details the reader is referred to [5].

3.3 Design Requirements

In the leader mode the problem can be viewed as a two player zero sum game, one player being the action of vehicle A and the other the disturbances (action of vehicle B and possible collisions). The two players compete over a number of cost functions, J_i , encoding various desirable properties of the system. All cost functions will be independent of the discrete state of the system ($q \in \{00, 01, 10, 11, CRASH\}$), therefore only the continuous state, x , will appear in the expressions.

1. Safety (No Collision):

$$J_1(x^0, u, d) = -\inf_{t \geq 0} x_3(t) \quad (14)$$

A safe maneuver is one where:

$$J_1(x^0, u, d) \leq C_1 = 0 \text{ m}$$

Allowing $J_1 = 0$ meters makes the limiting case (where the vehicles just touch with zero relative velocity) acceptable.

2. Safety (Low Relative Velocity Collision): Assume vehicles A and B collide at time T .

$$J'_1(x^0, u, d) = |x_4(T)| \quad (15)$$

A safe collision is one where the relative velocity is less than a certain threshold:

$$J'_1(x^0, u, d) \leq C'_1 = -v_a$$

In the subsequent analysis $v_a = -3ms^{-1}$ will be used.

3. Comfort (Bounded Jerk):

$$J_2(x^0, u, d) = \sup_{t \geq 0} |u(t)| \quad (16)$$

A comfortable maneuver is one where:

$$J_2(x^0, u, d) \leq C_2$$

The value $C_2 = 2.5ms^{-3}$ is suggested in the transportation studies literature.

4. Efficiency (Fast Convergence):

$$J_3(x^0, u, d) = \int_0^\infty (y(\tau) - y_d)^T P (y(\tau) - y_d) d\tau \quad (17)$$

where y_d is the desired fixed point for a given maneuver and $P \geq 0$. The fixed points and the choice of P will depend on the maneuver in question. For steady state leader operation and for the split maneuver, the fixed point is:

$$y_d^L = \begin{bmatrix} \lambda_v v_H + \lambda_p \\ 0 \\ v_H \end{bmatrix}$$

for some $\lambda_v, \lambda_p > 0$ (refer to [16]). For the join maneuver on the other hand the fixed point is:

$$y_d^J = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

with P having zeros in its third row and column. This reflects the fact that tracking the optimum velocity v_H is not important for the join maneuver, the objective is to catch up with the platoon ahead. Other cost functions may be used to encode efficiency, for example, convergence in minimum time. The choice will not influence the safety of the design.

The discussion of Section 3.2.3 indicates that, for the follower mode, the problem is harder to formulate as a two person game, as the lead vehicle information should also be taken into account. However, the design requirements on the control laws can still be expressed by similar cost functions.

3.4 Assumptions

The basic underlying assumption is what constitutes a “safe” system. Ideally we would like no collisions to occur on the AHS, under normal operation. Our analysis will indicate that this requirement may be too restrictive in terms of efficiency, as it does not allow platoons to join or break up. Previous studies (Hitchcock [4]) indicate that collisions with small relative velocities are not likely to result in serious damage. We will therefore assume that:

Assumption 1 (Low Relative Velocity Collisions) *Collisions between vehicles of comparable masses with relative velocity smaller than a threshold v_a will not result in structural or functional damage to the vehicles or injury to the passengers.*

Assumption 1 motivates the following definition:

Definition 3 *A **safe collision** between two vehicles is one where the relative velocity at impact is less than v_a . An Automated Highway System where vehicles experience only safe collisions will be called a **safe AHS**.*

Motivated by the analysis of [4] we will use $v_a = -3ms^{-1}$ in the calculations.

Producing a completely safe AHS design is likely to be impossible, as one can not exclude the occurrence of combinations of faults that may cause unsafe collisions at any moment (for examples see [48]). The following assumption is therefore crucial to proving safety:

Assumption 2 (Normal Mode AHS Operation) *Operation on the AHS is “normal”: no faults occur and the environmental conditions are benign.*

By assuming normal conditions we exclude hardware and software faults and adverse environmental conditions (such as snow) that limit the capabilities of the system. As a consequence of Assumption 2:

- The boundaries of sensor and actuator ranges (e.g. a_{min}^A , etc.) can be assumed to be feasible.
- Vehicles do not exhibit “abnormal” or “erratic” behavior, for example, do not change lane without warning due to a tire burst.

Our analysis can be extended to a more “fault tolerant” design [49], if appropriate extensions to the definitions of safety are given [48]. Refer to [35] for details.

Assumption 3 (Known Model) *All vehicle model parameters are known.*

This implies that linearization by state feedback (equation 8) is feasible. Assumption 3 can be relaxed by an adaptive or robust design. Refer to [5] for design of an adaptive controller for the case of followers in a platoon.

Assumption 4 (Perfect Sensors) *Sensors can be used to provide noiseless, continuous measurements of velocity and acceleration of the vehicle in question as well as distance and relative velocity with respect to the vehicle in front and in the adjacent lanes.*

A consequence of Assumption 4 is that the leader mode controllers can utilize full state feedback (without making use of an observer). We assume that the sensor ranges are limited. The limits (see [35]) and the analysis presented here can be used to infer limitations on the AHS operation dictated by safety (e.g. limits on the speed of travel). These issues are discussed further in Section 9.

Assumption 5 (Elastic Collisions) *Collisions are instantaneous, perfectly elastic and all vehicles have equal masses.*

This assumption is clearly unrealistic. Assuming perfectly elastic collisions is not unreasonable for low relative velocity collisions [45]. The assumption that all vehicles have equal mass can easily be relaxed. Assumption 5 leads to:

Fact 1 *Under Assumption 5, a collision with relative velocity at most v_a induces an instantaneous change in velocity of at most v_a in the colliding vehicles.*

Fact 1 allows us to model collisions as instantaneous changes in velocity as required by the hybrid vehicle model. It will be needed as an implicit assumption in the proofs of the subsequent lemmas.

Assumption 6 (Perfect Lateral Control) *Lateral operation is perfect*

This assumption is not too unrealistic, as both simulation and experimental results indicate [50, 22]. If needed, the techniques presented here can easily be used to modify the lateral design and/or obtain limits of guaranteed performance.

As discussed in Section 3.2.3, designing control laws for the followers is a lot more complicated than for the leaders. The additional complication arises mostly because of the extra information that is available to the follower in a platoon and that is needed for safe operation. Fitting the follower scenario in this framework is the topic of ongoing research. Here we will bypass the problem by introducing an additional assumption. We will assume that a follower control law, u_F , a safe set of initial conditions in the follower state space, V_F , and a time, T_F (possibly dependent on the size of the platoon) have been determined, such that:

Assumption 7 (Platoon String Stability under Front/Rear Collision) *If u_F is applied by all followers in a platoon during an interval $[t_i, t_f)$ with $t_i < t_f$ and:*

1. *The acceleration of the leader is bounded in the interval $[d_{min}, d_{max}]$, for all $t \in [t_i, t_f)$,*
2. *either the leader or the last vehicle of the platoon experiences at most one collision in $[t_i, t_f)$, with relative velocity at most v_a ,*
3. *The state of all followers is in V_F at time t_i ,*

then any collisions between vehicles in the platoon will be with relative velocity at most v_a . Moreover, no further collisions will take place T_F seconds after the first collision.

Note that this assumption allows us to mostly ignore the internal dynamics of the platoon. As a consequence we will collapse the platoons for the purposes of safety and assume that they are all one vehicle long. The work of [5, 45] leads us to believe that this is not an unrealistic assumption. We are currently working on modifying the follower design to fit it in this framework and subsequently prove Assumption 7 as a theorem. It seems likely that information about the last vehicle will need to be propagated to all vehicles in the platoon to guarantee Assumption 7.

Finally we introduce one more assumption relating to the follower operation:

Assumption 8 (Join/Split Termination) *After a safe collision, follower operation can be established between the colliding vehicles.*

This assumption is essentially a “corollary” of Assumption 7. If Assumption 7 holds, the initial condition resulting from a safe collision should be within the safe set for follower operation. Moreover, at impact the spacing is definitely small enough to establish communication.

4 Single Lane Safety Theorem

We will start by proposing a design for the discrete part of the hybrid control scheme and proving that it guarantees safe operation. The proof will be based on a series of lemmas concerning the continuous part of the hybrid control scheme. In subsequent sections we will derive conditions on the continuous controllers which guarantee that the lemmas indeed hold and provide possible designs that satisfy these conditions. The lemmas require the underlying Assumptions 2–6 (not all assumptions are needed by all the lemmas though). The proofs are given in Sections 6 and 7.

4.1 Background Lemmas

Leader law: In Section 6 a continuous control law, u_L , will be designed for a leader of a platoon. The design process will also establish a “safe” set of initial conditions, V_L :

$$V_L = \{x^0 \in \mathbf{X}_C | J_1(x^0, u_L, d) \leq C_1\}$$

for all d . For this pair, (u_L, V_L) , we will show that:

Lemma 1 (Leader Safety Lemma) *Assume that u_L is applied during an interval $[t_i, t_f]$ with $t_i < t_f$ and that:*

1. $\ddot{x}_B(t) \in [d_{min}, d_{max}]$, for all $t \in [t_i, t_f]$,
2. B experiences at most one collision in $[t_i, t_f]$, with relative velocity at most v_a ,
3. Vehicles C and A collide at most once in $[t_i, t_f]$, with relative velocity at most v_a ,
4. $x^0 = x(t_i) \in V_L$.

Then vehicles A and B will not collide in $[t_i, t_f]$. Moreover there exists a finite time T_L such that if x leaves V_L at time t , it is guaranteed to return to V_L by at most $t + T_L$.

Join and Split laws: In Section 7 the design of control laws for the leader of a platoon joining (u_J) and splitting (u_S) from the platoon ahead will be outlined. The design process will also produce “safe” sets of initial conditions, V_J and V_S for the two maneuvers:

$$\begin{aligned} V_J &= \{x^0 \in \mathbf{X}_C | J'_1(x^0, u_J, d) \leq C'_1\} \\ V_S &= \{x^0 \in \mathbf{X}_C | J'_1(x^0, u_S, d) \leq C'_1\} \end{aligned}$$

for all d . It will be shown that:

Lemma 2 (Join Safety Lemma) Assume that u_J is applied during an interval $[t_i, t_f)$ with $t_i < t_f$ and that:

1. $\ddot{x}_B(t) \in [d_{min}, d_{max}]$, for all $t \in [t_i, t_f)$,
2. B does not experience a collision in $[t_i, t_f)$,
3. Vehicles C and A do not collide in $[t_i, t_f)$,
4. $x^0 = x(t_i) \in V_J$.

Then vehicles A and B may collide at most once during $[t_i, t_f)$, with relative velocity at most v_a .

Lemma 3 (Split Safety Lemma) Assume that u_S is applied during an interval $[t_i, t_f)$ with $t_i < t_f$ and that:

1. $\ddot{x}_B(t) \in [d_{min}, d_{max}]$, for all $t \in [t_i, t_f)$,
2. B does not experience a collision in $[t_i, t_f)$,
3. Vehicles C and A do not collide in $[t_i, t_f)$,
4. $x^0 = x(t_i) \in V_S$.

Then vehicles A and B may collide at most once during $[t_i, t_f)$, with relative velocity at most v_a .

The calculations will indicate that, without loss of generality, $t_i = 0$ can be used in all the lemmas.

4.2 Safety Theorem

The following theorem states conditions on the discrete design such that the hybrid control scheme is safe.

Theorem 2 (Single Lane Safety Theorem) If:

1. The discrete controller may switch to u_i at time t only if $x(t) \in V_i$, where $i \in \{L, J, S, F\}$.
2. The discrete controller allows at most one maneuver (join or split) per vehicle at a time¹¹. For a given vehicle the beginning of a new maneuver takes place at least $T_F + T_L$ seconds after the end of the last maneuver.
3. After a collision between two vehicles follower operation is established.
4. Assumptions 2–8 are satisfied.
5. The AHS contains a finite number of vehicles.

Then the single lane AHS is safe in the sense of Definition 3.

¹¹Following [2], it is assumed that during a maneuver the joining/splitting vehicle and the vehicle being joined to/split from cooperate and therefore are both involved in the maneuver.

Comments: The first assumption of the theorem imposes requirements on the design of the interface between the continuous and discrete controllers. In particular the safe sets, V_i , determine the safety checks and terminating conditions that need to be checked by the interface before starting and finishing a maneuver (refer to [29] for more details). The “one at a time” part of the second theorem assumption is already satisfied by the coordination level design of [7]. Some additions are needed to guarantee the timing constraints. Justification for the third and fourth theorem assumptions is given in Section 3.4. It should be noted that the third assumption can easily be implemented by simple modification of the join and split protocols, in particular the conditions under which the maneuvers get completed or aborted respectively. The last assumption is need to “break the symmetry” of the problem and provides a starting point for the induction in the proof.

Proof: By design, any collision will occur while some u_i , $i \in \{L, J, S, F\}$, is being used. Following Assumption 7 we will collapse all platoons to a single vehicle and ignore the case $i = F$. Note that if Lemmas 1–3 hold, then the conclusion of the theorem follows trivially. Therefore we only need to check that the assumptions of the lemmas hold.

Assumption 1 of Lemmas 1–3 holds by theorem assumption 4. Assumption 4 of Lemmas 1–3 holds by theorem assumption 1. To check Assumptions 2 and 3 of the lemmas we will use an induction argument on the number of vehicles. The induction argument will start at 4 vehicles. The first vehicle will be executing the leader controller and can not experience a collision with anyone ahead of it (simply because there is no one there). The remaining three vehicles will be labeled B, A and C as in Figure 3. Let (i, j, k) denote the control laws executed by vehicle B, A and C respectively, where $i, j, k \in \{L, J, S\}$ (u is suppressed to simplify the notation). There are $3^3 = 27$ possible triplets. Theorem assumption 2 implies that some of them are impossible (all the ones with S or J in adjacent locations). This eliminates 16 triplets. We enumerate the remaining:

- for (L, L, L) all assumptions of Lemma 1 are satisfied for vehicles A, B and C.
- for (L, L, J) and (L, L, S) all assumptions of Lemma 1 are satisfied for vehicles A and B. Hence all assumptions of Lemma 2/3 are satisfied for vehicle C.
- for (L, S, L) and (L, J, L) all assumptions of Lemma 1 are satisfied for vehicles B and C and all assumptions of Lemma 2/3 for vehicle A.
- for (J, L, L) and (S, L, L) all assumptions of Lemma 1 are satisfied for vehicles A and C and all assumptions of Lemma 2/3 for vehicle B.
- for (J, L, J) , (J, L, S) , (S, L, J) and (S, L, S) all assumptions of Lemma 1 are satisfied for vehicle A and all assumptions of Lemma 2/3 for vehicles B and C.

Note that the 4 vehicle case contains the simpler 3, 2 and 1 vehicle cases (they reduce to $(L, *, *)$, $(L, L, *)$ and (L, L, L) respectively where $*$ denotes a “do not care” entry).

The above enumeration indicates that for 4 vehicles:

- the system is safe,
- a vehicle never collides under L ,

- any collision under S or J will be at relative velocity at most v_a

Note that the above assertions will also hold for the first 4 vehicles of any chain provided that the last vehicle is either executing J or S and is not hit from behind or is executing L and is hit from behind with relative velocity at most v_a .

The last observation allows us to extend the argument to an arbitrary chain of vehicles of finite length. Assume that the 3 assertions hold for a chain of N vehicles. Consider a chain of $N + 1$ vehicles. The following situations are possible:

- Vehicle $N + 1$ executes J or S . In this case vehicle N will have to be executing L by Theorem assumption 2. By induction hypothesis vehicle N will not experience a front collision. By Lemma 2/3 vehicle $N + 1$ can collide with vehicle N with relative velocity at most v_a . This collision is safe for $N + 1$ and leaves the N chain safe as well.
- Vehicle $N + 1$ executes L . Vehicle N can execute any control law. By induction hypothesis vehicle N can experience at most one front end collision with relative velocity at most v_a . By Lemma 1 vehicle $N + 1$ will not collide with vehicle N .

The conclusion follows by induction. $\square$

From the proof, it immediately follows that, under the theorem assumptions:

Corollary 1 (Leader Safety) *A vehicle under the leader control law, u_L , will never collide.*

Corollary 2 (Join/Split Safety) *The relative velocity of any collisions that take place during the join or split maneuvers will be smaller than v_a .*

Corollary 3 (Follower Safety) *The relative velocity of any collisions experienced by a follower will be smaller than v_a .*

The assumption that the chain of vehicles is finite is a bit disturbing, but it is needed to break the symmetry of the problem. It will be satisfied for example if we assume that the freeway is initially empty and is slowly populated by vehicles that follow the remaining assumptions of the theorem. Based on the theorem assumptions the task of designing the interface between the continuous and the discrete controllers becomes almost trivial. The complete interface design will be given after the more complicated safety theorem for the multi lane system is introduced in Section 5.

5 Multi Lane Safety Theorem

The only additional complication in a multi-lane AHS is that we have to guarantee that no unsafe collisions will occur during lane changes. Here we will assume the lane change scenario of [2], where a vehicle is a free agent (single car platoon) both before and after the lane change. With minimal changes the same analysis can be applied to other lane change scenarios (changing from/to the end/middle of a platoon, entire platoon lane change, etc.).

A typical lane change situation is shown in Figure 5. Vehicle A wishes to move to the lane where vehicles D and E are moving. To avoid introducing additional notation

Figure 5: Lane Change

let x_{AB} denote the state of vehicle A with respect to vehicle B. Here “state” has the same interpretation as in Section 3.2 (velocity, acceleration, spacing and relative velocity). Also let u_A denote the input applied by vehicle A and u_L^{AB} the input calculated by the lead controller of Section 6 for the state x_{AB} (similarly for the other subscripts and superscripts).

5.1 Background Lemmas

As for the single lane case, the safety theorem will be based on a sequence of lemmas about the individual maneuvers. The lemmas require the underlying Assumptions 2–8 (not all assumptions are needed by all the lemmas though). The proofs are given in Section 8.

In terms of continuous controllers, the lane change can be broken up into two parts. In the first part vehicle A is aligned with an appropriate gap in the target lane. This is achieved by deceleration of either vehicle A or vehicle D. The continuous law applied at this stage is called the **decelerate law**. In Section 8 a decelerate law (u_D) and a safe set of initial conditions (V_D) will be designed. It will be shown that:

Lemma 4 (Decelerate Law Safety Lemma) *Assume that u_D is applied by vehicle A during an interval $[t_i, t_f]$ with $t_i < t_f$ and that:*

1. $\ddot{x}_B(t) \in [d_{min}, d_{max}]$, for all $t \in [t_i, t_f]$,
2. B experiences at most one collision in $[t_i, t_f]$, with relative velocity at most v_a ,
3. Vehicles C and A do not collide in $[t_i, t_f]$,
4. $x_{AB}^0 = x_{AB}(t_i) \in V_D$.

Then vehicles A and B will not collide in $[t_i, t_f]$. Moreover, if the state leaves V_D at time t , it is guaranteed to return to V_D by at most $t + T_L$.

For some initial conditions, the decelerate law will have to be applied by vehicle D, to allow vehicle A to move into the lane ahead of it. This decision is taken by the coordination layer. Lemma 4 also holds in this case for vehicles D and E.

The second phase of the lane change is the actual movement of vehicle from lane to lane. Because of Assumption 6 we will only be concerned with the longitudinal aspects of this movement. In Section 8 longitudinal laws for vehicles A, C and D (u_{MA}, u_{MC} and u_{MD}) and safe sets of initial conditions (V_{MA}, V_{MC} and V_{MD}) will be designed. It will be shown that:

Lemma 5 (Change Lane Safety Lemma) *Assume that u_{MA}, u_{MC} and u_{MD} are applied during an interval $[t_i, t_f]$ with $t_i < t_f$ and that:*

1. $\ddot{x}_B(t) \in [d_{min}, d_{max}]$ and $\ddot{x}_E(t) \in [d_{min}, d_{max}]$ for all $t \in [t_i, t_f]$,
2. Vehicles B and E experience at most one collision each in $[t_i, t_f]$, with relative velocity at most v_a ,
3. Vehicle D experiences at most one rear-end collision in $[t_i, t_f]$, with relative velocity at most v_a ,
4. $x_{AB}^0 = x_{AB}(t_i) \in V_{MA}$, $x_{AE}^0 = x_{AE}(t_i) \in V_{MA}$, $x_{DA}^0 = x_{DA}(t_i) \in V_{MD}$ and $x_{CA}^0 = x_{CA}(t_i) \in V_{MC}$.

Then no collision between vehicles A, B, C, D, E will occur during $[t_i, t_f]$. Moreover, if x_{AB}, x_{AE}, x_{DA} and x_{CA} leave the corresponding safe sets at time t they are guaranteed to return by at most $t + T_L$.

The interval $[t_i, t_f]$ will typically represent the entire time it takes to move from one lane to the next (roughly 5 seconds under the current lateral laws [22]).

For the purposes of safety, entry and exit from the automated highway will be treated as a simplified version of a lane change. In particular, entry will be modeled as a lane change from the on-ramp to an automated lane, with vehicles C and B missing. Exit will be modeled as a lane change from an automated lane to an off ramp, with vehicles D, E and F missing. The entry/exit scheme obtained in this way will be safe, but may be inefficient in terms of throughput. For a more thorough treatment of entry and exit scenarios the reader is referred to [51]. All the scenarios discussed therein are amenable to our analysis techniques.

5.2 Safety Theorem

The following theorem states conditions on the discrete design such that the hybrid control scheme is safe.

Theorem 3 (Multi Lane Safety Theorem) *If:*

1. *The discrete controller can switch to u_i , $i \in \{L, J, S, F, D, MA, MC, MD\}$, only if the state is in the corresponding safe set.*
2. *The discrete controller allows each vehicle to be involved in at most one maneuver (entry, exit, decelerate, move, join or split) at a time. For a given vehicle, the beginning of new join or split maneuver takes place at least $T_F + T_L$ seconds after the end of the last join or split.*
3. *After any safe collision follower operation is established.*

4. Assumptions 2–8 are satisfied.

5. The AHS contains a finite number of vehicles.

Then the multi lane AHS is safe in the sense of Definition 3.

Theorem Assumption 2 is to be interpreted according to the communication protocol design of [7]. A maneuver involves at least two cooperating platoons. For a join/split both the joining/splitting platoon and the platoon being joined to/split from are involved. For a lane change/entry/exit the vehicle that is changing lane, a vehicle in the target lane (either D or E) and the vehicle in the lane adjacent to the target lane (F) are involved. The protocols do not require cooperation if some of these vehicles are missing.

The proof of Theorem 3 follows by an induction argument similar to the one given for Theorem 2 (slightly more complicated due to the presence of more maneuvers). The role of the lane changing vehicles in the proof is very similar to that of the lead vehicles in the proof of Theorem 2. In the multi-lane case we have, in addition to Corollaries 1 – 3:

Corollary 4 (Lane Change Safety) *A vehicle will never collide while executing a lane change (Decelerate and Move control laws) and Entry or an Exit.*

Assumption 1 of the theorem can be used to obtain an interface between the hybrid controller for the regulation layer and the finite state world of the coordination layer. The interface induced by the theorem is shown in Figure 6. It is essentially a finite state machine (does not have a continuous state of its own), whose transitions contain:

1. Guards on the continuous state of the regulation layer.
2. An event issued by the coordination layer. The event represents the maneuver commanded by the coordination layer: *Enter, Exit, Join, Split, Decelerate* and *Move*.

The transitions are taken when the coordination layer command is issued if the guard is satisfied. The interface of Figure 6 gives a compact representation of the necessary conditions that the guards on the edges need to satisfy. Transitions out of the states Move and Decelerate are automatically enabled if the entering transition guard is satisfied and the proposed control laws are applied (refer to the proofs of Lemmas 4 and 5). The transitions may be enabled for quite some time (possibly throughout the maneuver) before they are taken. When the transitions takes place will be determined by other considerations (coordination layer commands, criteria for aborting maneuvers or declaring them complete, etc.). Essentially each of the states of Figure 6 contains a small finite state machine that can be used to determine when transitions out of the state are executed (in addition to the guards shown in the figure). For a more detailed discussion of this point refer to [29].

6 The Leader Control Law

6.1 Design for safety

According to Lemma 1 the safety criterion used for the leader should be:

$$J_1(x^0, u, d) = - \inf_{t \geq t_i} x_3(t)$$

Figure 6: Interface Design

$t_i = 0$ can be assumed without loss of generality.

The design of a safe controller for the above criterion (no collision) can be posed as a reachability question on the hybrid automaton of Figure 4. To answer the safety question we would like to know under what conditions the discrete state *CRASH* is reachable. We will approach this problem from the point of view of dynamical games. In particular, we will seek a saddle solution (u_1^*, d_1^*) for the two player zero sum game with cost function J_1 . Because of the nature of the cost function it is impossible to tackle this problem with the conventional game theoretic techniques (Hamilton-Jacobi-Isaacs equations, Maximum Principle, etc.). Instead, we will try to guess the saddle solution and then show that it satisfies the definition. Consider the candidate saddle strategy, (u_1^*, d_1^*) , given by:

$$u_1^*(t) = \begin{cases} j_{min} & \text{if } t \leq T_1 \\ 0 & \text{if } t > T_1 \end{cases} \quad (18)$$

$$d_1^*(t) = \{\ddot{x}_B^*, (T_B^*, \delta v_B^*), (T_C^*, \delta v_C^*)\} \quad (19)$$

where:

$$\begin{aligned} \ddot{x}_B^*(t) &= \begin{cases} d_{min} & \text{if } t \leq T_2 \\ 0 & \text{if } t > T_2 \end{cases} \\ T_B^* &= t_i = 0 \\ \delta v_B^* &= \max\{v_a, x_4(T_B) + x_1(T_B)\} \\ T_C^* &= t_i = 0 \\ \delta v_C^* &= v_a \end{aligned} \quad (20)$$

T_1 is the time when the acceleration of vehicle A reaches a_{min}^A under j_{min} and T_2 the time

when vehicle B stops under d_{min} . Let T_3 be the time when vehicle A stops. Then:

$$T_1 = \frac{a_{min}^A - x_2^0}{j_{min}} \quad (21)$$

$$T_2 = -\frac{\delta v_B^* + x_1^0 + x_4^0}{d_{min}} \quad (22)$$

$$T_3 = \begin{cases} \frac{-x_2^0 - \sqrt{(x_2^0)^2 - 2j_{min}(x_1^0 - \delta v_C^*)}}{j_{min}} & \text{if } 0 \leq T_3 \leq T_1 \\ \frac{(a_{min}^A - x_2^0)^2 - 2j_{min}(x_1^0 - \delta v_C^*)}{2j_{min}a_{min}^A} & \text{if } T_1 \leq T_3 \end{cases} \quad (23)$$

A simple calculation shows that, under the assumed input and disturbance constraints:

Lemma 6 *If $x^0 \in \mathbf{X}_C$ then $x(t) \in \mathbf{X}_C$ for all $t \in [0, T_3]$.*

Lemma 7 *(u_1^*, d_1^*) is globally a saddle solution for cost $J_1(x^0, u, d)$.*

Proof: For (u_1^*, d_1^*) to be a saddle solution we need to show that a unilateral change in strategy leaves the player who decided to change worse off. Let $x^*(t)$ denote the state at time t under the inputs (u_1^*, d_1^*) . In particular:

$$\begin{aligned} x_3^*(t) &= \begin{bmatrix} 0 & -t^2/2 & 1 & t \end{bmatrix} x^0 - \int_0^t \frac{(t-\tau)^2}{2} u_1^*(\tau) d\tau + \int_0^t (t-\tau) \ddot{x}_B^*(\tau) d\tau \\ &\quad + (\delta v_B^* + \delta v_C^*) t \\ x_4^*(t) &= \begin{bmatrix} 0 & -t & 0 & 1 \end{bmatrix} x^0 - \int_0^t (t-\tau) u_1^*(\tau) d\tau + \int_0^t \ddot{x}_B^*(\tau) d\tau + (\delta v_B^* + \delta v_C^*) \end{aligned}$$

First, fix $d = d_1^*$ and let u vary. Let $x(t)$ denote the state at time t under the inputs (u, d_1^*) . Then:

$$\begin{aligned} x_4(t) &= \begin{bmatrix} 0 & -t & 0 & 1 \end{bmatrix} x^0 - \int_0^t (t-\tau) u(\tau) d\tau + \int_0^t \ddot{x}_B^*(\tau) d\tau \\ &\quad + (\delta v_B^* + \delta v_C^*) \\ \Rightarrow x_4(t) - x_4^*(t) &= \int_0^t (t-\tau) (u_1^*(\tau) - u(\tau)) d\tau \end{aligned}$$

We need to distinguish two cases:

1. $t \leq T_1$. The bounds on u imply that:

$$\begin{aligned} u(\tau) \geq u_1^*(\tau) &\Rightarrow \int_0^t (t-\tau) (u_1^*(\tau) - u(\tau)) d\tau \leq 0 \\ &\Rightarrow x_4(t) - x_4^*(t) \leq 0 \end{aligned}$$

2. $t \geq T_1$. Recall that $\ddot{x}_B^*(t)$ is piecewise constant, with a discontinuity at T_2 (which may be either greater or less than T_1). Therefore $x_4(t)$ and $x_4^*(t)$ are piecewise differentiable, with derivatives $-x_2(t)$ and $-x_2^*(t)$ respectively. By definition of T_1 , $x_2^*(t) = a_{min}^A \leq x_2(t)$ in the interval of interest. Therefore, as $x_4(0) = x_4^*(0)$, $x_4^*(t) \geq x_4(t)$.

In both cases $\dot{x}_3(t) = x_4(t) \leq x_4^*(t) = \dot{x}_3^*(t)$. Using the fact that $x_3^*(0) = x_3(0) = x_3^0$ and integrating:

$$\begin{aligned} x_3(t) &\leq x_3^*(t) \text{ for all } t \\ \Rightarrow -\inf_{t \geq 0} x_3(t) &\geq -\inf_{t \geq 0} x_3^*(t) \\ \Rightarrow J_1(x^0, u, d_1^*) &\geq J_1(x^0, u_1^*, d_1^*) \end{aligned} \quad (24)$$

Now fix u_1^* and allow d to vary. Let $x(t)$ denote the state at time t under the inputs (u_1^*, d) . Then:

$$x_4(t) = \begin{bmatrix} 0 & -t & 0 & 1 \end{bmatrix} x^0 - \int_0^t (t - \tau) u_1^*(\tau) d\tau + \int_0^t \ddot{x}_B(\tau) d\tau + \delta v_B 1_{T_B}(t) + \delta v_C 1_{T_C}(t)$$

Therefore:

$$x_4(t) - x_4^*(t) = \int_0^t (\ddot{x}_B(\tau) - \ddot{x}_B^*(\tau)) d\tau + (\delta v_B 1_{T_B}(t) - \delta v_B^*) + (\delta v_C 1_{T_C} - \delta v_C^*)$$

Note that:

$$\left. \begin{aligned} \delta v_C^* &= v_a \\ \delta v_C &\geq v_a \\ v_a &\leq 0 \end{aligned} \right\} \Rightarrow \delta v_C 1_{T_C}(t) - \delta v_C^* \geq 0$$

If $\delta v_B^* = v_a$, the same is true for the term $(\delta v_B 1_{T_B}(t) - \delta v_B^*)$. If $\delta v_B^* > v_a$, then $x_4^*(0) + x_1^*(0) = 0$ (recall that $T_B^* = 0$) and therefore $x_4^*(t) + x_1^*(t) \equiv 0$ (once vehicle B stops it never starts moving again under d_1^*). But, $x_4(t) + x_1(t) \geq 0$ (by the assumed state constraint) and $x_1(t) = x_1^*(t)$ (as $x_1(t)$ does not depend on δv_B). Therefore, if $\delta v_B^* > v_a$, $x_4(t) - x_4^*(t) \geq 0$ for all $t \geq 0$.

Overall, under the assumed constraints on δv_B and δv_C , either $x_4(t) \geq x_4^*(t)$ or the term outside the integral is positive. For the integral term we need to distinguish two cases:

1. $t \leq T_2$. The bounds on $\ddot{x}_B$ imply that:

$$\ddot{x}_B(\tau) \geq \ddot{x}_B^*(\tau) \Rightarrow \int_0^t (\ddot{x}_B(\tau) - \ddot{x}_B^*(\tau)) d\tau \geq 0$$

2. $t \geq T_2$. Then, by definition of T_2 , $\int_0^t \ddot{x}_B^*(\tau) d\tau = -(x_1^0 + x_4^0)$. The state constraints imply that $x_1(t) + x_4(t) \geq 0$ (vehicle B does not go backwards), therefore $\int_0^t \ddot{x}_B(\tau) d\tau \geq -(x_1^0 + x_4^0)$. Subtracting, $\int_0^t (\ddot{x}_B(\tau) - \ddot{x}_B^*(\tau)) d\tau \geq 0$.

The stopping time for B under d will always be greater than the stopping time under d_1^* . In both cases, we are able to conclude that $\dot{x}_3(t) = x_4(t) \geq x_4^*(t) = \dot{x}_3^*(t)$. Integrating this inequality from 0 to t and using the fact that $x_3^*(0) = x_3(0) = x_3^0$:

$$\begin{aligned} x_3(t) &\geq x_3^*(t) \text{ for all } t \\ \Rightarrow -\inf_{t \geq 0} x_3(t) &\leq -\inf_{t \geq 0} x_3^*(t) \\ \Rightarrow J_1(x^0, u_1^*, d) &\leq J_1(x^0, u_1^*, d_1^*) \end{aligned} \quad (25)$$

Combining inequalities 25 and 24:

$$J_1(x^0, u_1^*, d) \leq J_1^*(x^0) \leq J_1(x^0, u, d_1^*) \quad (26)$$

for all d and u . By definition, (u_1^*, d_1^*) is globally a saddle solution. $\square$

6.1.1 Safe Set of Initial Conditions

Next we need to determine the set of initial conditions that can be safe under the lead control. Let:

$$J_1^*(x^0) = J_1(x^0, u_1^*, d_1^*)$$

Recall that $x_3^*(t)$ is a continuously differentiable function of t defined on the compact interval $[0, \min\{T_3, t_f\}]$, with derivative $\dot{x}_3^*(t)$. Therefore:

Lemma 8 *There exist $\hat{T} \in [0, \min\{T_3, t_f\}]$ such that:*

$$J_1^*(x^0) = -x_3^*(\hat{T})$$

Moreover, either $\hat{T} = 0$ or $\hat{T} = \min\{T_3, t_f\}$ or $\dot{x}_3^(\hat{T}) = 0$.*

The calculations for analytically determining $J_1^*(x^0)$ from this lemma are rather messy. However, as the set of times T where $\dot{x}_3^*(T) = 0$ is finite, we can easily carry out the calculation numerically. Indeed, a simple computer program was written to calculate $J_1^*(x^0)$ for various values of x^0 . It should be noted that x_3^0 only enters the calculations as a constant offset on $x_3(t)$. Figure 7 shows the set of points where $J_1^*(x^0) = 0$ for some values of x_3^0 .

Figure 7: Safe set of initial conditions for $x_3^0 = 20, 30$ and 40 meters

Lemma 7 implies that the surfaces of Figure 7 are 2 dimensional slices of the 3 dimensional boundary of the safe set V_1 for various values of x_3^0 . Any initial condition on or above these surfaces will not lead to a collision, provided $u = u_1^*$. The higher surfaces correspond to smaller initial spacings x_3^0 (the top to 20m, the next to 30m etc.). As expected the safe set shrinks as x_3^0 decreases. Figure 7 can be used to infer certain interesting system

restrictions. For example, the graph indicates that steady state following at $25ms^{-1}$ can only take place safely at spacings of about $40m$ or greater (otherwise the initial conditions corresponding to $x_4^0 = 0m/s$ become unsafe).

It should be noted that the safe set depends on the discrete state:

$$q \in \{00, 01, 10, 11, CRASH\}$$

Even though J_1 is independent of q , the set of allowable disturbances is larger at $q = 00$, smaller for $q \in \{01, 10\}$ and even smaller for $q = 11$ ¹². In particular some collision disturbances are excluded in some discrete states. A simple corollary of the proof of Lemma 7 is:

Corollary 5 $(u_1^*, \{\ddot{x}_B^*, (t, 0), (T_C^*, \delta v_C^*)\})$, $(u_1^*, \{\ddot{x}_B^*, (T_B^*, \delta v_B^*), (t, 0)\})$ and $(u_1^*, \{\ddot{x}_B^*, (t, 0), (t, 0)\})$ are globally saddle solutions for J_1 on $(t, t_f]$, if the discrete state becomes $q = 10, 01, 11$ at time t respectively.

The effect of the reduced disturbance is to move the boundary of the safe set “down” (refer to Figure 7) by $|v_a|$ if $q \in \{01, 10\}$ and by $2|v_a|$ if $q = 11$.

We will not investigate these refinements further. We will define the **safe set** V_1 as the set of initial conditions for which the system is safe if $q = 00$, i.e.:

$$V_1 = \{x^0 \in \mathbf{X}_C | J_1^*(x^0) \leq C_1 = 0\} \quad (27)$$

V_1 still guarantees safety as it is contained in the safe sets for all q . It is not the best choice for a comfortable ride. However, this choice simplifies the calculations somewhat and circumvents the technological difficulty of how collisions of the preceding vehicle are to be detected.

6.1.2 The Class of Safe Controls

The above analysis also allows us to determine the class of **safe controls** $\mathcal{U}_1(x^0)$, i.e. the controls for which any initial condition $x^0 \in V_1$ can not result in a crash. Let ∂V_1 denote the boundary of V_1 in the induced topology of $\mathbf{X}_C$ as a subset of $\mathbb{R}^4$. Define the **interior of** V_1 as:

$$\text{int}(V_1) = V_1 \setminus \partial V_1$$

Lemma 9 (Class of Safe Controls for Leader Operation) *The class of safe controls for a given initial condition x^0 is given by:*

$$\begin{aligned} \mathcal{U}_1(x^0) &= \emptyset \text{ if } x^0 \in \mathbf{X}_C \setminus V_1 \\ u \in \mathcal{U}_1(x^0) &\iff \begin{cases} u(x) \in [u_{\min}(x), u_{\max}(x)] & \text{if } x \in \text{int}(V_1) \\ u(x) = u_1^* & \text{if } x \in \mathbf{X}_C \setminus \text{int}(V_1) \end{cases} \end{aligned}$$

where u_1^* is given by equation (18) with x_2^0 being the acceleration of the vehicle at the time the boundary is reached.

¹²Clearly the safe set is empty if $q = CRASH$.

Lemma 9 follows as a corollary of Lemma 7. The class of safe controls can be fully specified in feedback form (u_1^* is trivially a feedback controller). Notice that, if the discrete disturbances are removed, the control u_1^* is such that if the continuous state starts on the boundary of V_1 it will either “slide” along it or cross in the interior of V_1 , depending on the acceleration of vehicle B. However, in the presence of discrete disturbances, V_1 is **not** an invariant set under u_1^* . A collision of vehicle B and/or C may push the trajectory well outside V_1 . The effect of these collisions will be to change the discrete state to $q = 01$ or 10 or 11 (refer to Figure 4). Corollary 5 indicates that, after the collisions, the continuous state will still be in the safe set of the new discrete state. Overall, even though the continuous state trajectory crosses outside V_1 the system is still safe, as long as u_1^* is applied.

6.2 Design for comfort

Having established conditions for safety we can now improve the design by considering passenger comfort. We seek a saddle solution, (u_2^*, d_2^*) :

$$\begin{aligned} J_2^*(x^0) &= \max_{d \in \mathcal{D}} \min_{u \in \mathcal{U}_1(x^0)} J_2(x^0, u, d) \\ &= \min_{u \in \mathcal{U}_1(x^0)} \max_{d \in \mathcal{D}} J_2(x^0, u, d) \\ &= J_2(x^0, u_2^*, d_2^*) \end{aligned}$$

for the cost comfort cost function:

$$J_2(x^0, u, d) = \sup_{t \geq 0} |u(t)|$$

Assume $x^0 \in V_1$. Consider the candidate solution:

$$u_2^*(x) = \begin{cases} u_1^* & \text{if } x \in \mathbf{X}_C \setminus \text{int}(V_1) \\ 0 & \text{otherwise} \end{cases} \quad (28)$$

As neither d nor x enter the cost function J_2 , (u_2^*, d) will trivially be a saddle solution for every d . As before we can determine the set of initial conditions, V_2 , for which the requirement for comfort:

$$J_2^*(x^0) \leq C_2$$

can be satisfied. Assuming $C_2 < |j_{min}|$ this set is:

$$V_2 = \text{int}(V_1) \bigcup \{x \in \partial V_1 | x_2 = a_{min}^A\} \quad (29)$$

Moreover the class of comfortable controls for $x^0 \in V_2$ will be:

$$\mathcal{U}_2(x^0) = \{u \in \mathcal{U}_1(x^0) | u(t) \in [-C_2, C_2]\} \quad (30)$$

6.3 Design for efficiency

To complete the design the requirement for efficiency should also be addressed. We will not go into the details of the efficient design, as this problem can be approached in a number of ways and the solution does not affect safety in anyway. The saddle solution, (u_3^*, d_3^*) , for cost function J_3 can be sought, for example:

$$\begin{aligned} J_3^*(x^0) &= \max_{d \in \mathcal{D}} \min_{u \in \mathcal{U}_2(x^0)} J_2(x^0, u, d) \\ &= \min_{u \in \mathcal{U}_2(x^0)} \max_{d \in \mathcal{D}} J_3(x^0, u, d) \\ &= J_3(x^0, u_3^*, d_3^*) \end{aligned}$$

The result will be some form of H_∞ optimal design for u_3^* . Other designs (e.g. the one proposed in [16]) are also acceptable. As we do not set a threshold for J_3 the choice of u_3^* is not crucial. The requirement that $u_3^* \in \mathcal{U}_2(x^0)$ can be enforced a-posteriori, as will be shown in next section. To simplify the analysis, we will assume that the leader fixed point, y_d^L satisfies $y_d^L \in V_2$ and that u_3^* has been designed so that the vehicle velocity never exceeds the specified highway velocity v_H . Such a design can be easily obtained, for example, by switching from tracking y_d to tracking v_H whenever $x_1(t)$ exceeds v_H and back to tracking y_d whenever the spacing becomes less than the desired $x_3 < y_d^1$ (see [16] for more details). Such internal modifications of u_3^* leave the safety of the system unaffected.

6.4 Proof of the Leader Safety Lemma

Consider the following switched feedback law as the safe leader law:

$$u_L(x) = \begin{cases} u_3^* & \text{if } x \in V_2 \text{ and } u_3^* \in [-C_2, C_2] \\ C_2 & \text{if } x \in V_2 \text{ and } u_3^* > C_2 \\ -C_2 & \text{if } x \in V_2 \text{ and } u_3^* < -C_2 \\ u_1^* & \text{if } x \in \mathbf{X}_C \setminus V_2 \end{cases} \quad (31)$$

Let:

$$V_L = V_1 \quad (32)$$

Proof (of Lemma 1) Under this design for u_L and V_L , the “no collision” claim of Lemma 1 follows directly from Lemmas 7 and 9. In addition, the above design is guaranteed to satisfy the passenger comfort requirement as long as $x \in V_2$ (i.e. as long as safety is not an issue).

The only point that remains to be investigated is that there exists a finite time, T_L , such that, if the state leaves V_L , it returns at most T_L seconds later. Assume, for the sake of contradiction, that x exits V_L and never re-enters. Note that in $\mathbf{X}_C \setminus V_2$ (which contains the complement of V_L) u_1^* is applied (i.e. vehicle A decelerates as hard as possible). By Lemma 7 vehicles A and B will not collide. Moreover, if $x(t)$ stays outside V_L and u_1^* is applied, vehicle A will stop after at most T_3 (equation (23)) seconds. But once A stops without colliding, it will be safe from then on (in other words, all initial conditions with $x_1^0 = 0$ are in V_L). This contradicts our original assumption.

Figure 8: Controller Hybrid Automaton

The above discussion reveals that the state will return to V_L at most T_3 seconds after it leaves it. Equation 23 indicates that T_3 depends on $x_1^0, x_2^0, \delta v_C$ and the system constants. Therefore, taking:

$$T_L = \max\{T_3 | x_1^0 \in [0, v_H], x_2^0 \in [a_{min}^A, a_{max}^A], \delta v_C \in [v_a, 0]\} \quad (33)$$

will give an upper bound on the time it takes the state to return to V_L for any initial condition.

□

Note that the controller u_L can be easily encoded by a hybrid automaton. The structure can be directly inferred from equation (31) (Figure 8). Lemma 1 can then be interpreted as saying that in the interconnection of the hybrid automata of Figures 4 and 8, the states corresponding to the state *CRASH* are unreachable.

7 The Join Control Law

In the previous section a design for the leader of a platoon was pieced together. The design consists of a control law, u_L , and a set of initial conditions, V_L , such that if u_L is switched on while the state is in V_L no collision will occur, provided that the behavior of the neighboring vehicles satisfies certain constraints. Can this design also be used for joining and splitting platoons? Figure 9 shows three slices of the boundary of V_L for $x_3^0 = 1, 13$ and $16m$ respectively (starting from top to bottom) and $x_1^0 = 20m/s$. The figure was obtained by allowing vehicle B to collide once, with relative velocity at most v_a and not allowing vehicles A and C to collide. Recall that the join law should regulate to the follower fixed point, which is $x_4 = 0m/s$ and $x_3 = 1m$. From the figure it should be immediately apparent that, even for this reduced

disturbance, safe operation with u_L is impossible under these conditions, as any point with $x_4 = 0m/s$ is well outside the safe set for $x_1 = 1m$. In fact, for a meaningful design we would like the point $x_4 = 0m/s, x_2 = 0m/s^2$ to be within the safe set. The figure indicates that for this to happen a spacing of at least $13m$ is needed. Ideally we would like the system to be safe for the entire range of x_2 . For this spacings of $16m$ or greater are needed.

Figure 9: Boundary of the safe set for $x_1^0 = 20ms^{-1}$

What can be done to resolve this problem? The first option is to reduce the disturbances that vehicle A can face. This can be done in four ways:

1. Prevent vehicle B from colliding with the vehicle ahead of it.
2. Prevent vehicle C from colliding with vehicle A.
3. Reduce the range $[d_{min}, d_{max}]$ (in particular increase d_{min}).
4. Provide vehicle A with additional information, for example, assume the follower mode where $\ddot{x}_B$ is communicated to vehicle A.

For the purposes of join and split alternatives 1 and 2 will be considered. Eliminating collisions of vehicles B and C will be achieved by the “one maneuver at a time” assumption of Theorem 2.¹³ Alternative 3 is also feasible, but we will not investigate it here. In order to reduce the range of $\ddot{x}_B$ we need to make assumptions about vehicles downstream of vehicle B or significantly modify the communication protocols, both of which will considerably increase the complexity of the design¹⁴. Alternative 4 will be investigated in the follower design.

¹³This implies that if vehicle A is applying a join or split control law, vehicles B and C must be in the leader mode and apply the leader control law of the previous section.

¹⁴Interesting design alternatives can be obtained in this way. Some of them are briefly discussed in the concluding section.

Technological limitations (such as the range of the infrared communication device used to transmit $\ddot{x}_B$ information) make this alternative unattractive for joining and splitting.

Is this reduction in disturbance sufficient to allow us to solve the problem? The discussion in Section 6 indicates that eliminating the possibility of collisions of vehicle B has the effect of moving the boundary of the safe set in Figure 9 down by $v_a = -3m/s$ in the x_4 direction. This makes a few more initial conditions safe, but is still inadequate (for example the condition $x_3 = 1m, x_4 = 0m/s, x_2 = 0m/s^2$ is still unsafe). Clearly joining of a platoon can not take place under the requirement that no collision occurs. The next step therefore is to relax that requirement, in view of the fact that collisions with relative velocity smaller than v_a are considered safe (see also [31] and [17]). Therefore, in the subsequent design we will consider the cost function:

$$J'_1(x^0, u, d) = |x_4(T)| \quad (34)$$

where:

$$T = \min\{t \geq 0 | x_3(t) = 0\}$$

is the first collision time. The safety requirement will be encoded by:

$$J'_1(x^0, u, d) \leq C_1 = |v_a|$$

7.1 Design for Safety

The design of the join and split controllers can also be treated as a two player, zero sum game with cost function J'_1 . In this case one player is the control that the joining/splitting vehicle applies, while the other player is the acceleration of the preceding platoon. In our standard notation¹⁵:

$$d \in \mathcal{D}' = \{\ddot{x}_B(t) \in [d_{min}, d_{max}], (t_i, 0), (t_i, 0)\}$$

By abuse of notation we will use $d(t)$ to denote $\ddot{x}_B(t)$. This reduction in the disturbance has the following hybrid automata theoretic interpretation: the communication protocols designed in [7] are such that their interconnection with the hybrid automaton of Figure 4 for the joining/splitting vehicle and the vehicle being joined to/split from has the effect of disabling the transitions *Coll_B* and *Coll_C*.

Guessing a saddle solution for cost J'_1 is not as easy as it was for J_1 . It turns out that, for certain combinations of state constraints and initial conditions (not necessarily in the safe set), full deceleration by both the joining and the preceding vehicle is not the optimum. We will use (u_0^*, d_0^*) to denote the saddle solution for J'_1 .

Lemma 10 *The saddle solution (u_0^*, d_0^*) is such that:*

1. *at every time, u_0^* and d_0^* assume either their minimum or their maximum possible values (bang-bang solution)*
2. *at the time of impact, u_0^* and d_0^* assume their minimum values*
3. *If $x_4(T) < 0$ (non zero relative velocity collision), u_0^* and d_0^* involve at most one switching from their maximum to their minimum values. In particular, three kinds of behavior are possible:*

¹⁵There are other ways of encoding the “no collision” requirement in terms of d but, they are all equivalent.

- (a) Both optimum trajectories assume only their minimum.
- (b) d_0^* assumes its maximum first and then its minimum while u_0^* assumes only the minimum.
- (c) Both optimum trajectories start by assuming their maximum values and u_0^* switches to the minimum before d_0^* . A non zero amount of time elapses between the two switchings.

Proof: The proof will be based on writing J'_1 as an integral cost function and applying the Maximum Principle [41]. Recall that at the time of impact the relative velocity of the vehicles will have to be negative. Therefore:

$$\begin{aligned}
J'_1(x^0, u, d) = |x_4(T)| &= -x_4(T) \\
&= -x_4^0 - \int_0^T \dot{x}_4(t) dt \\
&= -x_4^0 + \int_0^T (x_2(t) - d(t)) dt
\end{aligned}$$

Define $L(x, u, d) = x_2 - d$. Then, for a given initial condition, the extrema of $J'_1(x^0, u, d)$ occur at the extrema of:

$$\int_0^T L(x(t), u(t), d(t)) dt$$

The following discussion will assume the existence of optimal controls and proceed to classify them using the Maximum Principle. Existence and uniqueness questions will not be investigated further here ¹⁶ as the justification for the analysis will be provided by numerical examples in Section 7.2 We form the Hamiltonian:

$$\begin{aligned}
\tilde{H}(x, p, p_0, u, d) &= p_0 L(x, u, d) + p'(Ax + Bu + Dd) \\
&= (p_0 + p_1 - p_4)x_2 + p_3x_4 + p_2u + (p_4 - p_0)d
\end{aligned}$$

As the terms in u and d conveniently decouple, we can take the maximum of $\tilde{H}$ over u and the minimum over d to obtain a **saddle solution** (u_0^*, d_0^*) for the two player game.

$$\begin{aligned}
H(x, p, p_0) &= \max_{u \in [u_{min}(x), u_{max}(x)]} \min_{d \in [d_{min}(x), d_{max}(x)]} \tilde{H}(x, p, p_0, u, d) \\
&= \min_{d \in [d_{min}(x), d_{max}(x)]} \max_{u \in [u_{min}(x), u_{max}(x)]} \tilde{H}(x, p, p_0, u, d) \\
&= \tilde{H}(x, p, p_0, u_0^*, d_0^*)
\end{aligned}$$

where:

$$u_0^*(t) = \begin{cases} u_{max}(x) & \text{if } p_2(t) > 0 \\ u_{min}(x) & \text{if } p_2(t) \leq 0 \end{cases} \quad (35)$$

$$d_0^*(t) = \begin{cases} d_{max}(x) & \text{if } p_4(t) - p_0 < 0 \\ d_{min}(x) & \text{if } p_4(t) - p_0 \geq 0 \end{cases} \quad (36)$$

¹⁶Existence or even uniqueness of optimal controls is likely to be guaranteed by the fact that the unconstrained dynamics are linear, the cost function is a linear function of the final state, all state constraints are convex and closed and the input constraints are compact intervals.

The Euler equation for p gives:

$$\dot{p} = -\frac{\partial H}{\partial x} = \begin{bmatrix} 0 \\ p_4 - p_0 - p_1 \\ 0 \\ -p_3 \end{bmatrix}$$

which can be integrated to:

$$\begin{aligned} p_1(t) &\equiv p_1(T) \\ p_2(t) &= -\frac{p_3(T)}{2}(T-t)^2 + (p_0 + p_1(T) - p_4(T))(T-t) + p_2(T) \\ p_3(t) &\equiv p_3(T) \\ p_4(t) &= p_3(T)(T-t) + p_4(T) \end{aligned}$$

Boundary condition (5) gives $p(T) = [0 \ 0 \ c \ 0]'$ for some $c \in \mathbb{R}$. Substituting this into the expression for $p(t)$ results in:

$$\begin{aligned} p_1(t) &\equiv 0 \\ p_2(t) &= -\frac{c}{2}(T-t)^2 + p_0(T-t) \\ p_3(t) &\equiv c \\ p_4(t) &= c(T-t) \end{aligned}$$

Note that $p_4(T) = 0 \geq p_0$, hence $d_0^*(T) = d_{min}$.

It should be noted that the solution is not completely characterized at this stage. There are three constants (p_0, c and T) to be determined from the boundary conditions:

- $x_3(T) = 0$
- $H(x, p, p_0) = 0$ for all times

The last constant can be normalized out as c and p_0 can not both be zero and they appear everywhere homogeneously. Unfortunately, the boundary conditions are too complicated to tackle analytically. Numerical calculations will be given in the next section. Here we will only try to determine whether it is possible for the optimal controls to switch. For this purpose we will make use of boundary condition (4), which at time T becomes:

$$p_0(x_2(T) - d_{min}(x(T))) + cx_4(T) = 0 \tag{37}$$

First assume $p_0 < 0$. We will distinguish a number of subcases, depending on the values of $x_2(T)$ and $d_{min}(x(T))$.

Case 1: $x_2(T) < d_{min}(x(T))$. As $x_4(T) \leq 0$, we must have $c > 0$. Then, for all t , $p_2 \leq 0$ and $p_4 \geq 0 > p_0$, therefore $d_0^*(t) = d_{min}$, $u_0^*(t) = u_{min}$.

Case 2: $x_2(T) > d_{min}(x(T))$. This time $c < 0$. Consider the following cases:

- $p_0 \leq cT < 0$: No switching is possible ($d_0^*(t) = d_{min}$, $u_0^*(t) = u_{min}$).
- $2p_0 \leq cT < p_0$: d_0^* exhibits switching. In particular:

$$\begin{aligned} u_0^*(t) &= u_{min} \\ d_0^*(t) &= \begin{cases} d_{max} & \text{if } t \in [0, T - p_0/c) \\ d_{min} & \text{otherwise} \end{cases} \end{aligned}$$

- $cT < 2p_0$: Both u_0^* and d_0^* exhibit switching. In particular:

$$\begin{aligned} u_0^*(t) &= \begin{cases} u_{max} & \text{if } t \in [0, T - 2p_0/c) \\ u_{min} & \text{otherwise} \end{cases} \\ d_0^*(t) &= \begin{cases} d_{max} & \text{if } t \in [0, T - p_0/c) \\ d_{min} & \text{otherwise} \end{cases} \end{aligned}$$

Case 3: $x_2(T) = d_{min}(x(T))$. If $x_4(T) < 0$, $c = 0$, which results in no switching. If $x_4(T) = 0$, the condition on H at time T used here can lead to no information about c . The condition at time 0 may provide more insight. In any case, collisions with zero relative velocity are not crucial from the point of view of vehicle safety.

The case $p_0 = 0$ can be treated similarly. By equation (37) and the fact that $c \neq 0$, $x_4(T) = 0$. Therefore, as in Case 3, this situation will result in a crash with zero relative velocity collision. The comments made for Case 3 also hold here. $\square$

7.2 Numerical Investigation

The above analysis indicates that, at least in theory, it is possible that the optimal controls may take their maximum values for certain segments of time. In terms of vehicles this implies that the best/worst strategy involves not only decelerating, but also accelerating. In particular, three behaviors are possible in theory:

1. Both optimum trajectories involve only maximum deceleration.
2. The optimum for B involves maximum acceleration first and then maximum deceleration while the optimum for A involves only maximum deceleration.
3. Both optimum trajectories start by maximum acceleration and vehicle A switches to maximum deceleration before vehicle B. A non trivial amount of time elapses between the two vehicles switching to full deceleration.

We would like to determine if there exist realistic conditions under which the optimum trajectories involve acceleration.

The terminal condition (37) provides considerable insight, when interpreted in the vehicle framework. First recall that, by the assumptions of the Maximum Principle (Theorem 1), $p_0 \leq 0$ and $p_0 = 0$ implies $c \neq 0$. The last observation together with equation (37) indicate that $p_0 = 0$ results in $x_4(T) = 0$, i.e. collisions with zero relative velocity. In terms of safety zero relative velocity collisions are not particularly interesting. We will therefore restrict our attention to the case $p_0 < 0$ and in particular situations where $x_4(T) \approx v_a = -3ms^{-1}$.

In order to gain some insight into situations that might lead to switching in u_0^* and d_0^* assume that the constraints on the jerk of vehicle A are large (in absolute value) compared with the constraints on the acceleration¹⁷. Recall that at the time of impact, T :

$$u^*(T) = u_{min}(x(T)) \quad d^*(T) = d_{min}(x(T))$$

Therefore, if the jerk is high enough:

$$x_2(T) \approx a_{min}^A \quad d(x(T)) \geq a_{min}^B$$

(depending on whether vehicle B has stopped or not). Moreover, $x_4(T) < 0$. If:

$$a_{min}^A \leq a_{min}^B$$

(i.e. vehicle A can decelerate at least as fast as vehicle B) the terminal condition (37) implies that $c > 0$. This in turn implies that the saddle inputs do not involve switching (Case 1 above). Moreover, even if $a_{min}^A > a_{min}^B$ but:

$$a_{min}^A \approx a_{min}^B$$

equation (37) implies that unsafe collisions can only occur if $\|c/p_0\|$ is small. This makes it unlikely for switching to occur in either u_0^* or d_0^* as, by Case 2 above, switching requires at least:

$$\left\| \frac{c}{p_0} \right\| T > 1$$

Summarizing, if the deceleration capabilities of both vehicles are comparable and the bounds on the jerk are not too conservative, we expect u_0^* and d_0^* to involve only maximum deceleration. This observation is also supported by the results of [17] where, assuming a second order model with delay for vehicle A and uniform deceleration capabilities, it was shown that the saddle solution involves only minimum deceleration by both vehicles.

These observations limit the conditions under which saddle trajectories that involve acceleration can be expected. Are there any conditions for which such behavior can be observed? To answer this question a C-program was written to estimate the value of c under the assumption that $p_0 < 0$ (which is a necessary condition for switching). The state and input constraints used were:

$$\begin{array}{llll} a_{min} = -5.0 & a_{max} = 3.0 & v_{min} = 0.0 & v_{max} = 50.0 \\ a_{min}^B = -8.0 & a_{max}^B = 3.0 & j_{min} = -15.0 & j_{max} = 15.0 \end{array}$$

Vehicle B is assumed to have greater deceleration capabilities than vehicle A, within reasonable limits though. Also the bounds on the jerk are slightly conservative. Consider the initial condition:

$$x^0 = \begin{bmatrix} 20.0ms^{-1} \\ 2.0ms^{-2} \\ 0.01m \\ 3.0ms^{-1} \end{bmatrix}$$

¹⁷If the jerk is unbounded, vehicle A can be described by a second order model without delay. In this case we can think of vehicle A as controlling its acceleration directly.

Note that, while the initial spacing is very small, the initial relative velocity is in favor of vehicle A, as it is moving away from vehicle B. The examples will indicate that this initial condition is unsafe. Figures 11 – 15 can be found in the appendix.

Figure 11 shows the state trajectory for $u(t) \equiv u_{min}(t)$ and $d(t) \equiv d_{min}(t)$, i.e. both vehicles braking as hard as possible. Because of the difference in deceleration capability, a collision occurs at $T = 1.075$ seconds, with relative velocity $x_4(T) = -1.858ms^{-1}$. This is quite a mild collision, well below the threshold $v_a = -3ms^{-1}$.

Assume that the trailing vehicle decides that braking as hard as possible is the best policy. Does Figure 11 depict the worst that can happen? Consider for d the trajectory shown in Figure 12, which involves accelerating before decelerating, making the time to collision larger. The resulting state trajectory is shown in Figure 13. Note that the collision which takes place at $T = 3.290$ seconds is a lot more severe: $x_4(T) = -4.822ms^{-1}$, substantially greater than the threshold.

Can vehicle A do better by accelerating? Consider the saddle solution (u_0^*, d_0^*) shown in Figure 14. Note that vehicle A also accelerates slightly before putting on its brakes. The resulting state trajectory is shown in Figure 15. The collision at time $T = 3.995$ seconds is still severe ($x_4(T) = -3.945ms^{-1}$) but not as severe as that of Figure 13.

7.3 Completing the Design

The analysis presented above allows us to determine the optimal control u_0^* and the worst case disturbance d_0^* for each initial condition x^0 . The corresponding $J_0^*(x^0) = J_1'(x^0, u_0^*, d_0^*)$ as well as the safe set of initial conditions can then be determined numerically.

Having established the set of safe initial conditions, the design of the join controller can be completed to take into account passenger comfort and efficiency. A controller needs to be designed to track the desired fixed point, y_d^J . Any controller that tracks this fixed point (for example [16, 31]) will suffice. Designs that try to minimize the cost function J_3 are preferable. Let u_3^J denote the chosen tracking controller, V_J denote the safe set whose computation was discussed in Section 7.1 and V_2^J its interior in the relative topology of $\mathbf{X}_C$. Then the complete safe, comfortable and efficient design for the join maneuver will be:

$$u_J(x) = \begin{cases} u_3^J & \text{if } x \in V_2^J \text{ and } u_3^J \in [-C_2, C_2] \\ C_2 & \text{if } x \in V_2^J \text{ and } u_3^J > C_2 \\ -C_2 & \text{if } x \in V_2^J \text{ and } u_3^J < -C_2 \\ u_0^* & \text{if } x \in \mathbf{X}_C \setminus V_2^J \end{cases} \quad (38)$$

Note that, unlike V_L the safe set V_J is an invariant set, under the assumed set of disturbances.

7.4 The Split Design

Most of the previous discussion still holds for the split controller as well. For example the controller design of equation (38) will also work for split, if u_3^J is replaced by some u_3^S designed

to track the split fixed point. Letting $V_S = V_J$ and $V_2^S = V_2^J$ as above:

$$u_S(x) = \begin{cases} u_3^S & \text{if } x \in V_2^S \text{ and } u_3^S \in [-C_2, C_2] \\ C_2 & \text{if } x \in V_2^S \text{ and } u_3^S > C_2 \\ -C_2 & \text{if } x \in V_2^S \text{ and } u_3^S < -C_2 \\ u_0^* & \text{if } x \in \mathbf{X}_C \setminus V_2^S \end{cases} \quad (39)$$

With a little more effort better designs (that avoid collisions whenever possible, switch to the leader law as soon as V_L is reached, etc.) can be constructed.

Overall, the above discussion provides guidelines for designing safe, comfortable and efficient controllers for the join and split maneuvers (u_J and u_S respectively) and determining the sets of initial conditions V_J and V_S for which these controllers can guarantee safe operation. Note that, as for the leader law, u_S and u_J are easily implemented by means of a hybrid automaton. If a design is carried out under these guidelines, the proofs of Lemmas 2 and 3 follow.

8 The Lane Change Laws

It should be noted that collisions between vehicles A and C are not possible in the lane change scenario. Because of the “one maneuver at a time” restriction, it is impossible for vehicle C to be joining or splitting to/from vehicle A while the lane change is taking place (the only situation that can lead to a collision in a single lane under corollaries 1 and 2). We still need to consider the possibility of vehicle D getting rear ended though. We will start with the move part of the lane change. The decelerate part will follow as a special case. Consider the following control laws for vehicles A, C and D:

$$u_{MA} = \min\{u_L^{AB}, u_L^{AE}\} \quad (40)$$

$$u_{MC} = u_L^{CA} \quad (41)$$

$$u_{MD} = u_L^{DA} \quad (42)$$

$$(43)$$

and define $V_{MA} = V_{MD} = V_{MC} = V_L$.

Proof (of Lemma 5): Note that, as $u_1^* = u_{min}$, $u_{MA} = u_1^*$ if either $u_L^{AB} = u_1^*$ or $u_L^{AE} = u_1^*$. Moreover, the design of u_L (equation (31)) dictates that $u_L = u_1^*$ if the state leaves the interior of V_L . In other words:

$$u_{MA}(x) = \begin{cases} \min\{u_L^{AB}, u_L^{AE}\} & \text{if } x_{AB} \in V_{MA} \text{ and } x_{AE} \in V_{MA} \\ u_1^* & \text{otherwise} \end{cases} \quad (44)$$

By assumption, both $x_{AB}^0 \in V_{MA}$ and $x_{AE}^0 \in V_{MA}$. Therefore, the proposed controller (44) satisfies the conditions of Lemma 1 for both x_{AB} and x_{AE} , hence vehicles A, B and E will not collide.

Similarly, as $u_{MC} = u_L^{CA}$ and $x_{CA}^0 \in V_{MC}$ vehicles A and C are guaranteed not to collide. Is it possible for vehicle C to collide to vehicle B after vehicle A leaves the lane? The “geometry” of the problem imposes at all times the condition that:

$$x_{CB_3} \geq x_{AB_3}$$

As the safe set V_L is monotone in x_3 and vehicle A is safe with respect to vehicle B, vehicle C will also be safe with respect to vehicle B. A similar argument for vehicle D completes the proof. $\square$

For the decelerate law consider:

$$u_D = \min\{u_L^{AB}, u_S^{AE}\} \quad (45)$$

$$V_D = V_L \quad (46)$$

Proof (of Lemma 4): Lemma 4 is a direct corollary of Lemma 1 and the argument given in the proof of Lemma 5. $\square$

It should be noted that vehicle A is safe with respect to both the origin and target lanes throughout the move maneuver. Likewise, vehicles C and D are also safe with respect to both the moving vehicle A and vehicles in their own lanes. Therefore the move can be safely aborted at any stage. This is a very desirable property as it allows us to safely decouple the lanes. For example it seems advantageous to abort the move if the deceleration in target lane gets large to avoid the propagation of decelerations from lane to lane. The monotonicity of the safe set with respect to x_3 implies that occlusion of vehicles by other vehicles during a lane change does not affect safety. For example, vehicle C will have sensory information about vehicle B only after vehicle A has effectively moved out of the lane. The proof of Lemma 5 indicates that this should not be a problem from the safety point of view. Finally, note that different control laws can be used instead of u_S^{AE} in the decelerate maneuver. For example control laws producing more modest decelerations (the initial condition is likely to be extreme for the split law) may be designed. The law used is not critical from the point of view of safety.

9 Key Points and Discussion

We presented a possible design of hybrid, low level controllers for automated vehicles in platoons. The design process was such that the resulting controllers can a-priori guarantee certain aspects of the system performance (most importantly safety) without the need for further verification. A few remarks are in order, concerning the results presented here.

Design Alternatives: The results presented above constitute a safe AHS regulation layer design that supports the formation of platoons. It should be noted, however, that the analysis on which the design was based is considerably more general. Most of the calculations rely on little more than the vehicle model and are therefore applicable verbatim to other designs. For example, our calculations trivially lead to safety requirements for concepts such as autonomous vehicle operation.

Throughput Abstractions: The time it takes leaders and followers to recover from collisions (T_L and T_F respectively) as well as the spacing requirements generated by the above calculations directly lead to abstractions of the various controllers discussed here in terms of their highway space-time requirements. The impact of these results on the expected throughput is currently under investigation.

Collision Free AHS: The design presented here can easily be trimmed to fit other specifications. For example, the above calculations also indicate the requirements that the system needs to satisfy for a collision free AHS design to be possible. Such a design could involve a simple join maneuver that brings the vehicle to the boundary of the leader safe set (under the assumption that no collisions of vehicle B and vehicle C are allowed). If it turns out that this spacing is within the domain of attraction of the follower control law and is small enough to allow the communication necessary for follower operation the join can be declared complete and the follower operation can be established. A similar modification can be used for the split maneuver, where the follower law brings the vehicle to the edge of the follower safe set (or the range of the communication devices, whatever is smaller). At that point leader operation is established, provided of course that the initial condition is within the leader safe set.

These simple changes, which are easily implemented using the calculations of Sections 6 and 7, will produce a regulation layer for which *no collisions* are possible. The feasibility of the design will depend heavily on subtle issues such as the communication device range, follower law domains of attraction etc. To avoid these complications we will not investigate it further here. The calculations of Section 6 can be used to obtain the minimum communication device range/follower domain of attraction for collision free operation.

Necessary & Sufficient: The conditions obtained by solving the game theoretic problems are sufficient and necessary in the sense of being tight. They are sufficient from the point of view of controller design: they state that if the designer ensures that the initial condition lies in the safe set V_i before controller u_i is invoked and that u_i equals to the saddle input on $\mathbf{X}_C \setminus \text{int}(V_i)$, then the closed loop hybrid design is guaranteed to be safe. The need for further verification is eliminated in this case by the design procedure.

The conditions are necessary from the point of view of verification. They state that, if the discrete design does not guarantee that $x \in V_i$ when controller u_i is applied, then there exist system trajectories that violate the closed loop requirements (in this case safety).

Improving performance using coordination: In the algorithm introduced in [1] the role of inter-agent coordination is to reduce the set of allowable disturbances. This has the effect of “biasing” the game in favor of the controller and hence increasing the range of conditions under which game winning controls exist and improving the overall system performance. Here we only investigated the possibility of using coordination to limit the discrete disturbances. In particular, communication protocols were used to allow vehicle A to join/split from vehicle B, without having to worry about vehicle C hitting it from behind or vehicle B hitting the vehicle ahead of it. Similarly, timing constraints on the protocols guaranteed adequate separation between collisions to allow vehicle A to recover while executing the lead controller.

Communication can also be used to reduce the continuous disturbances (in this case the acceleration range of vehicle B). The discussion of Section 7 indicates that the safety of the join/split maneuvers is very sensitive to the relative deceleration capabilities of the vehicles involved. In fact, safe joining/ splitting may not be possible in some cases. In these cases, communication can be used to limit the set of decelerations of vehicle B, to make joining/splitting safe and improve the performance of the AHS. For example, when vehicle A contacts vehicle B with the intention of joining/splitting it may also ask for a promise that vehicle B will not decelerate faster than a certain rate (which makes the maneuver safe for the given deceleration capabilities of vehicle A). Before giving permission to start the maneuver, vehicle B would decelerate (with at most the requested rate) to create adequate spacing from the platoon ahead of it. The spacing should be such that safe leader operation can be obtained under the limited deceleration expected from vehicle B. Vehicle A can then join safely knowing that the deceleration of vehicle B will not exceed the promised value. The discrete steps of this extended communication protocol (request to join/split, acknowledge the request, etc.) will be the same as the steps of the protocol of [7], but more continuous information (deceleration promises etc.) will need to be added. The calculations of Sections 6 and 7 can be used to determine the feasibility of such maneuvers (for given ranges of sensors and communication devices) and estimate its impact in terms of highway throughput.

Refining the space requirements: The design presented here is rather conservative. We can actually do a little better by getting into the details of the protocols and the structure of the plant.

- If vehicle C is joining to/splitting from vehicle A, then the disturbance set that needs to be considered is indeed $\mathcal{D}$. However, according to corollaries 1 and 2, if vehicles A and C are not involved in a join or split maneuver, the allowable disturbances reduce to:

$$\mathcal{D}' = \{\ddot{x}_B(t) \in [d_{min}, d_{max}], (T_B, \delta v_B \in [\max\{v_a, x_4(T_B) + x_1(T_B)\}, 0]), (0, 0)\}$$

i.e. the possibility of vehicle A being rear-ended is eliminated. The reduced disturbance implies that vehicle A can follow vehicle B a little closer if it is not involved in a join or split with vehicle C. This offers obvious advantages in terms of packing more vehicles into the same length of highway. On the other hand, if this space is utilized by an appropriate design, vehicle A has to decelerate slightly to increase its spacing from vehicle B before giving permission to vehicle C to begin a join or split maneuver. The choice to use this extra space or not will probably have to be based on more global traffic considerations, such as demand, spacing between entries and exits, etc.

- Similar savings can be expected for the case of a lane change. Before moving vehicle A establishes communication with either vehicle D or vehicle E in the target lane. If communication with vehicle D is established, then vehicle D can not be involved in a join or split maneuver with the vehicle behind it. Hence the possibility of vehicle D being rear ended is again eliminated and A can change lane a little closer to D. Similarly, if communication with vehicle E is established, E can not be involved in a join or split maneuver with the vehicle ahead of it. Hence the possibility of vehicle E being involved in a collision is eliminated and A can change lane a little closer to E. Finally, as A can

not be involved in a join or split maneuver throughout the lane change, it can not be rear ended by C, therefore the pairs A–E and A–B can be allowed to be a little closer.

- The overall efficiency of the lane change maneuver can be increased by combining the lateral and longitudinal motions in order to decrease the time of completion. Currently, lane change maneuver is broken up into three parts; gap creation, gap alignment and move over. Out of these, the gap creation by vehicle D and gap alignment by vehicle A are carried out at the same time under the name of *decelerate law*. The lateral motion begins after the vehicles E-A-D have aligned themselves with the steady state safe operating condition albeit in two different lanes. The performance can be improved by initializing the lateral motion during the decelerate law, as soon as the vehicles E-A-D are “safe” with respect to each other in the sense of leader law. It can be shown that if the vehicles D and A follow trapezoidal acceleration trajectories (refer to [16]), then one can solve an optimal control problem to determine the maximum comfortable deceleration levels for the two vehicles such that the trajectories of vehicles A and D enter respective “safe” sets in minimum time and remain in the safe set from then on. This approach results in substantial (up to 40%) reduction in lane change completion time.

The above modifications are based on information that is available to vehicle A through the current communication protocols. Effectively the design is being refined by reducing the disturbance set of vehicle A (in particular eliminating the possibility of certain collisions) by interconnecting the communication protocols with the hybrid automaton of Figure 4. It should be noted that the analysis of Section 6 can be trivially modified to produce safe sets for all these cases (by setting δv_B and δv_C to zero appropriately).

Reducing the application of u_1^* : As discussed earlier, collisions of vehicles B and C may push the state of vehicle A well outside the region V_L . The system remains safe as the assumptions of the theorem guarantee that, once a collision of a certain kind has occurred, a second collision of the same kind will not occur before the system has had time to recover. Therefore, vehicle A has to deal with a reduced set of disturbances for some time after each collision. This fact can be utilized to reduce the magnitude of the inputs, as the boundary of the safe set where u_1^* needs to be applied to guarantee safety moves after a collision occurs. Points in the interior of the safe set V_2 are mapped to points in the interior of the safe set for the reduced disturbance, therefore the milder controller for the interior can again be safely applied. This modification will increase the domain of applicability of the comfortable and efficient controller. The down side is that the proofs become a lot messier, especially the part concerning the time it takes for the state to return to V_L .

Refining u_3 : In the interior of the safe sets all the standard control tricks and any intuition the designer might have can safely be used. In particular, at no extra cost, one can add:

- safety margins around the boundary of V_L ,
- smoothing functions to avoid control discontinuities

- hysteresis to avoid chattering,
- time varying and/or nonlinear controllers, or controllers based on reference trajectories,
- adaptive controllers to deal with plant uncertainties.

As long as the designer guarantees that the safety boundary ∂V_L is not crossed (e.g. by applying u_1^* on ∂V_L) all the lemmas and theorems still hold. Similarly, as long as the designer guarantees that the input does not exceed C_2 in the interior of the safe set (e.g. by using a saturation function as in (31), the control will be guaranteed to be comfortable as much as possible.

Sensor ranges: The calculations of Sections 6 and 8 can also be used to provide specifications for the enabling sensor technology. For example, one would like vehicle A to be able to stop if it detects a stopped vehicle B at the end of it's front sensor range. The calculation of Section 6 can be used to obtain specifications for the minimum front sensor range as a function of velocity (Figure 10). The figure was obtained by assuming zero initial acceleration for

Figure 10: Minimum front sensor ranges for safe operation

vehicle A ($x_2^0 = 0ms^{-2}$) and allowing one rear end collision with vehicle C. If the collision with vehicle C is eliminated the specification curve moves right by v_a . In other words, a vehicle being joined to/split from has to move slower, if no vehicle exists in its sensor range.

Similar calculations can be carried out for the adjacent lane sensors. Hopefully, the sensor technology can provide the minimum ranges required for safety at the desired speeds. If this is not the case we may still be able to do something making use of the sensors of neighboring vehicles and the communication capabilities¹⁸. For example, if the adjacent lane

¹⁸This idea is further explored in [52], where the sensors of neighboring vehicles and the communication devices are used to recover information that has been lost due to sensor faults. In [52], a vehicle may even use communication and the actuators of neighboring vehicles to recover actuation capabilities lost to faults (for example brake faults of platoon followers). Refer to [35] for details.

sensor range is smaller than the front sensor range, vehicle A in Figure 5 may be unable to detect vehicle D, but vehicle D may be able to detect vehicle A, after the middle of the maneuver. In this case safe lane changes may be carried out at higher speeds if vehicle D establishes communication the moment it detects vehicle A and forces it to abort the lane change if x_{DA} is not in V_{MD} .

References

- [1] J. Lygeros, D. N. Godbole, and S. Sastry, "A design framework for hierarchical, hybrid control." (preprint, submitted to Special Issue on Hybrid Systems of the IEEE Transactions on Automatic Control), March 1996.
- [2] P. Varaiya, "Smart cars on smart roads: problems of control," *IEEE Transactions on Automatic Control*, vol. AC-38, no. 2, pp. 195–207, 1993.
- [3] S. Shalldover, "Operation of automated guideway transit vehicles in dynamically reconfigured trains and platoons," 1979.
- [4] A. Hitchcock, "Casualties in accidents occurring during split and merge maneuvers," tech. rep., PATH Technical Memo 93-9, Institute of Transportation Studies, University of California, Berkeley, 1993.
- [5] D. V. A. H. G. Swaroop, *String Stability of Interconnected systems: an application to platooning in automated highway systems*. PhD thesis, Department of Mechanical Engineering, University of California, Berkeley, California, 1994.
- [6] B. S. Y. Rao and P. Varaiya, "Flow benefits of autonomous intelligent cruise control in mixed manual and automated traffic," *Transportation Research Record*, no. 1408, pp. 36–43, 1993.
- [7] A. Hsu, F. Eskafi, S. Sachs, and P. Varaiya, "Protocol design for an automated highway system," *Discrete Event Dynamic Systems*, vol. 2, no. 1, pp. 183–206, 1994.
- [8] B. S. Y. Rao and P. Varaiya, "Roadside intelligence for flow control in an IVHS," *Transportation Research - C*, vol. 2, no. 1, pp. 49–72, 1994.
- [9] P. Li, R. Horowitz, L. Alvarez, J. Frankel, and A. Robertson, "Traffic flow stabilization," in *American Control Conference*, pp. 144–149, 1995.
- [10] R. W. Hall, "Longitudinal and lateral throughput on an idealized highway." PATH Technical Report, Institute of Transportation Studies, University of California, Berkeley, 1993.
- [11] M. E. Broucke and P. Varaiya, "A theory of traffic flow in automated highway systems." (preprint), 1995.
- [12] P. Varaiya and S. E. Shladover, "Sketch of an IVHS systems architecture," Tech. Rep. UCB-ITS-PRR-91-3, Institute of Transportation Studies, University of California, Berkeley, 1991.

- [13] P. Ioannou, C. Chen, and J. Hauser, "Autonomous intelligent cruise control," Tech. Rep. No 92-05-01, University of Southern California, Los Angeles, 1992.
- [14] W. Ren and D. Green, "Continuous platooning: a new evolutionary and operating concept for automated highway systems," Tech. Rep. UCB/ERL-M94/24, Electronic Research Laboratory, University of California Berkeley, 1994.
- [15] J. Forbes, T. Huang, K. Kanazawa, and S. Russel, "The BATmobile: Towards a bayesian automated taxi," in *International Conference on Artificial Intelligence (IJCAI-95)*, Morgan-Kaufmann, August 1995.
- [16] D. N. Godbole and J. Lygeros, "Longitudinal control of the lead car of a platoon," *IEEE Transactions on Vehicular Technology*, vol. 43, no. 4, pp. 1125–1135, 1994.
- [17] P. Li, L. Alvarez, and R. Horowitz, "AVHS safe control laws for platoon leaders." (preprint), January 1996.
- [18] S. Sheikholeslam and C. A. Desoer, "Longitudinal control of a platoon of vehicles," in *American Control Conference*, pp. 291–297, 1990.
- [19] S. Sheikholeslam and C. A. Desoer, "Combined longitudinal and lateral control of a platoon of vehicles," in *American Control Conference*, pp. 1763–1767, 1992.
- [20] S. Sheikholeslam and C. Desoer, "Indirect adaptive control of a class of interconnected non-linear dynamical systems," *International Journal of Control*, vol. 57, no. 3, pp. 743–765, 1993.
- [21] H. Peng and M. Tomizuka, "Lateral control of front-wheel-steering rubber-tire vehicles," Tech. Rep. UCB-ITS-PRR-90-5, Institute of Transportation Studies, University of California, Berkeley, 1990.
- [22] W. Chee and M. Tomizuka, "Lane change maneuver of automobiles for the intelligent vehicle and highway systems (IVHS)," in *American Control Conference*, pp. 3586–3587, 1994.
- [23] A. Agogino, K. Gobel, and S. Alag, "Intelligent sensor validation and sensor fusion for reliability and safety enhancement in vehicle control." California PATH Research Report UCB-ITS-PRR-95-40, Institute of Transportation Studies, University of California, Berkeley, 1995.
- [24] D. Koller, T. Luong, and J. Malik, "Binocular stereopsis and lane marker flow for vehicle navigation: Lateral and longitudinal control," Tech. Rep. UCB/CSD-94-804, University of California, Berkeley, 1994.
- [25] J. C. Gerdes, D. B. Maciucă, P. E. Devlin, and J. K. Hedrick, "Brake system modeling for IVHS longitudinal control." In proceedings of DSC-Vol. 53, Advances in Robust and Nonlinear Control Systems, ASME Winter Annual Meeting, 1994.

- [26] B. Foreman, "A survey of wireless communications technologies for automated vehicle control." SAE Paper # 951928, Presented at SAE Future Transportation Technology Conference, Costa Mesa, 1995.
- [27] S. Patwardhan, *Fault Detection and Tolerant Control for Lateral Guidance of Vehicles in Automated Highways*. PhD thesis, Department of Mechanical Engineering, University of California, Berkeley, California, 1994.
- [28] D. N. Godbole, J. Lygeros, and S. Sastry, "Hierarchical hybrid control: an IVHS case study," in *Hybrid Systems II* (P. Antsaklis, W. Kohn, A. Nerode, and S. Sastry, eds.), no. 999 in LNCS, Springer Verlag, 1995.
- [29] J. Lygeros and D. Godbole, "An interface between continuous and discrete event controllers for vehicle automation," in *American Control Conference*, pp. 801–805, 1994.
- [30] F. Eskafi, D. Khorramabadi, and P. Varaiya, "SmartPath: An automated highway system simulator." PATH Technical Report UCB-ITS-94-4. Institute of Transportation Studies, University of California, Berkeley, 1994.
- [31] J. Frankel, L. Alvarez, R. Horowitz, and P. Li, "Safety oriented maneuvers for IVHS," in *American Control Conference*, pp. 668–672, 1995.
- [32] A. Puri and P. Varaiya, "Driving safely in smart cars," in *American Control Conference*, pp. 3597–3599, 1995.
- [33] J. Lygeros, D. N. Godbole, and S. Sastry, "A game theoretic approach to hybrid system design," Tech. Rep. UCB/ERL-M95/77, Electronic Research Laboratory, University of California Berkeley, October 1995.
- [34] J. Lygeros, "To brake or not to brake? is there a question?." (preprint), March 1996.
- [35] J. Lygeros, *Hierarchical Hybrid Control of Large Scale Systems*. PhD thesis, Department of Electrical Engineering, University of California, Berkeley, California, 1996.
- [36] H. B. Khalil, *Nonlinear Systems*. MacMillan, 1992.
- [37] J. R. Munkres, *Topology, a First Course*. Prentice Hall, 1975.
- [38] L. Berkovitz, *Optimal Control Theory*. Springer-Verlag, 1974.
- [39] T. Başar and G. J. Olsder, *Dynamic Non-cooperative Game Theory*. Academic Press, second ed., 1995.
- [40] J. Lewin, *Differential Games*. Springer-Verlag, 1994.
- [41] L. C. Young, *Optimal Control Theory*. Chelsea, second ed., 1980.
- [42] R. Alur, C. Courcoubetis, T. A. Henzinger, and P. H. Ho, "Hybrid automaton: An algorithmic approach to the specification and verification of hybrid systems," in *Hybrid System* (R. L. Grossman, A. Nerode, A. P. Ravn, and H. Rischel, eds.), no. 736 in LNCS, pp. 209–229, New York: Springer Verlag, 1993.

- [43] A. Deshpande, *Control of Hybrid Systems*. PhD thesis, Department of Electrical Engineering, University of California, Berkeley, California, 1994.
- [44] A. Deshpande, D. Godbole, A. Gollu, L. Semenzato, R. Sengupta, D. Swaroop, and P. Varaiya, “Automated highway system tool interchange format.” (preprint) California PATH Technical Report, Institute of Transportation Studies, University of California, Berkeley, 1996.
- [45] Y. Yang and B. Tongue, “Intra-platoon collision behavior during emergency operations,” *Vehicle System Dynamics*, vol. 23, no. 4, pp. 279–292, 1994.
- [46] F. M. Callier and C. A. Desoer, *Linear System Theory*. Springer-Verlag, 1991.
- [47] S. Sheikholeslam, *Control of a class of interconnected nonlinear dynamical systems: The platoon problem*. PhD thesis, Department of Electrical Engineering, University of California, Berkeley, California, 1991.
- [48] D. N. Godbole, J. Lygeros, E. Singh, A. Deshpande, and A. Lindsey, “Design and verification of coordination layer protocols for degraded modes of operation of AHS,” in *IEEE Control and Decision Conference*, pp. 427–432, 1995.
- [49] J. Lygeros, D. N. Godbole, and M. E. Broucke, “Extended architecture for degraded modes of operation of IVHS,” in *American Control Conference*, pp. 3592–3596, 1995.
- [50] H. Peng and M. Tomizuka, “Vehicle lateral control for highway automation,” in *American Control Conference*, pp. 788–794, 1990.
- [51] D. N. Godbole, F. Eskafi, E. Singh, and P. Varaiya, “Design of an entry and exit maneuvers for AHS,” in *American Control Conference*, pp. 3576–3580, 1995.
- [52] J. Lygeros, D. N. Godbole, and M. E. Broucke, “Towards a fault tolerant AHS design.” SAE Paper # 951894, Presented at SAE Future Transportation Technology Conference, Costa Mesa, 1995.

A Simulation Plots

Figure 11: State trajectory under maximum braking

Figure 12: Maximum braking by vehicle A, worst case d

Figure 13: State trajectory under the inputs of Figure 12

Figure 14: Saddle solution (u_0^*, d_0^*)

Figure 15: State trajectory under (u_0^*, d_0^*)