QUALITATIVE ANALYSIS, MODEL CHECKING, AND CONTROLLER SYNTHESIS OF HYBRID SYSTEMS

by

Mireille Esther Broucke

Memorandum No. UCB/ERL M00/35

22 June 2000

QUALITATIVE ANALYSIS, MODEL CHECKING, AND CONTROLLER SYNTHESIS OF HYBRID SYSTEMS

by

Mireille Esther Broucke

Memorandum No. UCB/ERL M00/35

22 June 2000

ELECTRONICS RESEARCH LABORATORY

College of Engineering
University of California, Berkeley
94720

Qualitative Analysis, Model Checking, and Controller Synthesis of Hybrid Systems

by

Mireille Esther Broucke

B.S. (University of Texas at Austin) 1984
M.S. (University of California, Berkeley) 1987

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Engineering:
Electrical Engineering and Computer Sciences

in the

GRADUATE DIVISION
of the
UNIVERSITY of CALIFORNIA at BERKELEY

Committee in charge:

Professor Alberto Luigi Sangiovanni-Vincentelli, Chair
Professor Maria Domenica Di Benedetto
Professor Charles C. Pugh

Spring 2000

The dissertation of Mireille Esther Broucke is approved:

Chair Date

Date

Date

University of California at Berkeley

Spring 2000

Qualitative Analysis, Model Checking, and Controller Synthesis of Hybrid Systems

by

Mireille Esther Broucke

Abstract

Qualitative Analysis, Model Checking, and Controller Synthesis of Hybrid Systems

by

Mireille Esther Broucke

Doctor of Philosophy in Engineering:
Electrical Engineering and Computer Sciences

University of California at Berkeley

Professor Alberto Luigi Sangiovanni-Vincentelli, Chair

This thesis addresses problems of qualitative analysis, model checking, and controller synthesis of hybrid systems. The contributions are the following. We derive conditions for completeness of the space of non-Zeno hybrid trajectories accepted by a hybrid automaton. We derive conditions for continuous selections of hybrid trajectories, which had been elusive due to the inherent discontinuities permitted by hybrid systems. These results provide tools for qualitative analysis and are obtained in the general setting of hybrid systems with differential inclusions. Next, we present a new method of obtaining bisimulations for hybrid systems which is inspired by a geometric interpretation of the bisimulation for timed automata. This provides a much needed breakthrough for applying model checking to hybrid automata with non-trivial dynamics. We demonstrate the method through examples drawn from coordinated autonomous agent applications and from widely used models such as linear systems. Next, we turn to problems of controller synthesis. We present a theory of optimal controller synthesis for continuous time and hybrid systems using bisimulation. The resulting formulation leads to a dynamic programming problem on a finite graph. We obtain an single-pass algorithmic solution to this problem. Finally, we consider strategies for model checking when we do not have the benefit of bisimulation, as in hybrid systems with differential inclusions. We present a new intuitive proof of decidability of reachability

for rectangular automata.

Professor Alberto Luigi Sangiovanni-Vincentelli
Dissertation Committee Chair

Contents

List of Figures

Acknowledgements

Without a doubt the smartest move I made in the PhD, and the proof that I deserve my degree, occurred when I asked Alberto Luigi Sangiovanni-Vincentelli to be my advisor. He is the pivot point around which my hope spins. Alberto nurtured, bolstered, and scared me, made me *want* to set my alarm clock, was not easily convinced, is clever at multi-tasking, defined a fence but kept the gates open, noted my deficiencies, paced and induced pacing, administered reality checks... all the while leaving my assurance intact and my motivation bigger. There is a finesse to his advising that I did not master but smile about. His plenary talk at the 1999 CDC is unforgettable - he delivered a transformative vision with a retinue of sound effects and comic strips[1], like a good-tasting medicine badly needing to be taken. Alberto's finger information was a source of comfort to me, though it was usually outdated. Through Alberto I made two extended visits to Parades in Rome, something I will cherish for the rest of my career. The conditions that made this experience possible are centered on an international research community's belief in the triumvirate he comprises: insight into what is relevant, drive to be an agent of change in systems design, and technical know-how to make change possible.

The other half of my smartest move is that I gained the mentorship of an equally supportive advisor, Marika Di Benedetto, who, despite her obligations on multiple campuses, gave this work her careful evaluation and provided her always meaningful feedback. I was so lucky to have an advisor who would say things that conveyed a sense of immediate coherence (the "aha factor"). She is role model whom I hope to emulate.

Several professors at Berkeley helped me move forward in my research. I thank my qualifying exam committee: Robert Brayton, Karl Hedrick, Charles Pugh, and Alberto Sangiovanni-Vincentelli for their attentive regard and affirming feedback. I thank my dissertation committee: Marika Di Benedetto, Charles Pugh, and Alberto Sangiovanni-Vincentelli for their insightful reading of this thesis.

I had the good fortune of interacting with a number of people in Berkeley's exciting Math department. Foremost I thank Charles Pugh for contributing to my PhD experience in so many positive ways. Charles generously shared his time to contemplate and sharpen mathematical problems brought to him in amorphous form; and he did so with an acuity that

[1] thus touching the souls of the Belgians present

is exhilarating. I also thank André de Carvalho, Alan Weinstein, and Nikolai Reshetikhin for their interest and time in fielding my math questions.

I thank Tom Henzinger for our discussions which enabled me to appreciate his insight into reactive and hybrid systems. Two papers by Tom provided the spark for much of my research. Armed with a student's wooden tools of analysis and geometry, I took the first steps to reinterpret and extend his results and Alur and Dill's work for timed automata, which were rooted in a trust of formal logic.

I thank Pravin Varaiya who contributed several of the ideas appearing in Chapter 2. I thank Antonio Ornelas for sending his papers, which provided the crucial result needed for differential inclusions. John Canny and James Renegar answered all my computational geometry questions, which I regret did not get enough attention in this thesis (due to insufficient brain resources). Michael Singer provided guidance on decision procedures for local first integrals.

I thank my colleagues Andrea Balluchi, Soheila Bana, Luca Benvenuti, Michael Branicky, Akash Deshpande, Stephano di Gennaro, Farokh Eskafi, Datta Godbole, John Lygeros, George Pappas, Claudio Pinello, Anuj Puri, Sonia Sachs, Raja Sengupta, Slobodan Simic, Joao Sousa, Lixin Su, Tiziano Villa, and Howard Wong-Toi for stimulating and enjoyable discussions and collaborations.

Several UC Berkeley staff touched my trajectory in memorable ways. Maureen Master supplied the truly hilarious moments of my stay in Cory Hall. Her pencil-sharp satiric wit still evokes awe and abandon in me. Carla Trujillo's reinforcing words gave me courage when I needed it, and her financial support pulled me through. Brad Krebs mitigated my "Y2K bug" crises with aplomb. Jeff Wilkinson made me appreciate the pliability of the medium of time. Peggye Brown's kindness was a vertex of the friendly ambiance of the Berkeley CAD group. It is impossible to imagine navigating the degree requirements without the empathetic Ruth Gjerdes.

My (extended) education has been influenced by several people. I thank Tinsley Oden for clarifying, at a tender juncture, the difference between qualitative and quantitative, and Ari Arapostathis, whose vital way of teaching drew me to system theory. Tom Parker taught

me good programming style and dynamics.

I had the pleasure of working with many of the researchers in PATH's AVCS program, an incomplete list including Pravin Varaiya, Roberto Horowitz, Jason Speyer, Benson Tongue, Alex Skabardonis, Oliver O'Reilly, Karl Hedrick, Masayoshi Tomizuka, Randy Hall, and Petros Ioannou. I thank each of them for the shared learning experience.

I thank George Lakoff of the Berkeley Linguistics Department for his metaphors. His provocative ideas have crept like music into my conscience.

Two people stand out for the lasting impression they have made on me. I thank Jim Morehead for making me laugh, for his integrity, for the joy that comes from knowing him. And I thank Cormac Conroy for his loyalty, his reading of Eliot, and his empathy, which is unmatched.

I thank Sonia Sachs for her courage and laughter, and Denise Wolf, for her wit and grasp of the complex. Without Barbara Mills' penetrating analyses I would not be the same person. From Texas Gary Smith brightened my days with his enthusiasm for knowledge.

I thank Eleni Arapostathis for her open-heartedness and hospitality while I was in Greece; and my extended family for their hospitality while I was in Belgium.

I am grateful to my parents, Ingrid, and Daniel for their love and support. I was kept aglow in the bright rays of Isabel and Alexandra.

Most of all I thank Ari for his warmth and humanity, which sustained each hour, and for the sense of well-being he gave me.

Chapter 1

Introduction

The guts of any fiction is an anguished question.
- Wallace Stegner.

This thesis is concerned with a class of models called *hybrid systems* which evolved out of a synergy between control theory and verification in computer science. The model has been a topic of research for at least ten years though it is fair to say that our understanding of it is in a nascent state.

At Berkeley hybrid systems came to the forefront of systems research by way of applications. The term "hybrid dynamical system" probably first appeared in [45] and was used to model the regulation and coordination layer of a hierarchical architecture for automated highways [98]. Following that example a hierarchical architecture for air traffic management employed hybrid automata in an analogous way [95]. In the embedded systems domain, *embedded controllers* are modeled as hybrid automata [85].

On a separate front, hybrid systems appeared in the form of *switched systems*, a model fueled by numerous applications in mechanical and electrical engineering systems where switching phenomena are inherent or where only switching control strategies can do the job. Some of this research is reported in [70].

Elsewhere hybrid systems arose as an extension of timed automata in verification. Computer scientists realized the need to characterize real time processes using dense time, and this foray into the realm of the infinite lead to a watershed of models: timed, multirate, and rectangular automata, integration graphs, linear hybrid automata, and hybrid automata [4, 79, 56, 2, 64]. A key requirement is that these models admit a form of algorithmic (and non-approximative) analysis, and this was achieved for all of them, with the exception of

hybrid automata.

The state of affairs at the beginning of this research was that large-scale, widely relevant, and highly visible applications of hybrid systems were already in place. What the model would *do* or what is involved in designing systems based on such a model was only vaguely appreciated. That appreciation leaned heavily on hybrid automata with naive dynamics such as timed and rectangular automata, or on older methods in control theory such as stability and controller design for linear systems. This state of affairs, though perfectly understandable, was hardly satisfactory. It has been impossible to bring new techniques to applications without a dedicated theoretical study of the model, and relying on old ways to solve new problems has masked the power and expressiveness we gained from the model.

We felt it necessary to put aside the applications for a time and study what is the object before us. We will agree that the applications are of uncontestable relevance. The decision to study hybrid systems from a theoretical viewpoint is motivated not only by applications, but also by intrinsic factors about the model.

1.1 Paradigm Shifts

We were motivated by an appraisal of the paradigm shifts that hybrid systems represent. Here are those paradigm shifts:

1. A shift away from models that live only in one domain such as discrete event, continuous, stochastic, continuum, finite state, etc. to heterogeneous models [58].

2. A shift away from a centralized control scheme to autonomous and decentralized operation. (There has already been a trend to study decentralized problems in system theory, but that trend moved toward aggregate stochastic models for large-scale systems).

3. A shift away from either the purely deterministic or purely stochastic to models with *non-determinism*. This requires a new mindset not of what *will* happen or of what happens *on average* but of what *can* happen, the latter being a more realistic view for autonomous and embedded systems.

4. A shift away from purely continuous control design to designs that specifically rely

on switching to achieve performance requirements or which give up on smoothness, differentiability, or continuity to model discrete phenomena. Discrete-event dynamical systems reflect this shift.

5. A shift away from defining the state of a system as a point in the state space to a state being a region or equivalence class of the state space. Indeed individual trajectories or points can overwhelm us with information when all we really need to know is *in general* what is the "state" of the system. This has lead to the study of systems which are *abstractions* of other systems. These abstractions are usually quotient systems with some desirable property such as finiteness. Formerly there were attempts to form abstractions using aggregations of state values or using reduction techniques which ignore part of the state space. The new approach to abstraction is contributed by verification in computer science.

6. A shift away from analysis of steady-state phenomena to analysis of reactive, concurrent, and transient phenomena.

These paradigm shifts may seem unastounding [1] but they strain existing methods enough that we are forced to break with tradition and start afresh. Our mental pictures are new ones, albeit influenced by what we know, and the outcome is not certain.

Given these paradigm shifts, we ask, why do they lead to a model which is at once timely, meaningful, and having the potential to make an impact? We provide a series of arguments about why this model is the correct one to study *now*.

First, we argue there is historical precedent for the study of systems which exhibit discontinuous behavior, namely, approaches such as sliding mode or variable structure control [97], impulse control [15], and more recently switched systems [70] and control based on nonsmooth analysis [34]. What has been lacking in these models is a way to systematically characterize the *logic* part of the switching behavior. This limitation kept each of these models from becoming a mainstream engineering tool either because the model needed to be tailored to each application or it was interpreted as a purely mathematical entity. The historical efforts to characterize discontinuity in system theoretic models suggests that a more encompassing framework is needed. The trick all along has been to generalize the

[1] It can be argued that postmodernism is an example of an unastounding paradigm shift.

framework enough without introducing so much generality than analysis is no longer possible. The hybrid automaton framework seems, so far, to achieve a good balance.

The second argument concerns the fact that important theoretical results have shown that discontinuous phenomena are unavoidable in control theory. First, the Bang Bang theorem for time optimal control and the Pontryagin maximum principle show that piecewise constant controls can be a sufficiently rich class to achieve control objectives. Many results in geometric control theory [55] illuminate the importance of piecewise constant controls. Finally, there is Brockett's famous result that controllability does not imply the existence of a stabilizing continuous control law [21].

A third argument that these paradigm shifts are the right ones is from a view of theoretical development as an end in itself. In this view we see modern control theory progressing from linear systems analysis using Kalman's state space approach, optimal control and dynamic programming, local nonlinear control based on Frobenius theorem and the Lie algebra of vector fields, and discrete event dynamical systems. What would be the obvious next steps for the theory? There are four choices: (1) globalize the nonlinear theory, (2) integrate optimal control with the nonlinear theory in a coherent framework, (3) integrate the discrete-event view with the continuous-time view, and (4) invent something completely different. Barring the appearance of new methods like learning algorithms which seem to go in the direction of (4), it turns out that using the hybrid automaton model we have the potential to achieve the first three of these ends. We can think about the globalization of nonlinear control in terms of coordinate charts on a manifold. A flow is defined on each coordinate neighborhood, and we view the hybrid automaton as providing the rules for gluing the neighborhoods together. As for the second choice, we seek a way to encode the (inherently discontinuous) optimal control as a switching strategy between locations of the automaton. We will get some flavor of this idea later in the thesis.

A fourth argument is from the humanistic viewpoint. It cannot be overlooked (though it usually is in scientific circles) that the pursuit of knowledge is an activity not parametrized only by objectivity. The pursuit of knowledge is an activity which keeps men and women mentally occupied, and the qualitative types of knowledge we pursue has everything to do with who we are. Within each strand of inquiry there are different types of voices. A rich inquiry is one that benefits from a multitude of types who are in constant tension with each other. Control theory has, in my view, been starved of different visions, and this has kept it

from being appreciated in a wider sphere. The phenomenon that is occurring before us is a very human one in which a new voice is being injected into system theory. That voice brings its particular, preexisting sensitivities: to syntax, to logic, to language expressiveness, to non-determinism and chance, and to event-driven, discrete phenomena.

A fifth argument that these paradigm shifts are the right ones is that the new model enables us to *pose* and hopefully solve problems that we have been unable to pose before. This argument on behalf of hybrid automata may be the most compelling yet. The situation can be likened to the story of Bertrand Russell, who upon exclaiming to Lady Ottoline "I love you", realized that indeed he loved her. What we understand in the world are those things for which we have a means of expression.

One might say that it is more important to develop tools to solve existing problems. This is valid. There are many control problems which are solved in ad hoc ways because the theory cannot address them. Hybrid systems may help to alleviate this gap between theory and practice. But more interesting are new methods that allow the possibility to dream up new problems. They are, like an enzyme, essential enablers of lively scientific growth. Thus, as we go into the study of hybrid automata we must constantly be on the lookout for new problems that can be posed with the model. For instance, drawing from the connection between logic and automata, we can now state specifications of a system in terms of temporal logic thus inheriting a rich semantics for transient phenomena. Some results of this flavor have filtered into the literature, especially in robotics [9].

Finally, we must say a word about applications; namely a list of applications where the hybrid systems model is helpful, if not essential.

- **Coordinated autonomous agents** These are problems where dynamic agents such as robots, underwater vehicles, automobiles, aircraft, satellites, and other unmanned vehicles operate autonomously but collude to achieve a high level goal. See for instance [57] and [91]. Formerly there was no control theoretic way to discuss *liveness*, *fairness*, or *no deadlock* inspite of the fact that these are exactly the sort of specifications one wants to consider in a coordinated autonomous agent problem.

- **Switched systems** We have already mentioned that switched systems arise naturally in mechanical systems, such as engine control, and in electrical systems, such as switching power converters.

- **Nonlinear control systems** As already mentioned the objective here is to globalize nonlinear controllers. See [68]. The swinging up of a pendulum is one example [7]. Another example is nonholonomic control systems which cannot be stabilized by continuous controllers [18].

- **Embedded systems** In these systems there need not be inherent discontinuities but the environment in which the controller operates has mixed continuous and discrete components and the controller is a discrete supervisor implemented in software. The environment imposes events to which the controller must *react* in real time.

1.2 Overview of the thesis

In Chapter 2 we introduce the hybrid automaton model and several variants of it including timed and rectangular automata. We turn to the study of hybrid trajectories for which few results exist. We present three results. First we propose a metric for hybrid trajectories given by the Skorohod metric for stochastic processes. Using this metric we define several candidate metrics and pseudo-metrics for the space of trajectories accepted by a hybrid automaton. Then we give a result for completeness of the metric space of hybrid trajectories. This result in essence gives conditions when the limit of a Cauchy sequence of trajectories is both (1) non-Zeno, and (2) accepted by the automaton. This tool can be useful in further analysis of hybrid trajectories. Finally, we give conditions for the existence of continuous selections of trajectories of hybrid automata defined with Lipschitz inclusions. This result relies on the theory of Lipschitz inclusions and the Skorohod metric.

Chapter 3 is concerned with the problem of *model checking* for hybrid automata. Model checking, roughly speaking, involves automatically checking that a model satisfies a specification. It differs from simulation in that all initial conditions must be checked, and it differs from verification in that algorithmic analysis methods are sought that are usually automata-theoretic. A typical problem posed in model checking is the *safety problem*: Given hybrid automaton A determine if an unsafe set of states P can be reached from an initial set of states Q. The approach to model checking developed in Chapter 3 is to construct a *finite bisimulation*, which is an equivalence relation on the hybrid state space. If this equivalence relation has a finite number of cosets, then the quotient system is a finite automaton, and in this manner, problems about hybrid automata are reduced to problems about finite

automata. Our method is based on a geometric interpretation of the bisimulation for timed automata which allows us to extend the class of hybrid automata with finite bisimulations to ones with interesting dynamics. In the process we obtain an analytical representation of the bisimulation which then forms the *symbolic execution theory* for the hybrid automaton. In Chapter 4 we give examples drawn from coordinated autonomous agents, embedded systems, and hybrid systems with integrable Hamiltonian dynamics and linear dynamics.

In Chapter 5 we turn to problems of synthesis. We consider the synthesis of optimal controls for continuous feedback systems by recasting the problem to a hybrid optimal control problem, which is to synthesize optimal enabling conditions for switching between locations in which the control is constant. An algorithmic solution is obtained by translating the hybrid automaton to a finite automaton using a bisimulation and formulating a dynamic programming problem with extra conditions to ensure non-Zenoness of trajectories. We show that the discrete value function converges to the viscosity solution of the Hamilton-Jacobi-Bellman equation as a discretization parameter tends to zero. Then we show that an efficient single-pass algorithmic solution of the dynamic programming problem is obtained by a non-deterministic version of the Dijkstra algorithm. Finally we give examples of the method.

In Chapter 6 we demonstrate the importance of strategies without bisimulation using the example of rectangular automata, which do not have a finite bisimulation; nevertheless, the reachability problem is decidable. We give a new proof of decidability based on a direct analysis of the steps involved in symbolic model checking.

In Chapter 7 we say our final words.

Chapter 2

Hybrid Model and Trajectories

who pays any attention
to the syntax of things
will never wholly kiss you;
- ee cummings

2.1 Introduction

We begin with the syntax and semantics of hybrid automata and several variants which will appear in the thesis. We then turn to hybrid systems with Lipschitz differential inclusions and investigate the existence of continuous selections of trajectories with respect to the initial conditions. In order to study continuity in a setting where trajectories can change discontinuously due to resets of the hybrid system, we introduce the Skorohod metric as a suitable metric for hybrid trajectories. We define a metric on the set of trajectories accepted by the hybrid automaton and present conditions when this metric space is complete. Finally, the existence of continuous selections with respect to this metric is proved under relatively mild assumptions.

2.1.1 Motivation

Little work has appeared in the literature on hybrid systems studying their qualitative behavior. Partly this is a difficult task for hybrid systems permit a wide array of behaviors, each of which can be the subject of a deep investigation. We introduce some necessary analytical tools and take a fundamental step by demonstrating the existence of continuous selections of trajectories of hybrid automata with Lipschitz differential inclusions with re-

spect to initial conditions. Once such basic properties of hybrid trajectories are derived we hope to establish new connections between observation equivalences of hybrid automata, including those that are bisimulations, and qualitative features of trajectories starting from equivalent points. This research agenda was begun in [22].

An early paper by Witsenhausen [102] considers a model for switching between vector fields. The model eliminates non-determinacy by assuming that transitions are taken at the first time the enabling condition is reached, enabling conditions are non-overlapping (also a non-Zeno condition), and the reset map is the identity. The present work is a generalization as we permit non-determinacy in several features of our model: (1) the dynamics follow a differential inclusion, (2) multiple enabling conditions (thus, multiple edges) can be reached from a state, (3) a transition can be taken at any time while an enabling condition is enabled, or not at all, and (4) the reset map is non-deterministic. A paper by Tavernini [94] considers a hybrid system with differential equations in each location. The paper obtains a result on continuity with respect to initial conditions based on a transversality condition at the boundary of the enabling conditions. Our result on continuity with respect to initial conditions generalizes this work as we allow non-determinacy and consider differential inclusions. We require a result by Cellina and Ornelas [30] on continuous selections of Lipschitz inclusions and a more general transversality condition suitable for inclusions. Finally, the paper by Gupta et. al. [47] introduces a metric for finite trajectories of timed automata.

2.1.2 Notation

x' refers to the updated value of a variable x after a transition is taken. $\mathbb{I}(\cdot)$ is the indicator function. We denote by $|\cdot|$ the Euclidean norm and by $d(x,B)$ the distance from a point x to a set B defined by $d(x,B) = \inf_{y\in B}|x-y|$. $B(x,r)$ denotes the open ball centered at x of radius r. $cl(A)$ denotes the closure of set A. The Hausdorff distance between two compact sets d_H is $d_H(A,B) = \max\{\sup_{x\in A} d(x,B), \sup_{y\in B} d(y,A)\}$. For an interval $I = [t_0,t_1]$, let $C(I)$ and $C_{ac}(I)$ denote the spaces of continuous and absolutely continuous functions $f : I \to \mathbb{R}^n$, endowed with the sup norm $\|f\|_\infty$ and the norm $\|f\|_{ac} = |f(t_0)| + \int_I |\dot{f}(s)|ds$, respectively. We denote by $\mathcal{L}^1(I)$ the Lebesgue integrable functions on I. χ_E is the characteristic function of the set E.

All manifolds, vector fields, curves and maps are of class C^∞. Manifolds are assumed to be connected, paracompact, and Hausdorff. $C^\infty(M)$, $\mathcal{X}(M)$, and $\Omega^k(M)$ denote the sets of

smooth real-valued functions, smooth vector fields, and k-forms defined on a manifold M. Finally, $\mathcal{F}(\mathbb{R}^n)$ denotes the space of differential inclusions on $\mathbb{R}^n$ and $\mathcal{D}(I, \mathbb{R}^n)$ the space of all functions $f : I \to \mathbb{R}^n$ that are left continuous, $\lim_{t \uparrow a} f(t) = f(a)$, and have limits from the right.

2.2 Hybrid Automata

A *hybrid system* is a dynamical system consisting of one or more components called hybrid automata. A *hybrid automaton* is a tuple

$$H = (L, M, \Sigma, E, X, G, R)$$

with the following elements:

State space L is a finite set of automaton locations and M is a compact n-dimensional manifold with or without boundary consisting of $|L|$ connected components. Corresponding to each $l \in L$ is the component M_l of M.

Events Σ is a finite set of observations or control events. When we interpret the automaton as an open-loop system, the control events are partitioned into uncontrolled events Σ_u, which are supplied by the environment and controlled events Σ_c, which are supplied by a controller. When we interpret the automaton as an uncontrolled system the events record observations which need not be unique to each edge.

Edges E is a set of edges or control switches. $e = (l, \sigma, l')$ is a directed edge between a source location l and a target location l' with observation $\sigma \in \Sigma$. If H is an open-loop system then we partition E in the set of controlled edges E_c and the set of uncontrolled edges E_u.

Vector field $X \in \mathcal{X}(M)$ is a smooth tangent vector field on M. The vector field restricted to component M_l is denoted X^l.

Enabling conditions $G : E \to \{g_e\}_{e \in E}$ is a function assigning to each edge an enabling (or guard) condition $g \subseteq M_l$. We use the notation $G(e) = g_e$.

Reset conditions $R : E \to \{r_e\}_{e \in E}$ is a function assigning to each edge $e = (l, \sigma, l') \in E$ a reset condition, $r_e : M_l \to 2^{M_{l'}}$, where we use the notation $R(e) = r_e$.

2.2.1 Semantics

The *state* of the hybrid automaton is a pair $(l, x) \in l \times M_l$. $\Sigma(l)$ denotes the set of events possible at $l \in L$ and $E(l)$ denotes the set of edges possible at $l \in L$. Trajectories of H evolve in *steps* of two types. A *σ-step* is a binary relation $\xrightarrow{\sigma} \subset (L \times M) \times (L \times M)$ and we write $(l, x) \xrightarrow{\sigma'} (l', x')$ iff (1) $e = (l, \sigma', l') \in E$, (2) $x \in g_e$, and (3) $x' \in r_e(x)$. Define $\phi_t^l(x)$ to be the trajectory in location l, starting from x and evolving for time t. A *t-step* is a binary relation $\xrightarrow{t} \subset (L \times M) \times (L \times M)$, and we write $(l, x) \xrightarrow{t} (l', x')$ iff (1) $l = l'$, and (2) for $t \geq 0$, $x' = \phi_t(x, \sigma)$, where $\dot{\phi}_t(x) = X^l(\phi_t(x, \sigma), \sigma)$.

A *trajectory* or *orbit* π of H is a finite or infinite sequence $\pi : q_0 \xrightarrow{\tau_0} q_1 \xrightarrow{\tau_1} q_2 \xrightarrow{\tau_2} \cdots$ where $q_i \in L \times M$ and $\tau_i \in \Sigma \cup \mathbb{R}^+$. A trajectory is *accepted* by H if each step $q_i \xrightarrow{\tau_i} q_{i+1}$ is a t-step or σ-step of H. A *run* of H is the projection to the discrete part of a trajectory accepted by H; namely, a finite or infinite sequence $l_0, l_1, l_2, \ldots$ of admissible locations. A k-step run is a run of length k.

We want to exclude pathological trajectories of H, such as those that exhibit finite escape time for the continuous state, or admit an infinite number of σ-steps in a bounded time interval (i.e., lack of a *non-Zeno* condition). Therefore, we define the *trajectory language* Π as the set of trajectories accepted by H whose continuous trajectory belongs to $\mathcal{D}(\mathbb{R}_+, \mathbb{R}^n)$ and has a finite number of σ-steps in any bounded interval of time.

Assumption 2.2.1. For each e, e' in E, g_e is a closed set, r_e has closed values and

$$d(r_e(g_e), g_{e'}) > 0\,. \tag{2.2.1}$$

Assumption 2.2.1 combined with the vector field being Lipschitz continuous ensures that any trajectory of H, whose continuous trajectory belongs to $\mathcal{D}(\mathbb{R}_+, \mathbb{R}^n)$, satisfies the non-Zeno condition and has no finite escape time.

Remark 2.2.1.

1. An alternative concept of non-Zenoness is uniform non-Zenoness. H is *uniformly non-Zeno* if for any trajectory $\pi \in \Pi$, π has at most N_H control switches in any unit time interval. Notice that Assumption 2.2.1 is stronger: on a compact domain, the Lipschitz vector field is uniformly bounded, and there is a minimum distance $d(r_e(g_e), g_{e'})$ appearing in Assumption 2.2.1, so we can find a duration $\Delta > 0$ such that between any two σ-steps at least Δ units of time elapse.

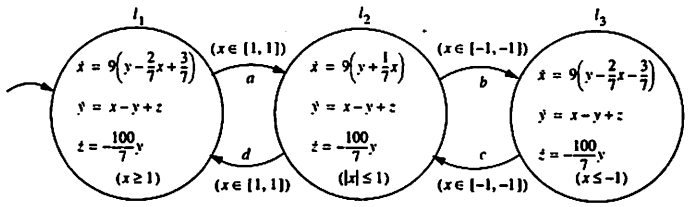

Figure 2.1: Double scroll hybrid automaton.

2. In the sequel we frequently view the trajectory as progressing in steps, where a *step* refers to a t-step followed by a σ-step. Associated with the kth step of a trajectory is the data $I^0 = [0, t^1]$ or $I^k = (t^k, t^{k+1}]$, for $k \geq 1$, the time interval of the step, $\tau^k = t^{k+1} - t^k$, its duration, and $q^k = \left(l^k, x^k(t)\right)$, the state, where l^k is fixed over I^k. Thus, the step can be represented as

$$(l^k, x^k) \xrightarrow{\tau^k} (l^k, x^k(t^{k+1})) \xrightarrow{\sigma} (l^{k+1}, x^{k+1}), \tag{2.2.2}$$

where $x^k(t^{k+1})$ denotes the value of the continuous state before the reset.

2.2.2 Example

Consider the hybrid automata of Figure 2.1. The invariants for locations l_1, l_2, l_3 are $x \geq 1, |x| \leq 1, x \leq -1$, respectively. The dynamics in each location are either affine linear or linear. It has been shown that this hybrid automaton has a homoclinic orbit and by Shilnikov's theorem the system has a Smale horseshoe implying the existence of a chaotic attractor [31].

2.2.3 Special classes of hybrid automata

We will encounter several special classes of hybrid automata.

Among the simplest is *timed automata* [4], a subclass in which the continuous dynamics define the *clock flow*, $\dot{x}_i = 1$. The *distinguished sets*: enabling, reset, invariant, initial, and final conditions, are built up from finite conjunctions and disjunctions of the formulas $x\%c$ where $\% \in \{<, \leq, =, >, \geq\}$ and $c \in \mathbb{Z}$.

Rectangular automata are a natural extension of timed automata [79]. They have the same syntax for their distinguished sets but allow more expressiveness in the dynamics. The

dynamics of the ith clock component is given by the rectangular inclusion $x_i \in [a_i, b_i]$, where $a_i, b_i \in \mathbb{R}$, which effectively models uncertainty or drift in the clocks. Rectangular automata have also been used to over-approximate vector fields [53].

Deterministic hybrid automata are hybrid automata which disallow non-determinism and have no external control events. The new restrictions are: (1) for each $l \in L$, $g_e \cap g_{e'} = \emptyset$, for all $e \neq e' \in E(l)$, (2) edges are taken at the first time they are enabled (hence interiors of enabling conditions can be ignored), (3) the reset maps are single-valued (including the empty set), and (4) there are no external events determining which edges are taken. This allows the model to operate or be viewed as completely autonomous.

These restrictions allow us to give the following more elegant definition. A deterministic hybrid automaton is a triple

$$H = (M, X, r)$$

where M and X are as above and r is a map from the boundary of M to the space of subsets of M. The (finite) components of M correspond to the locations of the automaton. r can be used to determine the edges of the automaton. There is an edge from l to l' if there exists $x \in M_l$ such that $r(x) \in M_{l'}$. The enabling condition of an edge consists of those $x \in M_l$ such that $r(x) \in M_{l'}$, and the reset condition is the restriction of r to the enabling condition.

Remark 2.2.2.

1. In the case of deterministic hybrid automata we can define trajectories that extend in forward and backward time. A *full trajectory* or *full orbit* of a deterministic hybrid automaton H is a bi-infinite sequence of σ- and t-steps accepted by H.

2. Suppose we are given a diffeomorphism $f : N \to N$, where N is a compact, connected manifold. We can define a deterministic hybrid automaton which is a Smale suspension of f [89]. Let I be the unit interval and define $M = N \times I$. The *Smale suspension* of f is the translation vector field X given by $\frac{\partial}{\partial y}$, where y is the coordinate of I. At $z = (x, 1)$, $r(z) = (f(x), 0)$, while r evaluates to the empty set for $y < 1$. This yields a hybrid automaton with a single location whose dynamics are given by X and with and an edge from the location to itself with the enabling condition $M \times \{1\}$. Thus, *deterministic hybrid automata are generalizations of Smale suspensions.*

In the next section we will encounter hybrid automata whose continuous dynamics are defined by Lipschitz differential inclusions evolving on $M = L \times \mathbb{R}^n$. Namely the X component of the hybrid automaton defined above is replaced by:

Differential Inclusion $X \in \mathcal{F}(\mathbb{R}^n)$ is a differential inclusion. X restricted to $l \times \mathbb{R}^n$ is denoted F_l.

2.3 Topologies for hybrid systems

We introduce suitable topologies for hybrid trajectories, using the Skorohod metric. The Skorohod metric was originally used in the study of stochastic processes with right (or left)-continuous sample paths, such as Poisson processes [17]. This metric is denoted by $d_s(\cdot,\cdot)$ and is defined as follows. Given two functions $f \in \mathcal{D}(I_f, \mathbb{R}^n)$ and $g \in \mathcal{D}(I_g, \mathbb{R}^n)$, $d_s(f,g)$ is the infimum of $\epsilon > 0$ for which there exists a strictly increasing, continuous, surjective function $\kappa : I_f \to I_g$ such that

(a) $\sup_{t \in I_f} |\kappa(t) - t| \leq \epsilon$ and

(b) $\sup_{t \in I_f} |f(t) - g(\kappa(t))| \leq \epsilon$.

2.3.1 The pseudo-metric space (Π, d^m)

We define a topology on Π via a family of pseudo-metrics that combine the Skorohod metric on the continuous parts of a pair of trajectories with the distance between the corresponding runs in the Cantor topology.

Let $\pi, \tilde{\pi} \in \Pi$ with $\pi = \left\{l^k, x^k(t)\right\}_{k=0}^{\infty}$ and $x(t) = \left\{x^k(t)\right\}_{k=0}^{\infty}$ referring to the entire continuous trajectory, where $x^k : (t^k, t^{k+1}] \to \mathbb{R}^n$. We adopt the analogous notation for $\tilde{\pi}$. Let $x^{(m)}, \tilde{x}^{(m)}$, $m \geq 1$, denote the restriction of $x, \tilde{x}$ on $[0, t^m]$ and $[0, \tilde{t}^m]$, respectively. We define the pseudo-metric $d^m(\cdot,\cdot)$ by

$$d^m(\pi, \tilde{\pi}) = d_s(x^{(m)}, \tilde{x}^{(m)}) + \sum_{k=0}^{m-1} \frac{1}{2^k} \mathbb{I}(l^k \neq \tilde{l}^k).$$

For fixed $m > 0$, (Π, d^m) denotes the pseudo-metric topology on the m-step trajectories of Π.

2.3.2 The metric space (Π, d^∞)

We give two ways to obtain a metric topology on Π. First, let $a \wedge b = \min\{a, b\}$, and $\hat{d}^m = 1 \wedge d^m$. Then we define the metric

$$\hat{d}^\infty = \sum_{m=1}^{\infty} \frac{\hat{d}_s^m}{2^m}.$$

An alternative approach to define a metric topology is to utilize the Skorohod metric for functions in $\mathcal{D}(\mathbb{R}_+, \mathbb{R}^n)$ (see [39]). This approach has the advantage that properties of this metric are readily available, though its definition is more complicated. Let Λ be the collection of strictly increasing, Lipschitz continuous functions $\kappa : \mathbb{R}_+ \to \mathbb{R}_+$ with $\kappa(0) = 0$ and $\lim_{t\to\infty} \kappa(t) = \infty$ such that

$$\gamma(\kappa) := \sup_{s>t\geq 0} \left| \log \frac{\kappa(s) - \kappa(t)}{s - t} \right| < \infty. \tag{2.3.1}$$

This function estimates how much $\kappa(t)$ increases relative to t. Notice that when $\gamma(\kappa)$ is large, then the maximum or minimum rate of change of κ is different from one. Also, when $\gamma(\kappa) = 0$, then $\kappa = t$. For $f, g \in \mathcal{D}(\mathbb{R}_+, \mathbb{R}^n)$, $\kappa \in \Lambda$ and $u \in \mathbb{R}_+$ define

$$\hat{d}_s(f, g, \kappa, u) := \sup_{t\geq 0} \min\{1, |f(t \wedge u) - g(\kappa(t) \wedge u)|\}. \tag{2.3.2}$$

The *Skorohod metric* $d_s^\infty(\cdot, \cdot)$ is defined by

$$d_s^\infty(f, g) = \inf_{\kappa\in\Lambda} \left[\max\{\gamma(\kappa), \int_0^\infty e^{-u} \hat{d}_s(f, g, \kappa, u)\, du\} \right]. \tag{2.3.3}$$

Let $\pi, \tilde{\pi} \in \Pi$ be as in Section 2.3.1. We define the hybrid metric d^∞ by

$$d^\infty(\pi, \tilde{\pi}) = d_s^\infty(x, \tilde{x}) + \sum_{k=0}^{\infty} \frac{1}{2^k} \mathbb{I}(l^k \neq l'^k). \tag{2.3.4}$$

It is well known ([39], Theorem 5.6, pg. 121) that $(\mathcal{D}(\mathbb{R}_+, \mathbb{R}^n), d_s^\infty)$ is a complete metric space. The main result of this section is that the metric space (Π, d^∞) is also a complete metric space. In other words, if we have a Cauchy sequence of non-Zeno trajectories accepted by H, then the limit of the sequence is also accepted by H and is non-Zeno. The next theorem gives conditions under which this is true.

Theorem 2.3.1. *Suppose that H satisfies Assumption 2.2.1, that r_e has closed values and is upper semicontinuous, for all $e \in E$, and that at each location l, F_l has nonempty, compact, convex values and is upper semicontinuous. Then the space (Π, d^∞) is a complete metric space.*

Proof. Consider a Cauchy sequence $\pi_j = \{l_j^k, x_j^k(t)\}_{k=0}^{\infty}$ in (Π, d^∞), where $x_j = \{x_j^k(\cdot)\}_{k=0}^{\infty}$ and $x_j^k : (t_j^k, t_j^{k+1}] \to \mathbb{R}^n$ is a solution of the inclusion $\dot{x}_j^k \in F_{l_j^k}(x_j^k)$. By (2.3.4), $\{x_j\}$ is Cauchy in $\big(\mathcal{D}(\mathbb{R}_+, \mathbb{R}^n), d_s^\infty\big)$ and thus converges to some $x \in \mathcal{D}(\mathbb{R}_+, \mathbb{R}^n)$. We must show that x is the continuous part of a trajectory $\pi \in \Pi$ and $d^\infty(\pi_j, \pi) \to 0$, as $j \to \infty$. By Proposition 5.2 in ([39], pg. 118), $\lim_{j\to\infty} d_s^\infty(x_j, x) = 0$ if and only if there exists $\{\kappa_j\} \subset \Lambda$ such that $\lim_{j\to\infty} \gamma(\kappa_j) = 0$ and

$$\lim_{j\to\infty} \sup_{0\le t\le T} \big|x_j(t) - x(\kappa_j(t))\big| = 0\,, \qquad \text{for all } T > 0. \tag{2.3.5}$$

Note also that $\lim_{j\to\infty} \gamma(\kappa_j) = 0$ implies that

$$\lim_{j\to\infty} \sup_{0\le t\le T} \big|\kappa_j(t) - t\big| = 0\,, \qquad \text{for all } T > 0. \tag{2.3.6}$$

Since the inclusion F_l has compact values and is upper semicontinuous it follows that all the solutions that lie in a bounded domain are equicontinuous, using Lemma A.3.2. Using this fact along with (2.3.5)–(2.3.6) and (2.2.1) one can show that $x(t)$ has at most a finite number of discontinuities in each bounded time interval. Moreover, if $\{t^k\}_{k=1}^{\infty}$ are the discontinuity points of x then $t_j^k \to t^k$ as $j \to \infty$. Since $\{\pi_j\}$ is Cauchy it follows from the definition of d^∞ that l_j^k converges to a constant l^k, as $j \to \infty$ for all k. Set $e^k = (l^k, \sigma^k, l^{k+1})$. Let x^k denote the restriction of x on $(t^k, t^{k+1}]$. The equicontinuity of $x_j(t)$ on bounded domains along with (2.3.5)–(2.3.6) implies that $x_j^k(t) \to x^k(t)$ uniformly on compact subsets of (t^k, t^{k+1}), as $j \to \infty$. Hence, by Lemma A.3.1 x^k is a solution of the inclusion $\dot{x}^k \in F_{l^k}(x^k)$ on (t^k, t^{k+1}). By left-continuity we have $x_j^k(t^{k+1}) \to x^k(t^{k+1})$ which implies, since g_{e^k} is closed, that $x^k(t^{k+1}) \in g_{e^k}$. The existence of right limits along with equicontinuity yields $x_j^k(t^k+) \to x^k(t^k+)$, and since the graph of r_{e^k} is closed, it follows that $x^k(t^k+) \in r_{e^k}\big(x^{k-1}(t^k)\big)$. Thus, π_j converges to $\pi := \{l^k, x^k(\cdot)\}_{k=0}^{\infty}$ in $\big(\Pi, d^\infty\big)$. □

2.4 Continuity w.r.t. initial conditions

Regularity, or equivalently, continuity with respect to initial conditions for hybrid systems with Lipschitz differential inclusions is established under a *transversality* condition, stated in Definition 2.4.1. Let π_0 be a trajectory starting from p_0. We show that if π_0 satisfies the transversality condition, and under mild assumptions on the automaton stated in Assumption 2.4.1, there exists a continuous selection of trajectories from (Π, d^m) on a neighborhood of p_0.

Consider the problem

$$\dot{x} \in F(x), \qquad x(0) = \xi\,, \tag{2.4.1}$$

on a time interval $[0,T]$, where ξ ranges over a compact $X_0 \subset \mathbb{R}^n$ with diameter D. In addition, we assume the following.

Assumption 2.4.1. The set-valued map F satisfies:

(a) The values of F are closed, nonempty subsets of $\mathbb{R}^n$.

(b) There exists $K > 0$ such that $d_H(F(x), F(x')) \leq K|x - x'|$, for all $x, x' \in \mathbb{R}^n$.

Under Assumption 2.4.1, an absolutely continuous solution to (2.4.1) exists for each $\xi \in X_0$ [41]. Let $\xi_0 \in X_0$ and $x(\cdot)$ be a solution of (2.4.1) such that $x(0) = \xi_0$. It is shown in [30] that there exists a selection $\varphi_t(\xi)$ from the set of solutions of (2.4.1) which is continuous in $\xi \in X_0$ and such that $\varphi_t(\xi_0) = x(t)$. A condensed version of the result is provided as background in the Appendix. The selection is found by constructing a sequence of approximate trajectories, $\{y_t^j(\xi)\}_{j=0}^{\infty}$ which are shown to form a Cauchy sequence in the normed space $C_{ac}([0,T])$. In particular, this sequence can be chosen to satisfy

$$\|y^j(\xi) - y^{j-1}(\xi)\|_{ac} \leq D\Big(\frac{(KT)^j}{j!} + \frac{e^{2KT}}{2^{j+1}}\Big)$$

using Theorem A.4.3, part (i). Thus,

$$\|\varphi(\xi) - y^0(\xi)\|_{ac} \leq D\big(e^{KT} + e^{2KT}\big)\,, \tag{2.4.2}$$

where

$$y_t^0(\xi) = \xi + \int_0^t \dot{x}_s(\xi_0)ds \tag{2.4.3}$$

is the initial guess of the approximate trajectories. Hence, we obtain the estimate

$$\|\varphi(\xi) - \varphi(\xi_0)\|_{ac} \leq D\big(e^{KT} + e^{2KT} + 1\big) \leq 3De^{2KT}\,. \tag{2.4.4}$$

Assumption 2.4.2. The automaton H satisfies the following:

(a) The inclusion $\dot{x} \in F_l(x)$ at each location l satisfies Assumption 2.4.1.

(b) For each $e \in E$, g_e is either a compact, n-dimensional smooth manifold with boundary, or an embedded $(n-1)$-dimensional submanifold.

(c) r_e is a lower semicontinuous reset map from $\mathbb{R}^n$ to the closed, convex subsets of $\mathbb{R}^n$.

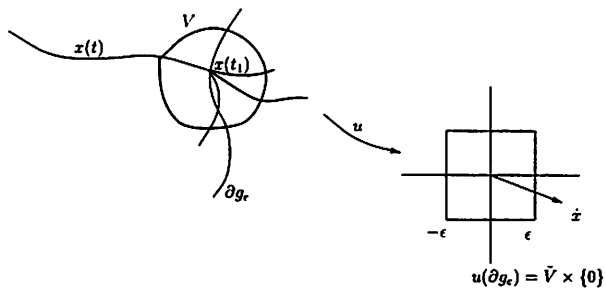

Figure 2.2: Transversal trajectory of a hybrid system with differential inclusions

Remark 2.4.1. Assumption 2.4.2 (c) makes possible the use of Michael's Selection Theorem A.2.3.

The following definition is essential for our main result. See Figure 2.2.

Definition 2.4.1. Let $e = (l, \sigma, l')$ and $x(t)$, $t \in [t_0, t_1]$, be a solution of $\dot{x} \in F_l(x)$ such that $x(t_1) \in \partial g_e$. We say that $x(t)$ is *transversal* to g_e at $x(t_1)$ if, for some $\epsilon > 0$,

(i) there exist a neighborhood V of $x(t_1)$, and local coordinates $u = (u_1, \ldots, u_n)$ centered at $x(t_1)$ mapping V onto $\tilde{V} \times (-\epsilon, \epsilon) \subset \mathbb{R}^{n-1} \times \mathbb{R}^n$ such that $u^{-1}(\tilde{V} \times \{0\}) \subset \partial g_e$ if g_e is an n-dimensional manifold or $u^{-1}(\tilde{V} \times \{0\}) \subset g_e$ if g_e is an $n-1$-dimensional submanifold. In addition, if g_e is n-dimensional, then $u_n(y) > 0, \forall y \in V \cap \text{int}(g_e)$.

(ii) there exists an extension of $x(t)$ on the interval $[t_0, t_1 + \epsilon]$ such that

$$\dot{x}(t) \cdot \nabla u_n(x(t)) \geq 1, \qquad \text{a.e. on } \{t : x(t) \in V\}.$$

We say that $x(t)$ is *strongly transversal* to g_e at $x(t_1)$ if, for some $\epsilon > 0$, condition (i) above is satisfied and

(ii) for all extensions of $x(t)$ on the interval $[t_0, t_1 + \epsilon]$, $x(t)$ satisfies

$$\dot{x}(t) \cdot \nabla u_n(x(t)) \geq 1, \qquad \text{a.e. on } \{t : x(t) \in V\}.$$

We say that a trajectory $\pi = \{l^k, x^k(t)\}_{k=0}^{\infty}$, whose steps are denoted as in (2.2.2), is a *(strongly) transversal trajectory* if for each k such that $x^k(t^{k+1}) \in \partial g_{e^k}$, $x^k(t)$ is (strongly) transversal to g_{e^k} at $x^k(t^{k+1})$.

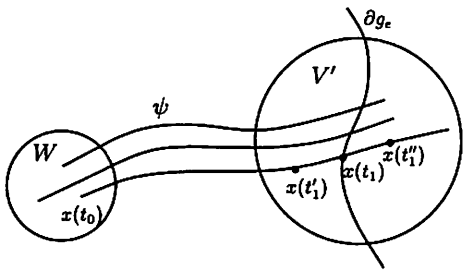

Figure 2.3: Continuous selections of transversal trajectories for Lipschitz inclusions

We make use of the following technical lemma. See Figure 2.3.

Lemma 2.4.1. *Let $\dot{x} \in F_l(x)$ be a Lipschitz inclusion satisfying Assumption 2.4.1, and let $x(t), t \in [t_0, t_1]$, be a solution that is transversal to g_e, $e = (l, \sigma, l')$ at $x(t_1)$. Then there exist $t_1'' > t_1$, a neighborhood W of $x(t_0)$, and a continuous selection $\varphi : W \to C_{ac}\big([t_0, t_1'']\big)$ of solutions of $\dot{\varphi} \in F_l(\varphi)$ satisfying:*

(a) $\varphi_t(x(t_0)) = x(t)$.

(b) there exists $t_1' \in (t_0, t_1)$ *such that, with* u *denoting the coordinates in Definition 2.4.1,*

$$\dot{\varphi}_t(\xi) \cdot \nabla u_n(\varphi_t(\xi)) \geq \frac{1}{2}, \qquad \text{a.e. on } [t_1', t_1''], \quad \forall \xi \in W.$$

(c) there exists a continuous $\tau : W \to [t_1', t_1'']$, *satisfying* $\tau\big(x(t_0)\big) = t_1$, *such that* $\varphi_{\tau(\xi)}(\xi) \in \partial g_e$, $\forall \xi \in W$.

Proof. By the transversality assumption there exists an open neighborhood V of $x(t_1)$ and coordinates $u : V \to \tilde{V} \times (-\epsilon, \epsilon) \subset \mathbb{R}^{n-1} \times \mathbb{R}$ such that x can be extended to $[0, t_1 + \epsilon]$ and $\dot{x}(t) \cdot \nabla u_n(x(t)) \geq 1$, a.e. on $\big\{t : x(t) \in V\big\}$. Since ∇u_n is continuous, we can select an open set $V' \subset V$, containing $x(t_1)$, and such that

$$\dot{x}(t) \cdot \nabla u_n(v) \geq \frac{3}{4}, \qquad \text{a.e. on } \big\{t : x(t) \in V'\big\}, \quad \forall v \in V'. \tag{2.4.5}$$

Select times $t_1' < t_1 < t_1''$ and $\delta' > 0$ such that $x(t) \in V'$, $\forall t \in [t_1', t_1'']$ and

$$B(x(t), \delta') \subset V', \qquad \forall t \in [t_1', t_1'']. \tag{2.4.6}$$

We use the construction in [30] also reviewed in Section A.4. Let $\{y_t^j(\xi)\}_{j=0}^{\infty}$ denote the sequence of approximate solutions in $C_{ac}([t_0, t_1'])$, with ξ in some neighborhood of $x(t_0)$, converging to $\varphi_t(\xi)$ uniformly in $C_{ac}([t_0, t_1'])$. Choose $D > 0$ to satisfy

$$|\varphi_t(\xi) - x(t)| \leq 3De^{2K(t_1'-t_0)} \leq \delta', \tag{2.4.7a}$$

$$2DKe^{2K(t_1'-t_0)} \cdot \sup_{v \in V'} |\nabla u_n(v)| \leq \frac{1}{4}. \tag{2.4.7b}$$

Let $\xi_0 := x(t_0)$. We claim that, for all $\xi \in B(\xi_0, \frac{D}{2})$

$$\dot{\varphi}_t(\xi) \cdot \nabla u_n(\varphi_t(\xi)) \geq \frac{1}{2}, \qquad \text{a.e. on } [t_1', t_1'']. \tag{2.4.8}$$

Indeed, combining (2.4.5), (2.4.7b) and (A.4.6) of Corollary A.4.4 and using the fact that $\dot{y}_t^0(\xi_i^0) = \dot{x}(t)$,

$$\begin{aligned} \dot{y}_t^j(\xi) \cdot \nabla u_n(y_t^j(\xi)) &\geq \dot{x}(t) \cdot \nabla u_n(y_t^j(\xi)) - |\nabla u_n(y_t^j(\xi))| \cdot |\dot{y}_t^j(\xi) - \dot{y}_t^0(\xi_i^0)| \\ &\geq \frac{3}{4} - \frac{1}{4} = \frac{1}{2}, \qquad \text{a.e. on } I_i(\xi), \quad \forall \xi \in B(\xi_0, \tfrac{D}{2}), \end{aligned}$$

thus establishing (2.4.8), by passing to the limit as $j \to \infty$. Parts (a) and (b) of the Lemma follow if we select $W = B(\xi_0, \frac{D}{2})$.

Finally, by (2.4.8), for each $\xi \in W$, there exists a unique $\tau(\xi) \in (t_1', t_1'')$ satisfying $\varphi_{\tau(\xi)}(\xi) \in \partial g_e$, or equivalently, $u_n(\varphi_{\tau(\xi)}(\xi)) = 0$. To prove continuity of $\tau(\cdot)$, we argue by contradiction. Suppose $\{\xi_k\} \subset W$ is a sequence converging to $\xi^* \in W$, as $k \to \infty$, but $\tau(\xi_k) \not\to \tau(\xi^*)$. Then along some subsequence also denoted by $\{\xi_k\}$, $\tau(\xi_k) \to \tau^*$ for some $\tau^* \neq \tau(\xi^*)$. It follows that $\varphi_{\tau(\xi_k)}(\xi_k) \to \varphi_{\tau^*}(\xi^*)$, and hence, $u_n\big(\varphi_{\tau(\xi_k)}(\xi_k)\big) \to u_n\big(\varphi_{\tau^*}(\xi^*)\big)$. But $u_n\big(\varphi_{\tau(\xi_k)}(\xi_k)\big) = 0$ implying $u_n\big(\varphi_{\tau^*}(\xi^*)\big) = 0$ which contradicts the uniqueness of $\tau(\xi^*)$. This proves part (c). □

Theorem 2.4.2. *Suppose H satisfies Assumption 2.4.2 and let π_0 be a transversal trajectory of H with initial state $p_0 = (l^0, \xi^0)$. For each $m > 0$, there exists a neighborhood (l^0, U) of p_0, with $U \subset \mathbb{R}^n$ open, and $\Psi(t, \xi)$, a selection of trajectories of H, such that $\Psi(t, \xi^0) = \pi_0(t)$ and $\xi \mapsto \Psi(\cdot, \xi)$ is continuous in (Π, d^m).*

Proof. Suppose that π_0 has an m step run $l^0, \ldots, l^{m-1}$, each step represented by (2.2.2), and visits the enabling conditions $g^0, \ldots, g^{m-1}$, with $r^0, \ldots, r^{m-1}$ denoting the corresponding reset maps. Observe that in order for a selection to be continuous in (Π, d^m), its trajectories must have identical runs $l^0, \ldots, l^{m-1}$.

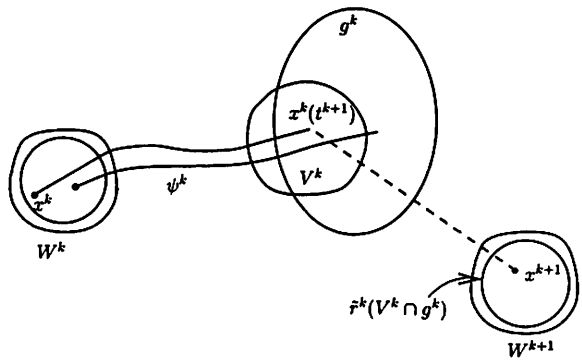

Figure 2.4: Theorem 2.4.2: Continuity with respect to initial conditions

First consider the reset of the kth step. Since r^k is locally selectionable, by Michael's Selection Theorem A.2.3, there exists a continuous selection $\tilde{r}^k$ of r^k, satisfying

$$\tilde{r}^k\big(x^k(t^{k+1})\big) = x^{k+1}. \tag{2.4.9a}$$

Therefore, given an open neighborhood W^{k+1} of x^{k+1}, there exists an open subset V^k containing $x^k(t^{k+1})$ such that

$$\tilde{r}^k\big(V^k \cap g^k\big) \subset W^{k+1}. \tag{2.4.9b}$$

If $x^k(t^{k+1}) \in \partial g^k$, then by Lemma 2.4.1, for each open set V^k containing $x^k(t^{k+1})$, there exists an open neighborhood W^k of $x^k(t^k+)$, a time $\hat{t}^{k+1} > t^{k+1}$, a continuous selection $\psi^k : W^k \to C_{ac}\big([0, \hat{t}^{k+1} - t^k]\big)$ of solutions of $\dot{\psi}^k = F_{l^k}(\psi^k)$, and a continuous map $\tau^k : W^k \to [0, \hat{t}^{k+1} - t^k]$ such that

$$\psi^k_t\big(x^k(t^k+)\big) = x^k(t + t^k), \qquad t \in (0, t^{k+1} - t^k], \tag{2.4.10a}$$

$$\tau^k\big(x^k(t^k+)\big) = t^{k+1} - t^k, \tag{2.4.10b}$$

$$\psi^k_{\tau^k(w)}(w) \in V^k \cap g^k, \qquad \forall w \in W^k. \tag{2.4.10c}$$

On the other hand, if $x^k(t^{k+1}) \in \mathrm{int}(g^k)$, then selecting an open neighborhood $V^k \subset g^k$ of $x^k(t^{k+1})$, and defining $\tau^k := t^{k+1} - t^k$, by the results in [30], there is a continuous selection ψ^k defined on some open set $W^k \ni x^k(t^k+)$ such that (2.4.10) holds.

A finite iteration of the arguments in the last two paragraphs yields collections of open sets $\{W^0, \ldots, W^{m-1}\}$ and $\{V^0, \ldots, V^{m-1}\}$ along with continuous selections $\{\psi^k\}_{k=0}^{m-1}$ and

continuous maps $\{\tilde{\tau}^k\}_{k=0}^{m-1}$ and $\{\tau^k\}_{k=0}^{m-1}$, as defined above, such that (2.4.9) and (2.4.10) hold.

Define $\tilde{\psi}^k : W^k \to V^k \cap g^k$ by $\tilde{\psi}^k(w) := \psi^k_{\tau^k(w)}(w)$. From the continuity of $w \mapsto \psi^k_t(w)$ and $w \mapsto \tau^k(w)$, the absolute continuity of $t \mapsto \psi^k_t(w)$, and the triangle inequality

$$|\tilde{\psi}^k(w) - \tilde{\psi}^k(w')| \le |\psi^k_{\tau^k(w)}(w) - \psi^k_{\tau^k(w')}(w)| + |\psi^k_{\tau^k(w')}(w) - \psi^k_{\tau^k(w')}(w')|\,, \tag{2.4.11}$$

we obtain that $\tilde{\psi}^k$ is continuous on W^k. Let $U = W^0$ and define for $\xi \in U$

$$\beta^k(\xi) = \tilde{\tau}^{k-1} \circ \tilde{\psi}^{k-1} \circ \cdots \circ \tilde{\tau}^0 \circ \tilde{\psi}^0(\xi)\,, \quad k = 1, \ldots, m\,; \qquad \beta^0(\xi) = \xi \tag{2.4.12}$$

$$t^k(\xi) = \sum_{\ell=0}^{k-1} \tau^\ell \circ \beta^\ell(\xi)\,, \qquad I^0(\xi) = \left[0, t^1(\xi)\right], \quad I^k(\xi) = (t^k(\xi), t^{k+1}(\xi)] \tag{2.4.13}$$

$$\Psi(t,\xi) = \left\{ \left(l^k, \psi^k_{t-t^k(\xi)} \circ \beta^k(\xi)\right), \ \ t \in I^k(\xi) \right\}_{k=0}^{m-1}. \tag{2.4.14}$$

It follows that $t^k(\cdot)$ and $\Psi(t,\cdot)$, for fixed t, are continuous on U. To show continuity of $\Psi(\cdot,\cdot)$ in (Π, d^m), let $\xi, \xi' \in U$ and define

$$\kappa(t) = \left(t - t^k(\xi)\right) \frac{t^{k+1}(\xi') - t^k(\xi')}{t^{k+1}(\xi) - t^k(\xi)} + t^k(\xi')\,, \qquad t \in I^k(\xi)\,. \tag{2.4.15}$$

It follows that $|t - \kappa(t)| \xrightarrow[\xi' \to \xi]{} 0$, uniformly on $[0, t^m(\xi)]$ and using a triangle inequality as in (2.4.11) we can easily show the same holds for $\left|\Psi(t,\xi) - \Psi(\kappa(t), \xi')\right|$. Therefore,

$$d^m\big(\Psi(t,\xi), \Psi(t,\xi')\big) \xrightarrow[\xi' \to \xi]{} 0\,,$$

and the proof is complete. □

Remark 2.4.2. A direct consequence of Theorem 2.4.2 is that a continuous selection exists, under the same assumptions, if π_0 is a *strongly* transversal trajectory of H.

Chapter 3

Model Checking

One has only learnt to get the better of words
For the thing one no longer has to say, or the way in which
One is no longer disposed to say it.
- T.S. Eliot.

3.1 Introduction

The goal of this chapter is to extend methods of obtaining bisimulations to hybrid systems with the application of model checking in mind. The approach is to generalize the work of Alur and Dill on timed automata [4] to hybrid systems with non-trivial continuous dynamics. We obtain results on bisimulations of hybrid automata by examining the geometric structure of the bisimulation of timed automata. This gives a new method to construct bisimulations, under a suitable compatibility condition and in the process we obtain new decidability results for the examples of the following chapter: coordinated aircraft, coordinated robots, engine control, and hybrid systems with linear dynamics.

3.1.1 Motivation

Verification was introduced for finite state programs to determine automatically if the states of the program satisfy a specification. A *safety* requirement ensures that a system does not exhibit some undesired behavior. The complement is a *liveness* requirement: that the system exhibit some desired behavior. Pnueli proposed the use of temporal logic for the specification of safety and liveness requirements [76]. The algorithmic verification of finite-state systems was started in 1981 by Clarke and Emerson [32] and by Sifakis [81]. The

procedure is to convert the finite state program to a finite graph M. Given a temporal formula ϕ, the verification question is: do all sequences defined by paths through M satisfy ϕ? The problem is termed *model checking* because we want to know if M is a model of ϕ. Vardi and Wolper [100] showed that one can construct a Buchi automaton that accepts sequences satisfied by formulas of PLTL (Propositional linear-time logic). If the program is viewed as a finite state generator P and the specification ϕ as a finite state acceptor, then the model checking problem is reduced to the automata-theoretic question of whether the language $L(P) - L(\phi)$ is empty, where $L(P)$ is the language generated by P and $L(\phi)$ is the language accepted by ϕ. For hybrid systems, model checking is performed by *abstracting* the system to obtain a finite quotient system. Bisimulation is the main step in constructing the quotient system. Intuitively, bisimulation is an equivalence relation on the hybrid state space that yields a partition "consistent" with the behavior of the automaton. This consistency enables one to make correct inferences about hybrid trajectories using only sequences of equivalence classes.

The need for new results on bisimulation is evident in three areas. First, modeling checking has been announced as a method that can supplant simulation in the design of concurrent systems [33]. In order to make this claim realizable for hybrid systems, model checking must be able to handle non-trivial dynamics. At present, it is incapable of doing so. Our positive results give encouragement to press ahead with a program of model checking for hybrid systems. Second, although state space partitions have been an underlying assumption in several separate research efforts such as [92] and [26], no method to obtain partitions was given. We show that a comprehensive methodology may be within reach. Finally, model checking and the related problem of controller synthesis are able to address problems that control theory has been unable to address because of a lack of expressiveness of control theoretic models. In particular, temporal logic enables a rich characterization of transient behavior in time, when the system operates in a *reactive* mode with its environment, in contrast with control theoretic specifications, such as stability and controllability, which have mostly focused on input-output behavior. Temporal specifications also express communication and coordination requirements of multiple agents. (Temporal specifications can encode requirements such as two agents cannot reach a deadlock in communications).

Inspite of this, few results on obtaining bisimulations or constructing partitions are available. We summarize those works we are aware of. The approach of [60] requires an iterative

scheme to compute the bisimulation and is built up from the theory of ominimal structures, which are boolean algebras of subsets of $\mathbb{R}^n$ with additional nice closure properties. An example is semi-algebraic sets. While this work is theoretically appealing, we feel there is a simpler way to go about things, using easier concepts and more computationally attractive methods. We obtain an analytical description of bisimulation that can be understood as a gestalt, which has the intuitive appeal that it is an immediate extension of the approach for timed automata. It relies on concepts that are accessible to computer scientists and familiar in geometric control theory [55], namely local coordinate transformations. The analytical description enables us to define the *symbolic execution theory* for the hybrid automaton. The method of [53] uses an over-approximation of vector fields by differential inclusions. At present obtaining the inclusions and the region over which it is valid is ad-hoc. We take the contrasting view that the vector fields capture important information about the model, which the designer has taken some trouble to identify, but the enabling and reset conditions are often design parameters that may be specified to the computational benefit of model checking. (Enabling and reset conditions are a priori given in models with inherent hybrid behavior, such as mechanics problem with contact).

3.2 Bisimulation

The concept of bisimulation was introduced by D. Park [74] in the context of concurrent processes modeled by finite transition systems. Let λ represent an arbitrary interval of time. Given the hybrid system H, a *bisimulation* of H is a binary relation $\simeq \ \subset (L\times M)\times(L\times M)$ satisfying the condition that for all states $p, q \in L \times M$, if $p \simeq q$ and $\sigma \in \Sigma \cup \{\lambda\}$, then
(1) if $p \xrightarrow{\sigma} p'$, then there exists q' such that $q \xrightarrow{\sigma} q'$ and $p' \simeq q'$, and
(2) if $q \xrightarrow{\sigma} q'$, then there exists p' such that $p \xrightarrow{\sigma} p'$ and $p' \simeq q'$.

There are a number of interpretations of bisimulation we which describe below. One should reason with the one that feels the best [1].

Geometric The view explored in this thesis; we develop it in this chapter.

Topological Stemming from fundamental work by McKinsey and Tarski [93], bisimulation was interpreted as a form of topological continuity by Jennifer Davoren [37].

[1] and is best suited to the problem at hand

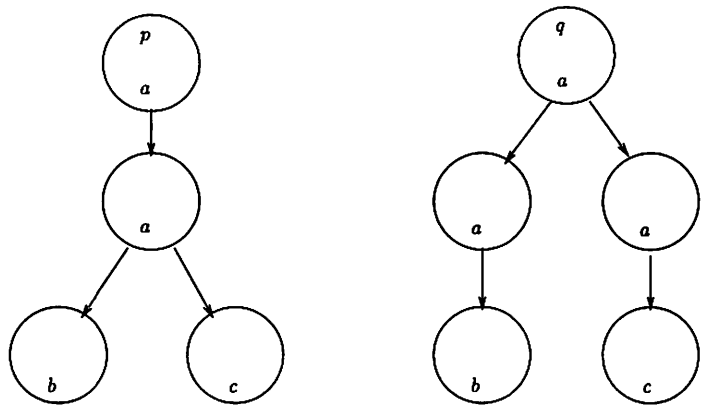

Figure 3.1: States p and q are not bisimilar.

Algebraic In an algebraic sense, bisimulation is a *congruence*; that is, an equivalence relation closed under concatenation, where by concatenation we mean successive σ- or t-steps of H.

Game-theoretic Bisimulation can be interpreted as a game between an automaton and its environment. In this view, the protagonist and the environment start at two states and take σ- or t- steps, each time recording an *observation*. The environment uses non-determinism advantageously to select a step the protagonist cannot match. If the protagonist matches the observations of the environment, the states are bisimilar. This view has special interest when non-determinism dominates the behavior of the automaton, whereas in the deterministic case it seems rather obvious. [2] For instance, borrowing an example from [5], the states p and q in Figure 3.1 with observations labeled $\{a, b, c\}$ are not bisimilar.

Constructive A constructive view and also a definition is that bisimulation is the *coarsest stable refinement* of an *observation equivalence* [69]. One uses a Paige-Tarjan type refinement algorithm [73] such that the fixed point of the algorithm gives the bisimulation partition. For instance, a refinement algorithm starting from the final set

[2] While non-determinism non-trivializes the concept of bisimulation for finite automata, non-determinism in the continuous dynamics of hybrid automata can ruin hopes of finding finite bisimulations, even in the simplest cases like rectangular automata [50].

$Q^f \subset L \times M$ is:

$Q := \{Q^f, L \times M - Q^f\}$

while $\exists Z, Z' \in Q$ and $\tau \in \Sigma \cup \mathbb{R}^+ \; . \; \emptyset \subset Z \cap Pre_\tau(Z') \subset Z$

do

$Q := (Q - \{Z\}) \cup \{Z \cap Pre_\tau(Z'), Z - Pre_\tau(Z')\}$

od

Pre is a predecessor operator defined in (3.4.4). This procedure terminates if $\simeq$ is finite. See [48], [60].

Inductive An inductive view (again, this can be taken as the definition) is that bisimulation is obtained inductively using an order of observation equivalences. Suppose we have an observation equivalence, $\simeq_0$, defined by: $p \simeq_0 q$ iff $O(p) = O(q)$, where O is an observation map from $L \times M$ to an observation set. We can define an equivalence $\simeq_k$ inductively. We say $p \simeq_k q$ iff

(1) $O(p) = O(q)$,

(2) if $p \to p'$, then $\exists$ state q' such that $q \to q'$ and $p' \simeq_{k-1} q'$,

(3) if $q \to q'$, then $\exists$ state p' such that $p \to p'$ and $q' \simeq_{k-1} p'$.

Bisimulation is the fixed point of this process.

Lemma 3.2.1. $\simeq = \bigcap_{k=0}^{\infty} \simeq_k$.

Let Q be the set of equivalence classes of $\simeq$. A bisimulation is finite if it has a finite number of equivalence classes. Using $\simeq$, a quotient system $H_\simeq$ can be constructed. If $\simeq$ is finite, the quotient system is the finite automaton

$$H_\simeq = (Q, \Sigma \cup \lambda, E_\simeq).$$

$Q = L \times M/_\simeq$ are the cosets of $\simeq$. $q \in Q$ can be written as $q = [(l, x)]$ for some $l \in L$, $x \in M_l$ such that $(l, x) \in q$. The transitions of $H_\simeq$, defined by $E_\simeq$ and denoted $\to_\simeq$, are as follows. For $q = [(l, x)], q' = [(l', x')]$, $q \to_\simeq q'$ iff there exists $(l, y) \in q$ and $(l', y') \in q'$ such that $(l, y) \to (l', y')$ is either a t-step or a σ-step of H (for t-steps, q and q' are contiguous). $H_\simeq$ is referred to as an *abstraction* of H.

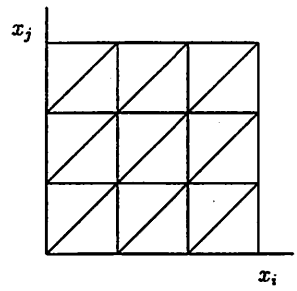

Figure 3.2: Bisimulation for timed automata.

Remark 3.2.1.

1. The importance of $H_{\simeq}$ is that it captures the salient features of the dynamics of H in a time abstract model. The abstraction of time enables the reduction from an infinite state space to a finite one. If the bisimulation is not finite the reduction can still be done to an infinite automaton, and model checking algorithms can be applied, but they may not terminate.

2. If initial conditions Q^0 or final conditions Q^f are specified with H, then these sets are quotiented by $\simeq$ as well.

Example 3.2.1. It is illuminating to examine the bisimulation of timed automata with a geometric lens.

For $y \in \mathbb{R}$, let $\lfloor y \rfloor$ be its integer part and $\langle y \rangle$ its fractional part. Let L be the set of locations, $x \in \mathbb{R}^n$ the clock variables, and m_i the largest integer the ith clock is compared to in an enabling condition. We say $(l, x) \simeq (l', x')$ iff (1) $l = l'$, (2) for all $i = 1, \ldots, n$, $x_i > m_i$ iff $x'_i > m_i$, or $\lfloor x_i \rfloor = \lfloor x'_i \rfloor$, (3) for every $x_i, \leq m_i$ and $x_j \leq m_j$, $\langle x_i \rangle \leq \langle x_j \rangle$ iff $\langle x'_i \rangle \leq \langle x'_j \rangle$ and $\langle x_i \rangle = 0$ iff $\langle x'_i \rangle = 0$.

Figure 3.2 shows the bisimulation for timed automata projected to the $x_i - x_j$ plane. We observe the following features:

1. The bisimulation is defined on a compact region of the state space where the interesting dynamics occur. Outside this region, the dynamics are sufficiently benign that they can be handled by one equivalence class.

2. The partition is described as a gestalt rather than as an iterative procedure that

terminates at a fixed point.

3. The partition uses hypersurfaces that are either invariants or transversals of the flow to build up equivalence classes.

4. The hypersurfaces are propitiously selected to be compatible with the syntax of the enabling, reset, initial and final conditions. That is, the syntax of timed automata does not imply a further refinement of the "proposed" partition.

5. The hypersurfaces are defined by analytical expressions. The atomic expressions provide an alternative description of the bisimulation [33, p.280], and can be used to define the *symbolic execution theory* [49].

3.2.1 Stable partitions and compatibility

In this section we develop the construction of bisimulations for hybrid automata using our geometric insights. First, we show how a concept of stable partitions with respect to a flow combined with a natural compatibility condition on the enabling and reset (and initial and final) conditions leads to a bisimulation. This step is rather straightforward. Assuming the compatibility conditions are met, there is only constructing stable partitions.

For each $l \in L$, let $\simeq^l$ be an equivalence relation on $\{l\} \times M_l$ and let P^l be the partition on $\{l\} \times M_l$ defined by $\simeq^l$. We say P^l is a *stable partition of the flow* ϕ^l or $\simeq^l$ defines a *stable partition of the flow* ϕ^l if $(l,x) \simeq^l (l,x')$ implies that for all $y \in M_l$, $t \geq 0$, if $y = \phi^l_t(x)$, then there exists $y' \in M_l$ and $t' \geq 0$ such that $y' = \phi^l_{t'}(x')$ and $(l,y) \simeq^l (l,y')$.

Let $e = (l, \sigma, l') \in E$ and $\mathcal{P} = \{P^l \mid l \in L\}$, a set of stable partitions defined by equivalence relations $\{\simeq^l\}_{l \in L}$. Given $\simeq^l$ at $l \in L$, we say g_e *is compatible with* $\simeq^l$ if $(l,x) \in \{l\} \times g_e$ implies $[(l,x)] \in \{l\} \times g_e$. That is, the enabling condition is a union of cosets of $\simeq^l$. Similarly we say Q^0 *is compatible with* $\simeq^l$ if $(l,x) \in Q^0$ implies $[(l,x)] \in Q^0$. The analogous definition applies to Q^f. For $e = (l, \sigma, l')$ we say that r_e *is compatible with* $\simeq^{l'}$ if $(l', x') \in \{l'\} \times r_e(x)$ implies $[(l', x')] \in \{l'\} \times r_e(x)$, and $[(l,x)] = [(l,x')]$ implies $r_e(x) = r_e(x')$. Finally, we say H *is compatible with* $\{\simeq^l\}$ if for each $e \in E$, g_e and r_e are compatible with $\simeq^l$, $\simeq^{l'}$, respectively, and for each $l \in L$, Ω^l is compatible with $\simeq^l$, and Q^0 and Q^f are compatible with $\{\simeq^l\}$.

Lemma 3.2.2. *Given hybrid automaton H and $\{\simeq^l\}$ defining a set of stable partitions with respect to the flows of H, suppose H is compatible with $\{\simeq^l\}$. Then $\simeq \subset Q \times Q$ defined by: $(l,x) \simeq (l',x')$ iff (1) $l = l'$, and (2) $(l,x) \simeq^l (l',x')$, is a bisimulation for H.*

Proof. Let $\simeq$ be an equivalence relation satisfying conditions (1) and (2) and suppose $(l,x) \simeq (l',x')$. This implies $l = l'$ and $(l,x) \simeq^l (l,x')$.

Suppose $(l,x) \xrightarrow{t} (l,y)$ is a t-step of H. Because $\simeq^l$ defines a stable partition, there exists $y' \in M_l$ and $t' \geq 0$ such that $y' = \phi^l_{t'}(x')$ and $(l,y) \simeq^l (l,y')$. Hence $(l,y) \simeq (l,y')$.

Suppose $(l,x) \xrightarrow{\sigma} (\tilde{l},y)$ is a σ-step of H. This implies $x \in g_e$ for $e = (l,\sigma,\tilde{l})$. Since g_e is compatible with $\simeq^l$, $x' \in g_e$. Since r_e is compatible with $\simeq^{l'}$ we can find $y' \in r_e(x')$ such that $[(\tilde{l},y)] = [(\tilde{l},y')]$, since $r_e(x) = r_e(x')$. Hence $(\tilde{l},y) \simeq (\tilde{l},y')$. □

Remark 3.2.2.

1. The definition of stable partition says two equivalent points *can* each take a time step to the same equivalence class, not that they will. Thus, it applies to differential inclusions as well as vector fields.

2. The compatibility condition on r_e is a sufficient condition. A necessary condition is that for $e = (l,\sigma,l')$, r_e is compatible with $\simeq^{l'}$ if for $(l,x) \in \{l\} \times g_e$ and $[(l,x)] = [(l,x')]$, if $y \in r_e(x)$ then there exists $y' \in r_e(x')$ such that $[(l',y)] = [(l',y')]$. This weaker condition is closer to what we observe in examples, but from the point of view of verification, it is no different than imposing the stronger condition that we stated. For example, in timed automata it is the sufficient condition for compatibility which holds when one of the clocks of the automaton is reset to an integer value while the other clocks take the identity reset. It has the same effect, in symbolic model checking, as resetting the other clocks non-deterministically to a range corresponding to the equivalence class that lies in the image of the reset.

3. The compatibility definitions are the natural ones to ensure that bisimulation is preserved over σ-steps. One could also take the view that the enabling and reset conditions are given in an arbitrary form. For safety controller synthesis starting from *bad* states, to obtain the bisimulation one over-approximates the enabling and reset conditions by compatible ones. For reachability analyses starting from *good* states, one under-approximates. The approximative view is described in [23].

3.2.2 Foliations and first integrals

We build stable partitions using foliations, flow boxes and first integrals. We assume knowledge of some differential geometry (see [101]).

Given an n-dimensional manifold M a smooth *foliation* of dimension p or codimension $q = n - p$ is a collection of disjoint connected subsets $F = \{S_\alpha\}$ whose disjoint union forms a partition of M. The foliation satisfies the property that each point of M has a neighborhood U and a system of coordinates $y : U \to \mathbb{R}^p \times \mathbb{R}^q$ such that for each S_α, the (connected) components of $(U \cap S_\alpha)$ are given by

$$\begin{aligned} y_{p+1} &= c_1 \\ &\vdots \\ y_{p+q} &= c_q \end{aligned}$$

where $c_i \in \mathbb{R}$. Each connected subset is called a *leaf* of the foliation, and each leaf is a submanifold of dimension p in M. See [61] for more background on foliations.

We want foliations whose leaves are regular submanifolds. The Pre-Image theorem [101, p. 31] provides a way to construct regular submanifolds, and, in particular, the pre-image of a submersion defines a foliation with regular leaves. A foliation globally defined by a submersion is called *simple*.

Let $X \in \mathcal{X}(M)$. We define two types of simple co-dimension one foliations with respect to X, called tangential and transversal foliations. For this we require a notion of transversality of foliations. Let TF be the field of tangent spaces to the leaves of F. A map $h : M \to N$ is *transverse* to a foliation F of N if for every $x \in M$, $h_* T_x M + T_{h(x)} F = T_{h(x)} N$, where h_* is the push-forward map of h. A submanifold W on M is *transverse* to foliation F of M if the inclusion map $i : W \to M$ is transverse to F. A foliation F' is said to be *transverse* to F if each leaf of F' is transverse to F. A foliation does not in general admit a transversal foliation, but for each $x \in M$ there exists a neighborhood of x such that F restricted to the neighborhood has a local transversal foliation. A *tangential foliation* F of M is a co-dimension one foliation that satisfies $X(x) \in T_x F, \forall x \in M$; that is, X is a cross-section of TF. A *transversal foliation* $F_\perp$ of M is a co-dimension one foliation that

satisfies $X(x) \notin T_xF, \forall x \in M$.

Let $\{F_i\}$ be a collection of $n-1$ tangential foliations on $U \subset M$ and one transversal foliation $F_n := F_\perp$ on U, which, additionally, satisfies a *regularity condition*: for each $x \in M$, $T_xF_1 + \cdots + T_xF_n = \mathbb{R}^n$. For simple foliations the following lemma provides an algebraic test for regularity.

Lemma 3.2.3. *Let M be an n-dimensional manifold and define $h_i : M \to \mathbb{R}, i = 1, ...n$, a collection of submersions on M. If dh_i are linearly independent on $U \subset M$, then the foliations defined by $h^{-1}(\mathbb{R})$ are independent on U.*

Proof. It suffices to consider two leaves $S_1 = h_i^{-1}(c_1)$ and $S_2 = h_j^{-1}(c_2)$ and $S_1 \cap S_2 \neq \emptyset$. Suppose $x \in S_1 \cap S_2$ and S_1 and S_2 are not transversal at x. Note that $(dh_1) : T_xS_1 \to T_{h(x)}\mathbb{R}$ satisfies $(dh_1)_x = 0, \forall x \in S_1$. Similarly, $(dh_2)_x = 0, \forall x \in S_2$. Define $(dh)_x = [(dh_1)_x \ (dh_2)_x]^T$. Since S_1 and S_2 are tangential at x, there exits vector v satisfying $v \in T_xS_1$ and $v \in T_xS_2$. Therefore $v \in \text{kernel}(dh)_x$, implying dimension of kernel$(dh)_x$ is $n-1$. But by assumption, rank $(dh)_x$ is 2, which provides the contradiction. □

We will not use all of the leaves of a foliation, but a finite subset of them. We *discretize* a foliation as follows. Let $h : M \to \mathbb{R}$ be the submersion of a simple co-dimension one foliation F. Given an interval $[a, b]$, a gridsize $\Delta = \frac{b-a}{2^k} > 0$ with $k \in \mathbb{Z}^+$, define the finite collection of points $C_k = \{a, a + \Delta, \ldots, b\}$. Then, $h^{-1}(C_k)$ is the discretization of F on $h^{-1}([a, b])$.

A bisimulation can be constructed using foliations by elaborating the following steps:

1. Find $(n-1)$ simple co-dimension one tangential foliations on $U \subset M$, for each $X^l, l \in L$.
2. Construct either a local or global (on U) transversal foliation for each X^l.
3. Check the regularity condition on U.
4. Discretize the foliations using a gridsize Δ.

To obtain tangential foliations we use local first integrals. A *first integral* of $\dot{x} = X(x)$ is a function $\Psi : M \to \mathbb{R}$ satisfying $L_X\Psi = 0$, where $L_X\Psi$ is the Lie derivative of Ψ along X.

Theorem 3.2.4 (Flow Box). *Let X be a vector field on M with $X(x) \neq 0$. Then there exist coordinates y defined on a neighborhood V of x such that*

$$X = \frac{\partial}{\partial y_n} \qquad \text{on } V.$$

Here is our main result on stable partitions.

Theorem 3.2.5. *Given $X \in \mathcal{X}(M)$, compact $U \subseteq M$, and coordinates y, if (y, U) is a flow box for X, there exists a stable partition with respect to X on U.*

Proof. By the Flow Box theorem, there exists a diffeomorphism $h : U \to V \subset \mathbb{R}^n$, where $V = [-1, 1]^n$, such that $\dot{x} = X(x)$ expressed in $y = h(x)$ coordinates is

$$\dot{y}_1 = 0, \dot{y}_2 = 0, ...\dot{y}_n = 1. \tag{3.2.1}$$

There exist $n-1$ independent functions $y_1 = c_1, \ldots, y_{n-1} = c_{n-1}$ that are first integrals of (3.2.1), and they define $(n-1)$ independent submanifolds, passing through each $y = (c_1, \ldots, c_{n-1}, y_n)$. A submanifold transversal to the flow of (3.2.1) is given by $y_n = c_n$.
Fix $k \in \mathbb{Z}^+$ and let $\Delta = \frac{1}{2^k}$. Define

$$C_k = \{0, \pm\Delta, \pm 2\Delta, \ldots, \pm 1\}. \tag{3.2.2}$$

Each $y_i = c$ for $c \in C_k$, $i = 1, \ldots, n$ defines a hyperplane in $\mathbb{R}^n$ denoted $\tilde{W}_{i,c}$, and a submanifold $W_{i,c} = h^{-1}(\tilde{W}_{i,c})$. The collection of submanifolds is denoted

$$\mathcal{W}_k = \{\ W_{i,c} \mid c \in C_k, i \in \{1, \ldots, n\}\ \}. \tag{3.2.3}$$

$U \setminus \mathcal{W}_k$ is the union of $2^{n(k+1)}$ disjoint open sets $\mathcal{V}_k = \{V_j\}$.

We define an equivalence relation $\simeq^e$ on $\mathbb{R}^n$ as follows. $x \simeq^e x'$ iff
(1) $x \notin V$ iff $x' \notin V$, and
(2) if $x, x' \in V$, then for each $i = 1, \ldots, n$, $x_i \in (c, c+\Delta)$ iff $x' \in (c, c+\Delta)$, and $x_i = c$ iff $x'_i = c$, for all $c \in C_k$.

We define the equivalence relation $\simeq$ on $\{l\} \times M$ by $x \simeq x'$ iff $h(x) \simeq^e h(x')$. $\simeq$ is clearly a stable partition with respect to X^l because the invariant submanifolds enclose trajectories starting at equivalent points so that they can only visit the same next equivalence class. □

Remark 3.2.3.

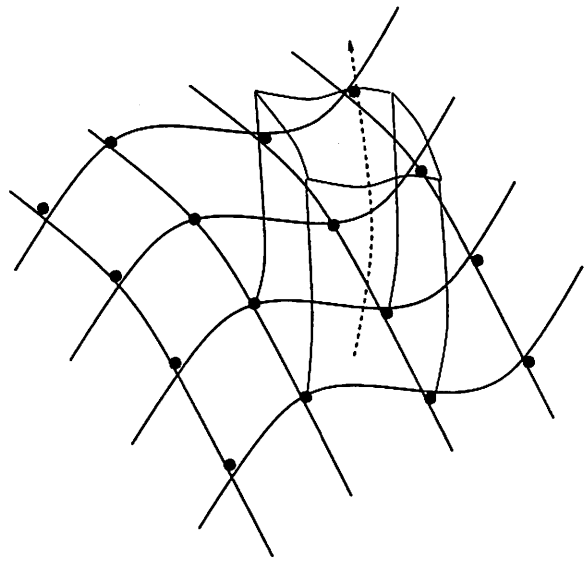

Figure 3.3: Partition for $\simeq$. The leaves of the tangential foliations form boundaries that are invariants of the flow.

1. One can show that the closure of an equivalence class of $\simeq$ is a union of equivalence classes of $\simeq$. This implies that the interior of an equivalence class is either the empty set or the class itself. The picture of $\simeq$ is something like Figure 3.3. The equivalence classes are the open line segments, points, interiors of cells, etc.

2. Suppose a stable partition has been constructed for a smooth vector field X on M using the steps outlined above. Let Y on N be a smooth vector field topologically conjugate to X; that is, there exists a homeomorphism h taking orbits of X through $x \in M$ to orbits of Y through $h(x) \in N$ and preserving the sense of the orbit. Then h can be used to construct a stable partition with respect to Y. First, if g is a first integral of X then $g \circ h^{-1}$ is a first integral of Y since $L_Y(g \circ h^{-1}) = d(g \circ h^{-1})(h_* X) = dg \cdot X = L_X g$. In this manner, tangential and transversal foliations are mapped through h to tangential and transversal foliations of Y, respectively. If the foliations of X are independent so are the foliations of Y. Also, since h maps fixed points of X to fixed points of Y, a stable partition defined on $U \subset M$ for X non-vanishing on U is well-defined for $h(U) \subset N$ and Y is non-vanishing on $h(U)$.

3.3 Exterior differential systems

A natural setting for finding first integrals is provided by exterior differential systems [88, 24]. Let $\Omega(M) = \oplus_{k=0}^{\infty}\Omega^k(M)$ with the wedge product $\wedge$ be the exterior algebra on M. $d : \Omega^k(M) \to \Omega^{k+1}(M)$ is the exterior derivative. Recall that $\omega \in \Omega^k(M)$ is *exact* if there exists an $\alpha \in \Omega^{k-1}(M)$ such that $\omega = d\alpha$. A set of independent one-forms $\omega^1, \ldots, \omega^n$ generates a *Pfaffian system* $P = \{\omega^1, \ldots, \omega^n\} = \{\sum f_k\omega^k | f_k \in C^\infty(M)\}$. The Pfaffian system satisfies the *Frobenius condition* if $d\omega^i$ is a linear combination of $\omega^1, \ldots, \omega^n$.

Theorem 3.3.1 (Frobenius). *Let $P = \{\omega^1, \ldots, \omega^n\}$ be a Pfaffian system with one-forms satisfying the Frobenius condition for $i = 1, \ldots, n$. Then there exist coordinates $h_1, \ldots, h_n$ such that $P = \{dh_1, \ldots, dh_n\}$.*

In this case the Pfaffian system is said to be *completely integrable* and the h_i are the first integrals of P. Thus, the Frobenius theorem provides an alternative and equivalent route to existence of local first integrals as the Flow Box theorem. We have found it useful in applications to work with systems in Pfaffian form. Also, it is easy to state results about parallel composition of hybrid automata in terms of the vector fields in Pfaffian form. We give such a result next, but we remark that this is a first step: interesting extensions are possible using the theory of exterior differential systems.

3.3.1 Parallel composition

Parallel composition is an important operation on hybrid automata as we are typically interested in checking properties of automata that operate concurrently, where each automaton models a concurrent process, reactive system, or autonomous agent. Bisimulation for hybrid systems is, in general, not closed under parallel composition of automata. We give a sufficient condition on the Pfaffian form of the continuous dynamics of each control location so that if two hybrid automata have a finite bisimulation, then so does their parallel composition.

Suppose we have hybrid automata $H_i = (L_i \times M_i, \Sigma_i, , E_i, X_i, G_i, R_i)$, $i = 1, 2$. We label the components of the continuous variables of H_1, $x_1, \ldots, x_n$, and of H_2, $x_{n+1}, \ldots, x_{n+m}$. The *parallel composition* of H_1 and H_2 is

$$H_1 \times H_2 = (L_1 \times L_2 \times M_1 \times M_2, \Sigma_1 \cup \Sigma_2, E, X, G, R)$$

$X : L_1 \times L_2 \to \mathcal{X}(M_1 \times M_2)$ assigns vector field $[X^l \; X^{l'}]^T$ to location (l, l'). $e = ((l_1, l_2), \sigma, (l_1', l_2')) \in E$ if one of the following is true:

1. $\sigma \in \Sigma_1 \setminus \Sigma_2$ and $e_1 = (l_1, \sigma, l_1') \in L_1$.
   Then $g_e = g_{e_1} \times M_2$ and $r_e(x^1, x^2) = [r_{e_1}(x^1) \; x^2]^T$, where $x^1 \in M_1$ and $x^2 \in M_2$.

2. $\sigma \in \Sigma_2 \setminus \Sigma_1$ and $e_2 = (l_2, \sigma, l_2') \in L_2$.
   Then $g_e = M_1 \times g_{e_2}$ and $r_e(x^1, x^2) = [x^1 \; r_{e_2}(x^2)]^T$.

3. $\sigma \in \Sigma_1 \cap \Sigma_2$, $e_1 = (l_1, \sigma, l_1') \in L_1$ and $e_2 = (l_2, \sigma, l_2') \in L_2$.
   Then $g_e = g_{e_1} \times g_{e_2}$ and $r_e(x^1, x^2) = [r_{e_1}(x^1) \; r_{e_2}(x^2)]^T$.

Theorem 3.3.2 (Parallel Composition). *Given H_1 and H_2, suppose bisimulations exist using the stable partitions method on $U_1 \subseteq M_1$ and $U_2 \subseteq M_2$. If for each pair $(l_i, l_j) \in L_1 \times L_2$, there exists a one-form of the Pfaffian system at l_i*

$$h(dx_1, \ldots, dx_n) - dt = 0,$$

and a one-form of the Pfaffian system at l_j

$$h'(dx_{n+1}, \ldots, dx_{n+m}) - dt = 0,$$

such that the one-form

$$h(dx_1, \ldots, dx_n) - h'(dx_{n+1}, \ldots, dx_{n+m}) = d\alpha_{ij},$$

is exact, and α_{ij} is independent of the first integrals of X^{l_i} on U_1 and X^{l_j} on U_2, then, assuming the appropriate compatibility conditions are satisfied, a bisimulation of $H_1 \times H_2$ can be constructed.

Proof. Since the bisimulations of H_1 and H_2 have been constructed with the stable partitions method, we have $n-1$ first integrals for each X^{l_i}, $l_i \in L_1$ and $m-1$ first integrals for each X^{l_j}, $l_j \in L_2$, giving $n+m-2$ first integrals for the vector field $X = [X^{l_i} \; X^{l_j}]^T$. To construct a stable partition on $U_1 \times U_2$ we require $n+m-1$ independent first integrals and the missing one is supplied by α_{ij}. To see that $L_X \alpha_{ij} = 0$, observe that

$$dt = \frac{dx_i}{X_i(x)} = h(dx_1, \ldots, dx_n) = h'(dx_{n+1}, \ldots, dx_{n+m})$$

where X_i is the ith component of X and $i \in 1, \ldots, n+m$. □

3.4 Implementation

In this section we discuss the implementation of our method. There are two steps: (1) automatic generation of stable partitions, (2) construction of $H_{\simeq}$. The essence of the first step is to automatically generate local first integrals. We rely on the Prelle-Singer procedure [78], which has been implemented in computer algebra packages [66]. Building the automaton $H_{\simeq}$ involves labeling equivalence classes of the stable partitions, checking compatibility conditions, and defining transitions. Both in this approach and the approximative approach of [23], determining the edges of $H_{\simeq}$ corresponding to σ-steps of H can be stated as a problem of existential quantifier elimination. This problem is beyond the scope of this thesis but will the addressed in our future work. (We have not even touched the computational geometry view, in which the bisimulation partition is a *cell decomposition.*)

3.4.1 Automatic generation of first integrals

Prelle and Singer [78] showed that if a differential equation has an elementary first integral (using elementary functions sin, cos, exp, log, arctan, etc.) they must be of a special form. This lead to a semi-decision procedure for finding first integrals. Its extension to vector fields with transcendental terms was described in [66]. We outline the procedure for nth order differential equations following [67].

Consider the differential equation $\dot{x} = f(x)$, $x \in \mathbb{R}^n$ and define the differential operator $D = \sum_{i=1}^{n} X_i \frac{\partial}{\partial x_i}$. The Prelle-Singer procedure involves the following steps.

(1) Set N = 1.

(2) Find all monic, irreducible polynomials g_i with degrees $\leq N$ such that g_i divides Dg_i.

(3) Let $Dg_i = g_i h_i$. Decide if there are constants n_i not all zero such that $\sum_{i=1}^{m} n_i h_i = 0$. If such n_i exist, then $\Pi_{i=1}^{m} g_i^{n_1}$ is a first integral. If no such n_i exist then go to the next step.

(4) Increase N by 1.

The procedure is a semi-decision procedure because an effective bound on N is unknown. Step (2) is the most involved and is discussed in [66].

3.4.2 Symbolic model checking

The size of the automaton $H_{\simeq}$ is exponential in the number of parallel components (automata) of the hybrid system and the dimension of the continuous state space. Therefore, rather than *enumerating* all the states of $H_{\simeq}$, the *symbolic* approach explores only the parts of the state space that are relevant and it does so using a symbolic representation of the state space. This approach has reported remarkable results for hardware verification [25]. Symbolic model checking involves computing a fixed point of a functional on the state space. Questions about whether a system satisfies a specification (expressed in a temporal logic formula) can be reduced to a reachability analysis on the hybrid state space. The symbolic reachability analysis is performed by iterating on a *Pre* or *Post* operator, which operate on sets of formulas that represent regions of the hybrid state space; hence the term "symbolic".

We define some notation following [1]. A subset of M is called a *region*. A subset of $Q = \cup_{l \in L}\{l\} \times M_l$ is called a *zone*. Each zone Z can be uniquely decomposed into a collection $\bigcup_{l \in L}\{l\} \times U^l$, where each U^l is a region. We say $Z \subset Q$ is a *simple zone* if $Z = \{l\} \times U$, where U is a region. We define the set of all zones to be $\mathcal{Z}$.

Let $Z \in \mathcal{Z}$ be a simple zone, $\sigma \in \Sigma$, $t \in \mathbb{R}^+$, and $\Sigma' \subseteq \Sigma$. We define the post operators

$$Post(Z,\sigma) = \{q \in Q \mid \exists q' \in Z \,.\, q' \xrightarrow{\sigma} q\} \tag{3.4.1}$$

$$Post(Z,t) = \{q \in Q \mid \exists q' \in Z, \exists t \in \mathbb{R}^+ \,.\, q' \xrightarrow{t} q\} \tag{3.4.2}$$

$$Post(Z,\Sigma') = \bigcup_{\sigma \in \Sigma'} Post(Z,\sigma). \tag{3.4.3}$$

We define the pre operators,

$$Pre(Z,\sigma) = \{q \in Q \mid \exists q' \in Z \,.\, q \xrightarrow{\sigma} q'\} \tag{3.4.4}$$

$$Pre(Z,t) = \{q \in Q \mid \exists q' \in Z, \exists t \in \mathbb{R}^+ \,.\, q \xrightarrow{t} q'\} \tag{3.4.5}$$

$$Pre(Z,\Sigma') = \bigcup_{\sigma \in \Sigma'} Pre(Z,\sigma). \tag{3.4.6}$$

Let S be a set of formulas in the variables $q \in L \times M$. $\langle Z \rangle$ denotes a (non-unique) set of formulas that define Z. Following [48], H is *effective* if there is a class of formulas S which permits the symbolic analysis of H; namely

1. The emptiness problem for each predicate of S is decidable.
2. S is closed under boolean operations and *Pre* and *Post* operations.

3. The initial and final regions satisfy $\langle Q^0 \rangle, \langle Q^f \rangle \in \mathcal{S}$.

Let $\{\Psi_1^l, \ldots, \Psi_n^l\}$ be the euclidean coordinates for location $l \in L$. Define $\mathcal{S}$ to be the class of formulas

$$\{l\} \times \left(\Psi_i^l(x) \ \% \ c_i\right)$$

with $\% = \{\leq, <, =, >, \geq\}$, $l \in L$, $i = 1, \ldots, n$, and all finite conjunctions and disjunctions of these expressions.

Theorem 3.4.1. *H with $\mathcal{S}$ is effective.*

Proof. We observe that: (1) Q^0, Q^f can be represented as predicates of $\mathcal{S}$ by the compatibility assumption, (2) $\langle Pre(Z,t) \rangle$, $\langle Pre(Z,\sigma) \rangle$, $\langle Post(Z,\sigma) \rangle$, $\langle Post(Z,t) \rangle \in \mathcal{S}$ for $\langle Z \rangle \in \mathcal{S}$, by the compatibility of g_e and r_e and the stable partitions construction, (3) the emptiness problem for $\mathcal{S}$ is decidable. Indeed, consider a predicate defining a closed subset of M: $\exists x.(c_1 \leq \Psi_1(x) \leq d_1) \wedge \cdots \wedge (c_n \leq \Psi_n(x) \leq d_n)$. This predicate is equivalent to the quantifier free expression $(c_1 \leq d_1) \wedge \cdots \wedge (c_n \leq d_n)$. □

Chapter 4

A Menagerie of Examples

I shall take the liberty to defy that convention
and to tell you that the lunch on this occasion began with soles.
After that came the partridges, but if this suggests
a couple of bald, brown birds on a plate you are mistaken.
- Virginia Woolf.

In this chapter we present several applications. These applications fall in the category of verification of *dynamic agents*. "Dynamic agents" is a broad term encompassing autonomous systems that possess non-trivial dynamics and act or react to an environment that may include other dynamic agents. The very vagueness of this definition suits our purposes, for we do not yet know precisely what sort of dynamic agents will be the best candidates for model checking. Indeed, there is a gap between the idea of model checking of hybrid systems and applications where verification is proven to be effective, which will have to be closed in near term research.

Model checking of dynamic agents can be positioned in a hierarchy of models to which verification methods are being applied, going from the easiest to the most difficult. This hierarchy contains the following models:

1. **Finite automata.** Verification methods involve brute-force graph reachability analyses.

2. **Timed automata.** Finite number of modes, disturbances are discrete events, controls are discrete events. The dynamic agent either has trivial dynamics, or if it has non-trivial dynamics such as an aircraft or train, then it is restricted to follow a fixed track with a constant speed. Only temporal relationships are verified. An example is

a water level or temperature controller.

3. **Rectangular automata.** Finite number of modes, disturbances are discrete events, controls are discrete events. The dynamic agent either has trivial dynamics, or if it has non-trivial dynamics, then it is restricted to follow a fixed track with a speed lying within a constant range. Only temporal relationships are verified.

4. **Hybrid automata.** Finite number of modes, disturbances are discrete events, controls are discrete events. The dynamic agent can following the dynamics of each mode, not fixed to a track. Coordinated aircraft and robots are a good example.

5. **Hybrid automata + continuous disturbances** The same model as hybrid automata but we also permit continuous disturbances in each discrete mode. An example is an inverted pendulum controlled by a switching controller and subject to a wind disturbance.

6. **Continous open-loop model + discrete disturbance** Infinite number of modes (corresponding to an infinite number of feedback control laws). An example is an open-loop system subject to a component failure. The verification problem is to determine a feedback control such that control objectives are met in the face of a failure.

7. **Hybrid automaton + continuous open-loop models + continuous disturbance** The dynamic agent has a finite number of discrete modes and open-loop continuous dynamics (the velocity is often the input). Examples are a dog-fight between fighter aircraft and two cars trying to merge into the same lane. These problems have been solved using game theory [80, 63] and when the solution using the maximum principle yields a switching strategy, it can be encoded by a hybrid automaton.

8. **Hybrid automaton + continuous open-loop models + continuous and discrete disturbances** These are the most difficult models to verify. They include all the previous phenomena. Examples are the model considered in [16] and the powertrain control models studied in [10] and its references.

In this chapter we concentrate on model checking problems for the fourth level of difficulty: hybrid automata. Thus, we do not permit continuous disturbances or continuous open-loop dynamics. We show how to obtain the bisimulation for timed automata and linear

systems in Brunovsky normal form and Jordan form. We look at problems of coordinated autonomous agents, which make a compelling case for the need for a paradigm shift in control design and verification. Some examples are cooperating automated vehicles, aircraft, underwater vehicles, and mobile robots. We show how bisimulations can be constructed for coordinated aircraft and coordinated mobile robots. An important area where bisimulation can have an impact is in embedded systems design. We consider an automotive engine model which has served as a fertile testbed for development of new algorithmic approaches to design of embedded systems [11, 13]. Finally, we consider hybrid automata with integrable Hamiltonian dynamics.

4.1 Timed automata

A timed automaton has dynamics in Pfaffian form given by

$$\begin{aligned} dx_1 - dt &= 0 \\ &\vdots \\ dx_n - dt &= 0. \end{aligned}$$

There are $n-1$ independent tangential foliations defined by the submersions:

$$\begin{aligned} x_1 - x_2 &= c_1 \\ &\vdots \\ x_{n-1} - x_n &= c_{n-1}. \end{aligned}$$

where $c_i \in \mathbb{R}$. Note that the leaves of each foliation have dimension $n-1$. A transversal foliation is

$$x_n = d_n,$$

though the partition of [4] uses more transversal foliations because of the nature of the enabling and reset conditions:

$$\begin{aligned} x_1 &= d_1 \\ &\vdots \\ x_n &= d_n. \end{aligned}$$

Each of the leaves of the transversal foliations are transverse to every integral curve. Since the dynamics of each location is the same, the stable partition obtained from the foliations is the same, so the enabling conditions and reset conditions are compatible between locations.

4.2 Mobile robots

Consider the coordination problem of two mobile robots A and B, operating in a closed workspace of a factory. The robots are modeled using hybrid automata, with each control location corresponding to an atomic maneuver, such as "move forward", or "change direction". Each location of the automaton has the kinematic model of the associated maneuver. We assume in each automaton location, the control inputs are constant, but they are allowed to change instantaneously upon switching locations. The kinematic model for each robot, converted to chained form [71] is the following:

$$\begin{aligned} \dot{x}_1 &= u_1 \\ \dot{x}_2 &= u_2 \\ \dot{x}_3 &= x_2 u_1 \\ \dot{x}_4 &= x_3 u_1. \end{aligned}$$

There are three tangential foliations given by the equations

$$\begin{aligned} x_2 - \frac{u_2}{u_1} x_1 &= c_2 \\ x_3 - \frac{u_1}{2u_2} x_2^2 &= c_3 \\ x_4 + \frac{1}{3}\left(\frac{u_1}{u_2}\right)^2 x_2^3 - \frac{u_1}{u_2} x_2 x_3 &= c_4. \end{aligned}$$

and a transversal foliation given by:

$$x_1 = c_1.$$

To show these foliations define a bisimulation for each robot, we must check the regularity condition:

$$Dh = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -\frac{u_2}{u_1} & 1 & 0 & 0 \\ 0 & -\frac{u_1}{u_2} x_2 & 1 & 0 \\ 0 & -\frac{u_1}{u_2} x_3 + \left(\frac{u_1}{u_2}\right)^2 x_2^2 & -\frac{u_1}{u_2} x_2 & 1 \end{bmatrix}$$

This matrix has full rank so long as $u_1 \neq 0$ and $u_2 \neq 0$. Thus, the partition for each robot is defined globally on $\mathbb{R}^4$.

When we take their parallel composition, an extra tangential foliation is introduced:

$$u_{1B}x_{1A} - u_{1A}x_{1B} = c_{AB}.$$

A calculation similar to the next example shows that a bisimulation for the parallel composition exists.

4.3 Planar aircraft

Consider the coordination problem of two aircraft A and B flying at a fixed altitude, which was studied in the hybrid systems context in [95]. Each aircraft is modeled by a hybrid system in which an automaton location corresponds to an atomic maneuver performed with constant control inputs. The control inputs are changed instantaneously upon switching control locations. The state g is an element of the special euclidean group $SE(2)$, and X is an element of its algebra $se(2)$. Assuming the aircraft does not exercise it's pitch control, the kinematic dynamics of aircraft A are given by $\dot{g} = gX$ where

$$g = \begin{bmatrix} \cos\phi & -\sin\phi & x \\ \sin\phi & \cos\phi & y \\ 0 & 0 & 1 \end{bmatrix}$$

and

$$X = \begin{bmatrix} 0 & -u_1 & u_2 \\ u_1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

ϕ is the yaw angle, and the inputs u_1, u_2 control the yaw and velocity, respectively. There are two tangential foliations given by equations

$$\begin{aligned} u_1 x - u_2 \sin\phi &= c_x \\ u_1 y + u_2 \cos\phi &= c_y \end{aligned}$$

and a transversal foliation given by

$$\phi = c_\phi.$$

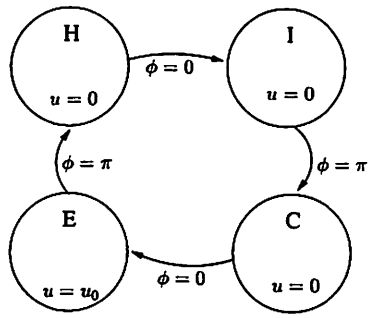

Figure 4.1: Hybrid model for a single four-stroke cylinder.

Letting the state variables and inputs of aircraft B be ϕ_B, x_B, y_B, u_{1B}, and u_{2B}, analogous expressions for the tangential and transversal foliations are obtained for aircraft B. An additional tangential foliation is found for the parallel composition of the two systems given by

$$u_{1B}\phi_A - u_{1A}\phi_B = c_{AB}.$$

We check the regularity condition on the five tangential foliations and either of the two transversal foliations. Namely,

$$Dh = \begin{bmatrix} u_{1A} & 0 & -u_{2A}\cos\phi_A & 0 & 0 & 0 \\ 0 & u_{1A} & -u_{2A}\sin\phi_A & 0 & 0 & 0 \\ 0 & 0 & u_{1B} & 0 & 0 & -u_{1A} \\ 0 & 0 & 0 & u_{1B} & 0 & -u_{2B}\cos\phi_B \\ 0 & 0 & 0 & 0 & u_{1B} & -u_{2B}\sin\phi_B \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

This matrix has full rank so long as $u_{1A}, u_{1B} \neq 0$, so the partition is defined globally on $\mathbb{R}^4 \times \mathbb{T}^2$. If, in addition, $\frac{u_{1A}}{u_{1B}}$ is rational, a finite bisimulation on $U \times \mathbb{T}^2$, for compact $U \subset \mathbb{R}^4$, exists.

4.4 Powertrain model

Hybrid control of the powertrain of an automotive engine was studied in [12, 11]. The model has inherent hybrid behavior because of the action of the four-stroke cylinders and

is complicated by the fact that the input to the continuous dynamics is determined by variables computed in an earlier mode. Following [12], each four-stroke cylinder can be modeled as a hybrid automaton with locations { H, I, C, E } corresponding to the state of the piston: exhaust (H), intake (I), compression (C), and expansion (E) (see Figure 4.1). The continuous dynamics in each of these modes captures the relationship between axel torsion angle, crankshaft angle and speed, wheel speed and the input torque. After a coordinate transformation the powertrain model is:

$$\begin{bmatrix} \dot{x}' \\ \dot{x} \\ \dot{\phi} \end{bmatrix} = \begin{bmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda & -\omega & 0 \\ 0 & \omega & \lambda & 0 \\ 1 & 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} x' \\ x \\ \phi \end{bmatrix} + bu$$

where u is the torque and ϕ is the crankshaft angle. The control objective is to minimize the peak acceleration a where $a = cx$ for a constant $c \in \mathbb{R}^{1\times 2}$ (assuming u is constant).

The control inputs are the fuel injection and the spark advance which are computed in the transitions from modes E to H and I to C, and which determine the torque applied in mode E. As in [12], we will treat the problem of torque generation based on fuel injection and spark advance as an off-line calculation. We compute the torque as a continuous input directly, but include the correct delay in it's generation in the hybrid model. The torque takes one of a finite number of constant values $U = \{u_1 = 0, \ldots, u_m\}$. Figure 4.2 shows the proposed approach for the case of two values of the control. The locations H, I, and C are combined since $u = 0$ in these states. The control for location E is determined by the continuous state in the transition from E to HIC, based on the enabling conditions g_e. The enabling conditions are selected such that the the peak acceleration is minimized. This objective can either be encoded as a cost function, but inherits the difficulty of not being differentiable, or it can be encoded in a myopic, greedy control strategy. We take the latter approach. Let $z = [0\ x\ 0]^T$. At each point $y = [x'\ x\ \phi]^T$ we select the control to be

$$u(y) = \arg\max_{u\in U}\{\ -(Ay + bu)^T \cdot z\ \}.$$

That is, we pick the control $u(y)$ such that the component of the vector field $Ay + bu(y)$ in the direction of $-x$ is maximized. The enabling conditions are defined by switching boundaries at which $-(Ay+bu_1)^T \cdot z = -(Ay+bu_2)^T \cdot z$ for any $u_1 \neq u_2 \in U$. The enabling conditions can be synthesized using the bisimulation for linear systems found in the next section.

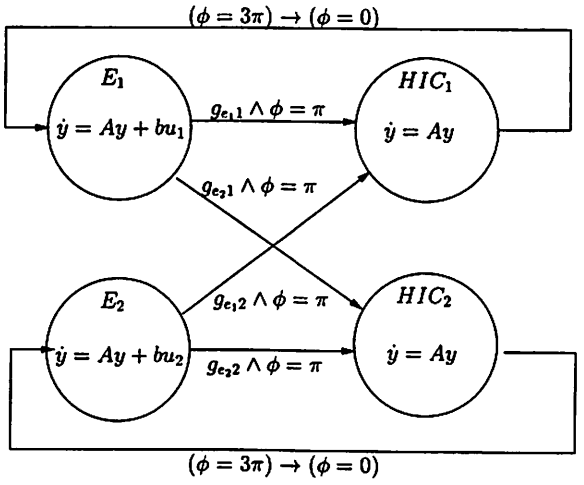

Figure 4.2: Hybrid control for a single four-stroke cylinder.

4.5 Linear systems

We present results for Brunovsky normal form and for Jordan form (though this is slightly repetitive) to demonstrate a procedure for finding first integrals when an explicit solution of the ODE is available.

Suppose we have the differential equation

$$\dot{x} = f(x), \qquad x(0) = c \in \mathbb{R}^n \tag{4.5.1}$$

and a solution $x = \phi(t, c)$. Then

$$F(t, x, c) = x - \phi(t, c)$$

vanishes on solutions of (4.5.1). For values of c where F is non-singular we use the implicit function theorem to obtain

$$\begin{aligned} c_1 &= g_1(x, t) \\ &\vdots \\ c_{n-1} &= g_{n-1}(x, t) \\ t &= g_n(x, c). \end{aligned}$$

$g_1, \ldots, g_{n-1}$ are time-varying first integrals of (4.5.1). To obtain time-invariant first integrals we substitute t in $F(t,x,c)$ to obtain $\overline{F}(x,c)$. Using $\overline{F}$ we seek functions $\Psi_i(\cdot) : \mathbb{R}^n \to \mathbb{R}$ for $i = 1, \ldots, n-1$ such that $\overline{F}_i(x,c) = 0 = \Psi_i(x) - \Psi_i(c)$. $\Psi_i(x)$ are time-invariant first integrals of (4.5.1).

4.5.1 Brunovsky normal form

Consider a hybrid automaton whose continuous dynamics are in Brunovsky normal form:

$$\begin{aligned} \dot{x}_1 &= x_2 \\ &\vdots \\ \dot{x}_{m-1} &= x_m \\ \dot{x}_m &= u \end{aligned}$$

where $u \in \mathbb{R}$. The solution is $x_i(t) = u\frac{t^{k+1}}{(k+1)!} + \sum_{j=0}^{k} c^{m-k+j}\frac{t^j}{j!}$ where $c \in \mathbb{R}^n$ is the initial condition. We obtain a recursive expression for the first integrals:

$$\Psi_{m-k} := x_{m-k} - \frac{x_m^{k+1}}{(k+1)!u^k} - \sum_{j=1}^{k-1} \frac{x_m^j}{j!u^j}\Psi_{m-k+j}.$$

We show these are first integrals by an inductive argument. First we verify that $D\Psi_m \cdot f = 0$, where f is the Brunovsky normal form vector field. Suppose $D\Psi_{m-j} \cdot f = 0$, for $j = 1, \ldots, k-1$. Then

$$\begin{aligned} D\Psi_{m-k} \cdot f &= x_{m-k+1} - \frac{x_m^k}{k!u^{k-1}} - \sum_{j=1}^{k-1} \frac{x_m^{j-1}}{(j-1)!u^{j-1}}\Psi_{m-k+j} \\ &= x_{m-k+1} - \frac{x_m^k}{k!u^{k-1}} - \sum_{l=1}^{k-2} \frac{x_m^l}{l!u^l}\Psi_{m-k+1+l} - \Psi_{m-k+1} \\ &= 0. \end{aligned}$$

A transversal foliation is defined by

$$\Psi_m := x_m = c_m.$$

It is easy to check that $\{\Psi_1, \ldots, \Psi_m\}$ are independent so long as $u \neq 0$, so the partition is globally valid.

4.5.2 Jordan form

For each $l \in L$, the procedure is the following: (1) for each type of elementary Jordan block derive expressions for the local first integrals, defining a set of tangential foliations, (2) for each pair of elementary Jordan blocks derive an expression for the coupling first integral, defining another tangential foliation, and finally, (3) derive an expression for the submersion corresponding to a foliation transverse to the linear flow.

We consider the linear system

$$\dot{x} = Ax \tag{4.5.2}$$

where $A \in \mathbb{R}^{n \times n}$ is of the form $A = diag(J^r \cdots J^r J^c \cdots J^c)$. J^r and J^c are elementary Jordan blocks corresponding to the real (repeated) eigenvalues and complex (repeated) eigenvalues of A, respectively. Following the proposed procedure, we first derive the local first integrals for J^r and J^c.

Real Eigenvalues

Consider the elementary Jordan block $J^r \in \mathbb{R}^{m \times m}$ given by

$$J^r = \begin{bmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & & 1 \\ & & & \lambda \end{bmatrix} \tag{4.5.3}$$

where $\lambda \in \mathbb{R}$. The solution of $\dot{x} = J^r x$ with initial condition $c \in \mathbb{R}^m$ is

$$x(t) = e^{\lambda t} \begin{bmatrix} 1 & t & \frac{t^2}{2!} & \cdots & \frac{t^{m-1}}{(m-1)!} \\ & 1 & t & \cdots & \\ & & \ddots & \ddots & \vdots \\ & & & 1 & t \\ & & & & 1 \end{bmatrix} c. \tag{4.5.4}$$

We obtain $m-1$ first integrals $\Psi_1^r, \ldots, \Psi_m^r$ as follows. From the solution of x_m we find

$$e^{\lambda t} = \frac{x_m}{c_m}. \tag{4.5.5}$$

The solution of x_{m-1} combined with (4.5.5) gives

$$t = \frac{x_{m-1}}{x_m} - \frac{c_{m-1}}{c_m}. \tag{4.5.6}$$

Substituting (4.5.6) in (4.5.5) we obtain the first integral

$$\Psi^r_{m-1} := x_m \exp\left(-\lambda \frac{x_{m-1}}{x_m}\right) = d_{m-1} \tag{4.5.7}$$

where $d_{m-1} \in \mathbb{R}$. The remaining $m-2$ first integrals are found by substituting (4.5.5) and (4.5.6) in the solutions for x_1 through x_{m-2}. Carrying out this operation recursively, we obtain the first integrals

$$\Psi^r_{m-2} := \frac{x_{m-2}}{x_m} - \frac{x^2_{m-1}}{2x^2_m} = d_{m-2} \tag{4.5.8}$$

$$\Psi^r_{m-3} := \frac{x_{m-3}}{x_m} - \frac{x_{m-2}x_{m-1}}{x^2_m} - \frac{x^3_{m-1}}{3x^3_m} = d_{m-3} \tag{4.5.9}$$

$$\vdots$$

$$\Psi^r_{m-k} := \frac{x_{m-k}}{x_m} - \sum_{j=1}^{k-2} \frac{1}{j!} \frac{x^j_{m-1}}{x^j_m} \Psi^r_{m-(k-j)} - \frac{1}{k!} \frac{x^k_{m-1}}{x^k_m} = d_{m-k} \tag{4.5.10}$$

where $d_j \in \mathbb{R}$. We show these are first integrals by an inductive argument. First, $D\Psi_{m-2} \cdot J^r x = 0$. Suppose $D\Psi^r_{m-j} \cdot J^r x = 0$ for $j = 2, \ldots, k-1$. Then

$$D\Psi_{m-k} \cdot J^r x = \frac{x_{m-k+1}}{x_m} - \frac{x^{k-1}_{m-1}}{(k-1)! x^{k-1}_m} - \sum_{j=1}^{k-2} \frac{x^{j-1}_{m-1}}{(j-1)! x^{j-1}_m} \Psi^r_{m-k+j} = 0.$$

Complex Eigenvalues

Consider the elementary Jordan block $J^c \in \mathbb{R}^{m \times m}$ given by

$$J^c = \begin{bmatrix} D & I_2 & & \\ & \ddots & \ddots & \\ & & & I_2 \\ & & & D \end{bmatrix} \tag{4.5.11}$$

where

$$D = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}; \qquad I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Following [54], the solution of $\dot{x} = J^c x$ is found by converting to the complex domain. Let $z : \mathbb{R} \to \mathbb{C}^{\frac{m}{2}}$, $i \cdot i = -1$, and consider $\dot{z} = Bz$, where

$$B = \begin{bmatrix} \mu & 1 & & \\ & \ddots & \ddots & \\ & & & 1 \\ & & & \mu \end{bmatrix} \quad ; \qquad \mu = a + ib. \tag{4.5.12}$$

We identify $\mathbb{C}^{\frac{m}{2}}$ with $\mathbb{R}^m$ by the correspondence

$$(z_1, \ldots, z_{\frac{m}{2}}) = (x_1 + ix_2, \ldots, x_{m-1} + ix_m).$$

The solution of $\dot{z} = Bz$ is

$$z_k(t) = e^{\mu t} \sum_{j=k}^{\frac{m}{2}} \frac{t^{j-k}}{(j-k)!} c_j.$$

We obtain $m-1$ first integrals $\Psi_1^c, \ldots, \Psi_m^c$ as follows. First, from the solutions of x_{m-1} and x_m we derive the useful expressions:

$$e^{at} = \left(\frac{x_{m-1}^2 + x_m^2}{c_{m-1}^2 + c_m^2} \right)^{\frac{1}{2}} \tag{4.5.13}$$

$$e^{at} \cos bt = \frac{c_{m-1} x_{m-1} + c_m x_m}{c_{m-1}^2 + c_m^2} \tag{4.5.14}$$

$$e^{at} \sin bt = \frac{c_{m-1} x_m - c_m x_{m-1}}{c_{m-1}^2 + c_m^2}. \tag{4.5.15}$$

Let

$$X_{k+} = \frac{x_{m-k} x_{m-1} + x_{m-k+1} x_m}{x_{m-1}^2 + x_m^2}$$

$$X_{k-} = \frac{x_{m-k} x_m - x_{m-k+1} x_{m-1}}{x_{m-1}^2 + x_m^2}.$$

Evaluating X_{3+} gives

$$t = \frac{x_{m-3} x_{m-1} + x_{m-2} x_m}{x_{m-1}^2 + x_m^2} - \frac{c_{m-3} c_{m-1} + c_{m-2} c_m}{c_{m-1}^2 + c_m^2}. \tag{4.5.16}$$

Equipped with (4.5.13) - (4.5.16) we can find $m-1$ first integrals. Considering the last two equations of $\dot{x} = J^c x$ and using polar coordinates, we obtain a first integral

$$\Psi_{m-1}^c := \sqrt{x_m^2 + x_{m-1}^2} \exp\left(-a X_{3+}\right) = d_{m-1} \tag{4.5.17}$$

where $d_{m-1} \in \mathbb{R}$. The remaining $m-2$ first integrals are found by evaluating X_{k+} and X_{k-} for $k = 3, 5, 7, \ldots, m-1$ and substituting (4.5.13) - (4.5.16) in the solutions for x_m to x_1. Considering the evaluation of X_{k-} we obtain the first integrals

$$\begin{aligned} \Psi^c_{m-2} &:= X_{3-} = d_{m-2} \\ &\vdots \\ \Psi^c_{m-k+1} &:= X_{k-} - \sum_{j=1}^{\frac{k-3}{2}} \frac{1}{j!} X_{3+}^j \Psi^c_{m-k+1+2j} = d_{m-k+1}. \end{aligned}$$

Considering the evaluation of X_{k+}, we first obtain the first integral

$$\Psi^c_{m-3} := \frac{x_{m-3}^2 + x_{m-2}^2}{x_{m-1}^2 + x_m^2} - X_{3+}^2 = d_{m-3}.$$

The remaining first integrals for $k = 5, 7, \ldots$ are

$$\begin{aligned} \Psi^c_{m-5} &:= X_{5+} - \frac{1}{2} X_{3+}^2 = d_{m-5} \\ &\vdots \\ \Psi^c_{m-k} &:= X_{k+} - \sum_{j=1}^{\frac{k-5}{2}} \frac{1}{j!} X_{3+}^j \Psi^c_{m-k+2j} - \frac{1}{p!} X_{3+}^p = d_{m-k} \end{aligned}$$

where $p = \frac{k-1}{2}$.

Coupling integrals

It remains to find the first integrals describing the coupling between elementary Jordan blocks. We consider the pairs (J^r, J^r), (J^r, J^c), and (J^c, J^c).

For the coupling between a J^r and a J^c block, it suffices to find a coupling first integral for the system

$$\dot{x} = \begin{bmatrix} \lambda & 0 & 0 \\ 0 & a & -b \\ 0 & b & a \end{bmatrix} x. \tag{4.5.18}$$

Using polar coordinates $x_2 = r\cos\theta$, $x_3 = r\sin\theta$, we have $\dot{r} = ar$, from which it is seen that

$$x_1^a (x_2^2 + x_3^2)^{-\frac{\lambda}{2}} = d$$

where $d \in \mathbb{R}$. For the coupling between two J^r blocks it suffices to find a first integral for the system

$$\dot{x} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} x \tag{4.5.19}$$

which corresponds to the last row of each J^r block. We obtain

$$\lambda_2 x_1 - \lambda_1 x_2 = d.$$

For the coupling between two J^c blocks it suffices to consider the system

$$\dot{x} = \begin{bmatrix} \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} & \\ & \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} \end{bmatrix} x. \tag{4.5.20}$$

Converting to polar coordinates, we have $\dot{\theta}_1 = b_1$ and $\dot{\theta}_2 = b_2$, so

$$b_2 \tan^{-1}(\frac{x_2}{x_1}) - b_1 \tan^{-1}(\frac{x_4}{x_3}) = d.$$

Transversal foliation

An expression for the submersion defining the transversal foliation is found by considering a particular instance of the A matrix. Because of the diagonal structure of the Jordan form, an initial candidate is $\Psi_m := x_m = d_m$, but better candidates are often available which are independent of the first integrals over a larger domain.

In two dimensions there is a canonical choice for the transversal foliation given by the first integral of a complementary vector field. Suppose we have $\dot{x} = A_1 x$ with A_1 non-singular and we want to find A_2 such that for all x, $A_1 x$ and $A_2 x$ are not colinear. That is, there does not exist $\lambda \in \mathbb{R}$ such that $\lambda A_1 x = A_2 x$. Equivalently, $A^{-1} A_2$ has no real eigenvalues (it always involves a rotation). We select

$$A_2 = A_1 \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

A first integral of $\dot{x} = A_2 x$ defines of a transversal foliation of $\dot{x} = A_1 x$.

Finally, in practice it is often advantageous to introduce extra transversal foliations or submanifolds (as in timed automata) in order to achieve compatibility conditions or to keep the equivalence classes from being too large.

4.5.3 Decidability of hybrid systems with linear dynamics

Let $\Psi = \{\Psi_i^l\}_{i\in\{1,\dots,n\},l\in L}$ be the set of submersions obtained in the steps above.

Theorem 4.5.1. *Let H be a hybrid automaton with linear dynamics in Jordan form and let Ψ be such that for each $l \in L$, $\{\Psi_1^l, \dots, \Psi_n^l\}$ form a set of euclidean coordinates on M_l. If H is compatible with the equivalence relations $\{\simeq^l\}$ defined using Ψ, then the reachability problem for H is decidable.*

4.6 Integrable Hamiltonian hybrid automata

We consider hybrid automata in which the continuous state space is a *symplectic manifold* endowed with a nondegenerate skew symmetric bilinear form ω^2 and denoted (M,ω^2). For each $x \in M$, $\omega^2 : T_xM \times T_xM \to \mathbb{R}$ is closed. Since non-degenerate skew-symmetric forms exist only on even dimensional spaces, M is even dimensional with dimension n. The dynamics of location l are given in local coordinates q_i, p_i, $i = 1, \dots, \frac{n}{2}$ by

$$\begin{aligned} \dot{q} &= \frac{\partial \mathcal{H}_l}{\partial p} \\ \dot{p} &= -\frac{\partial \mathcal{H}_l}{\partial q} \end{aligned}$$

where $\mathcal{H}_l : M \to \mathbb{R}$ is the *Hamiltonian.*

We require some definitions from [6]. Let $y \in T_xM$. Associated with y is a one-form $\omega_y^1(v) = \omega^2(v,y)$ where $v \in T_xM$. This defines an isomorphism $I : T_x^*M \to T_xM$ between the one-forms and vector fields on a symplectic manifold (M,ω^2). Let $g_1, g_2 : M \to \mathbb{R}$ be two functions on M. The *Poisson bracket* of g_1, g_2 is $\{g_1,g_2\} = g$ where $[Idg_1, Idg_2] = Ig$ and $[\cdot,\cdot]$ is the Lie bracket. Thus, the Poisson bracket is the dual of the Lie bracket on a symplectic manifold. We say $g_1, g_2 : M \to \mathbb{R}$ are *in involution* if their Poisson bracket is equal to zero.

If there exist $\frac{n}{2}$ independent first integrals $\Psi_1, \dots, \Psi_{\frac{n}{2}} = \mathcal{H}$ which are in involution then the *Hamilton-Jacobi method* provides a prescription for finding the remaining $\frac{n}{2} - 1$ first integrals $\Psi_{\frac{n}{2}+1}, \dots, \Psi_{n-1}$. The essence of the method, following the model of the Frobenius theorem and Flow Box theorem, is to select $\Psi_1, \dots, \Psi_{\frac{n}{2}}$ as the first $\frac{n}{2}$ coordinates and then construct the remaining independent coordinates. Thus, we define a coordinate

transformation $(q,p) \to (q',p')$ by a generating function $S(q,p')$ satisfying

$$p = \frac{\partial S}{\partial q_i}, \qquad q' = \frac{\partial S}{\partial p'}.$$

The generating function has the form

$$S = \int P(q,p')dq$$

where P is the solution of

$$\begin{aligned} \Psi_1(q,p) &= p'_1 \\ &\vdots \\ \Psi_{\frac{n}{2}}(q,p) &= \mathcal{H}. \end{aligned}$$

Th closedness of the one-form $P(q,p')dq$ is proved using the involutivity of the Ψ_i. In the new coordinates we have

$$\dot{q}' = \frac{\partial \mathcal{H}'_l}{\partial p'}, \qquad \dot{p}' = -\frac{\partial \mathcal{H}'_l}{\partial q'}$$

with $H'(q',p') = p'_{\frac{n}{2}}$ or

$$\begin{aligned} \dot{p}' &= 0 \\ \dot{q}'_1 &= 0 \\ &\vdots \\ \dot{q}'_{\frac{n}{2}-1} &= 0 \\ \dot{q}'_{\frac{n}{2}} &= 1. \end{aligned}$$

Thus, we have achieved a simple translation flow, just as in the Flow Box theorem. The new first integrals are $\Psi_{\frac{n}{2}+i} = q'_i$ for $i = 1, \ldots, \frac{n}{2} - 1$. A transversal foliation is defined by $\Psi_n = q'_{\frac{n}{2}}$.

Remark 4.6.1. Recall that a system $\dot{x} = f(x)$ is said to be completely integrable if there exist $(n-1)$ independent first integrals. What we have seen up to now is that existence of $(n-1)$ independent first integrals for each vector field of automaton H and the compatibility of H with the stable partitions together are a *sufficient* condition for H to admit a finite bisimulation. The example of integrable Hamiltonian vector fields shows that existence of $(n-1)$ independent first integrals is not a necessary condition. Indeed complete integrability is obtained even if there are fewer than $(n-1)$ first integrals.

Examples of integrable Hamiltonian hybrid automata abound and many of them are quite interesting in engineering (and physics) applications. We consider a familiar example that will motivate the next chapter.

4.6.1 Inverted Pendulum

Suppose we have a planar pendulum with mass $m = 1$ suspended from a link of length $l = 1$. The objective is to swing the pendulum up to a vertical position. Let θ be the angle the pendulum makes with the vertical such that $\theta = 0$ at the top. Suppose we attach a string to the pendulum so that a horizontal force denoted u can be applied to the mass. Letting $x_1 = \theta$ and $x_2 = \dot{\theta}$, the equations of motion are

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= g \sin x_1 - u \cos x_1. \end{aligned}$$

Using feedback linearization we can find the stabilizing controller

$$u_f = \frac{g \sin x_1 + a_1 x_1 + a_2 x_2}{\cos x_1}$$

but this controller is valid only locally near the origin. To obtain a globally valid controller we use a switching strategy as proposed in [7]. There are a number of ways to swing up the pendulum depending on how many swings it takes before reaching the "capture zone" of u_f. Ideally we want a synthesis procedure that automatically finds all possible switching strategies. We using our bisimulation approach to do this. Suppose that we allow the control to take three values $u = \{0, 2g, 3g\}$. The system has the first integral

$$\Psi_2 = \frac{1}{2} x_2^2 + g \cos x_1 + u \sin x_1.$$

A transversal foliation valid over the region $[-\pi, \pi] \times [-4, 4]$ is

$$\Psi_1 = \frac{x_2}{(x_1 \pm \pi)^2}.$$

The bisimulation partition is shown in Figure 4.3 for $u = 0$ and Figure 4.4 for $u = 2g$. (We have added some additional transversal submanifolds so that the two dimensional equivalence classes are roughly the same size).

The hybrid automaton would consist of four locations: three for the three values of u and one for the controller u_f. The synthesis problem is to find the enabling conditions which

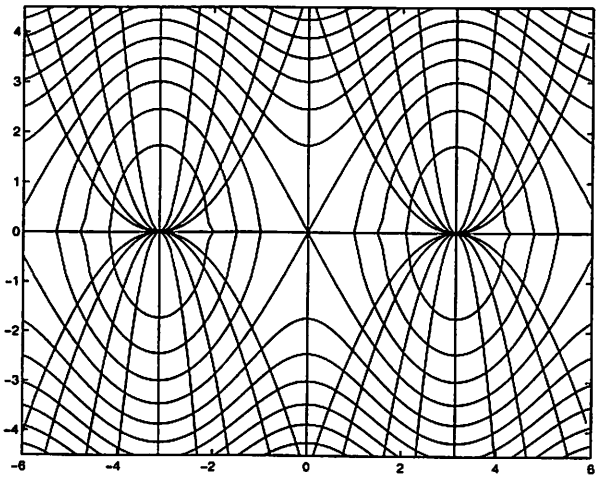

Figure 4.3: Bisimulation partition for the pendulum with $u = 0$.

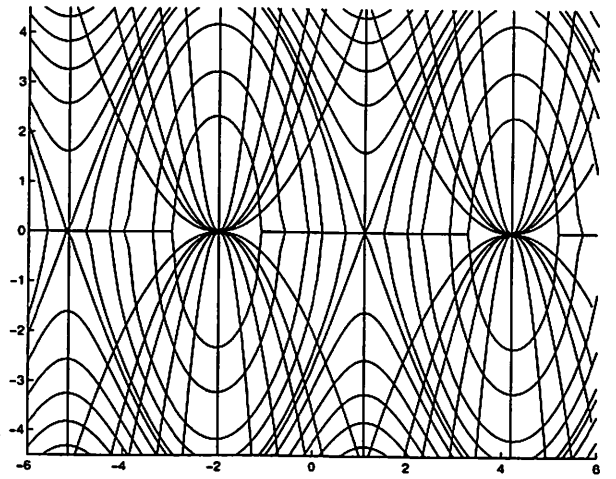

Figure 4.4: Bisimulation partition for the pendulum with $u = 2g$.

swing the pendulum to the capture region of u_f. Finally, it is of interest to synthesize controllers using the bisimulation approach which also satisfy some other criterion, such as minimum effort or minimum time. This is the subject of the next chapter.

Chapter 5

Optimal Controller Synthesis

To make a prairie it takes a clover and one bee,
One clover and a bee, and revery.
The revery alone will do,
If bees are few.
- Emily Dickinson.

5.1 Introduction

The goal of this chapter is to develop of a computationally appealing technique for synthesizing optimal controls for continuous feedback systems $\dot{x} = f(x, u)$ and hybrid systems, which reduces substantially the complexity of the problem. The goal is achieved by recasting the problem to a hybrid optimal control problem. The hybrid problem is obtained by approximating the control set $U \subset \mathbb{R}^m$ by a finite set $\Sigma \subset U$ and defining vector fields for the locations of the hybrid system of the form $f(x, \sigma)$, $\sigma \in \Sigma$; that is, the control is constant in each location. The hybrid control problem is, then, to synthesize an optimal switching rule between locations, or equivalently, optimal enabling conditions, such that a target set $\Omega_f \subset \Omega$ is reached while a hybrid cost function is minimized, for each initial condition in a specified set $\Omega \subset \mathbb{R}^n$.

Casting the problem into the domain of hybrid control is not appealing per se, on the contrary! Algorithmic approaches for solving the controller synthesis problem for specific classes of hybrid systems have appeared [65, 103] but no general, efficient algorithm is yet available. Hence, to be able to solve the (nonlinear) hybrid optimal control problem, we exploit the bisimulation, if it exists, of the hybrid automaton, which translates the problem to an equivalent discrete one.

Using the quotient system obtained from the bisimulation, we synthesize a discrete supervisor, assigning a switching rule between locations of the automaton, that minimizes a discrete cost function approximating the original cost function, for each initial discrete state. We provide a dynamic programming solution to this problem, with extra constraints to ensure non-Zenoness of the closed-loop trajectories. By imposing non-Zeno conditions on the synthesis we obtain piecewise constant controls with a finite number of discontinuities in bounded time.

The discrete value function depends on the discretizations of U and of Ω using the bisimulation. We quantify these discretizations by parameters δ and δ_Q, respectively. The main theoretical contribution is to show that as $\delta, \delta_Q \to 0$, the discrete value function converges to the unique viscosity solution of the Hamilton-Jacobi-Bellman (HJB) Equation.

5.1.1 Motivation

This approach to optimal control is a variant of *regular synthesis*, introduced in [19], in the sense that both restrict the class of controls to a set that has some desired property and both use a finite partition to define switching behavior. For linear systems, the results on regular synthesis are centered on the Bang-Bang principle [77], stating that a sufficient class of optimal controls is piecewise constant. If U is a convex polyhedron, then the number of discontinuities of the control is bounded. There is no hope that general Bang-Bang results are available due to the following example.

Example 5.1.1 (Fuller's problem [44]). Consider the optimal control problem

$$\dot{x}_1 = x_2 \tag{5.1.1}$$

$$\dot{x}_2 = u \tag{5.1.2}$$

with $|u| \leq 1$ and the cost function $J(x, \mu) = \int_0^{T(x,\mu)} x_1^2(s)ds$. If $y \in \mathbb{R}^2$ is any point except the origin, then there exists a unique optimal control driving y to the origin, and it is bang-bang with infinite number of switchings. In fact Kupka has shown in [59] that this phenomenon is generic at sufficiently high dimensions.

Inspite of Fuller's example, in many (engineering) applications the optimal control is a piecewise continuous function, and therefore methods of regular synthesis of such controls

are worth investigating. A good review of the results on regular synthesis can be found in the summary article [86].

Our work focuses on piecewise constant controls and provides a constructive approach to obtain a cell decomposition by using a finite bisimulation, which further allows us to formulate the synthesis problem on its quotient system - a finite automaton.

The idea of using a time abstract model formed by partitioning the continuous state space has been pursued in a number of papers recently. Stiver, Antsaklis, and Lemmon [92] use a partition of the state space to convert a hybrid model to a discrete event system (DES). This enables them to apply controller synthesis for DES's to synthesize a supervisor. While our approach is related to this methodology, it differs in that we have explicit conditions for obtaining the partition. In [82] hybrid systems consisting of a linear time-invariant system and a discrete controller that has access to a quantized version of the linear system's output is considered. The quantization results in a rectangular partition of the state space. This approach suffers from *spurious solutions* that must be trimmed from the automaton behavior.

Hybrid optimal control problems have been studied in papers by Witsenhausen [102] and Branicky, Borkar, Mitter [20]. These studies concentrate on problems of well-posedness, necessary conditions, and existence of optimal solutions but do not provide algorithmic solutions.

5.2 Optimal control problem

Let U be a compact subset of $\mathbb{R}^m$, Ω an open, bounded, connected subset of $\mathbb{R}^n$, and Ω_f a compact subset of Ω. Define $\mathcal{U}_m$ to be the set of meansurable functions mapping $[0,T]$ to U. We define the minimum hitting time $T : \mathbb{R}^n \times \mathcal{U}_m \to \mathbb{R}^+$ by

$$T(x,\mu) := \begin{cases} \infty & \text{if } \{t \mid \phi_t(x,\mu) \in \Omega_f \} = \emptyset \\ \min\{t \mid \phi_t(x,\mu) \in \Omega_f\} & \text{otherwise.} \end{cases} \tag{5.2.1}$$

$\phi_t(x,\mu)$ denotes the trajectory of $\dot{x} = f(x,\mu)$ starting from x and using control $\mu(\cdot)$.

A control $\mu \in \mathcal{U}_m$ specified on $[0,T]$ is *admissible* for $x \in \Omega$ if $\phi_t(x,\mu) \in \Omega$ for all $t \in [0,T]$. The set of admissible controls for x is denoted $\mathcal{U}_x$. Let

$$\mathcal{R} := \{\ x \in \mathbb{R}^n \mid \exists \mu \in \mathcal{U}_x.\ T(x,\mu) < \infty \ \}.$$

We consider the following optimal control problem. Given $y \in \Omega$,

$$\text{minimize} \qquad J(y,\mu) = \int_0^{T(y,\mu)} L(x(t),\mu(t))dt + h(x(T(y,\mu))) \tag{5.2.2}$$

$$\text{subject to} \qquad \dot{x} = f(x,\mu), \qquad a.e.\ t \in [0,T(y,\mu)] \tag{5.2.3}$$

$$x(0) = y \tag{5.2.4}$$

among all admissible controls $\mu \in \mathcal{U}_y$. $J : \mathbb{R}^n \times \mathcal{U}_m \to \mathbb{R}$ is the *cost-to-go* function, $h : \mathbb{R}^n \to \mathbb{R}$ is the *terminal cost*, and $L : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}$ is the *instantaneous cost*. At $T(y,\mu)$ the terminal cost $h(x(T(y,\mu)))$ is incurred and the dynamics are stopped. The control objective is to reach Ω_f from $y \in \Omega$ with minimum cost.

Assumption 2.1.

(1) $f : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ satisfies $\|f(x',u') - f(x,u)\| \le L_f\big[\|x'-x\| + \|u'-u\|\big]$ for some $L_f > 0$. Let M_f be the upper bound of $\|f(x,u)\|$ on $\Omega \times U$.

(2) $L : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}$ satisfies $|L(x',u') - L(x,u)| \le L_L\big[\|x'-x\| + \|u'-u\|\big]$ and $1 \le |L(x,u)| \le M_L$, $x \in \Omega$, $u \in U$, for some $L_L, M_L > 0$.

(3) $h : \mathbb{R}^n \to \mathbb{R}$ satisfies $|h(x') - h(x)| \le L_h\|x'-x\|$ for some $L_h > 0$, and $h(x) \ge 0$ for all $x \in \Omega$. Let M_h be the upper bound of $|h(x)|$ on Ω.

Remark 2.1. These assumptions ensure existence of solutions and continuity of the value function, defined below. Weaker assumptions are possible but since our goal is to introduce a method rather than obtain the most general setting for it, we are satisfied with these. See [14] for other possibilities.

The *value function* or optimal cost-to-go function $V : \mathbb{R}^n \to \mathbb{R}$ is given by

$$V(y) = \inf_{\mu \in \mathcal{U}_y} J(y,\mu)$$

for $y \in \Omega \setminus \Omega_f$, and by $V(y) = h(y)$ for $y \in \Omega_f$. A control μ is called *ϵ-optimal* for x if $J(x,\mu) \le V(x) + \epsilon$.

It is well-known [43] that V satisfies the *Hamilton-Jacobi-Bellman* (HJB) equation

$$-\inf_{u \in U}\left\{L(x,u) + \frac{\partial V}{\partial x} f(x,u)\right\} = 0 \tag{5.2.5}$$

at each point of $\mathcal{R}$ at which it is differentiable. The HJB equation is an infinitesimal version

of the equivalent *Dynamic Programming Principle* (DPP) which says that

$$\begin{aligned} V(x) &= \inf_{\mu\in\mathcal{U}_x}\left\{\int_0^t L(\phi_s(x,\mu),\mu(s))ds \;+\; V(\phi_t(x,\mu))\right\}, \quad x\in\Omega\setminus\Omega_f \\ V(x) &= h(x) \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad x\in\Omega_f. \end{aligned}$$

The subject of assiduous effort has been that the HJB equation may not have a C^1 solution. This gap in the theory was closed by the inception of the concept of viscosity solution [62, 35], which can be shown to provide the unique solution of (5.2.5) without any differentiability assumption. In particular, a bounded uniformly continuous function V is called a *viscosity solution* of HJB provided, for each $\psi\in C^1(\mathbb{R}^n)$, the following hold:

(i) if $V-\psi$ attains a local maximum at $x_0\in\mathbb{R}^n$, then

$$-\inf_{u\in U}\left\{L(x_0,u)+\frac{\partial\psi}{\partial x}(x_0)f(x_0,u)\right\}\le 0,$$

(ii) if $V-\psi$ attains a local minimum at $x_1\in\mathbb{R}^n$, then

$$-\inf_{u\in U}\left\{L(x_1,u)+\frac{\partial\psi}{\partial x}(x_1)f(x_1,u)\right\}\ge 0.$$

Assumption 2.2. For every $\epsilon>0$ and $x\in\mathcal{R}$, there exists $N_\epsilon>0$ and an admissible piecewise constant ϵ-optimal control μ having at most N_ϵ discontinuities and such that $\phi_t(x,\mu)$ is transverse to $\partial\Omega_f$.

The transversality assumption implies that the viscosity solution is continuous at the boundary of the target set, a result needed in proving uniform continuity of V over a finite horizon. The assumption can be replaced by a small-time controllability condition. For a treatment of small time controllability and compatibility of the terminal cost with respect to continuity of the value function, see [14]. The finite switching assumption holds under mild assumptions such as Lipschitz continuity of the vector field and cost functions, and is based on approximating measurable functions by piecewise constant functions.

5.3 Hybrid Automaton

The approach we propose for solving the continuous optimal control problem first requires a mapping to a hybrid automaton and, second, employs a bisimulation to formulate a dynamic programming problem on the quotient system. In this section we define the hybrid optimal

control problem. First, we discretize U by defining a finite set $\Sigma_\delta \subset U$ which has a mesh size

$$\delta := \sup_{u \in U} \min_{\sigma \in \Sigma_\delta} \|u - \sigma\|.$$

We define the hybrid automaton $H := (\Sigma \times \mathbb{R}^n, \Sigma_\delta, D, E_h, G, R)$. The elements are defined as in Section 2.2 with a few differences that we point out here:

State set $\Sigma \times \mathbb{R}^n$ consists of the finite set $\Sigma = \Sigma_\delta \cup \{\sigma_f\}$ of control locations and n continuous variables $x \in \mathbb{R}^n$. σ_f is a terminal location when the continuous dynamics are stopped (in the same sense that the dynamics are "stopped" in the continuous optimal control problem). Notice that the locations of the automaton are named using control event labels.

Events Σ_δ is a finite set of control event labels.

Control switches $E_h \subset \Sigma \times \Sigma$ is a set of control switches. $e = (\sigma, \sigma')$ is a directed edge between a source location σ and a target location σ'. If $E_h(\sigma)$ denotes the set of edges that can be enabled at $\sigma \in \Sigma$, then $E_h(\sigma) := \{(\sigma, \sigma') \mid \sigma' \in \Sigma \setminus \sigma\}$ for $\sigma \in \Sigma_\delta$ and $E_h(\sigma_f) = \emptyset$. Thus, from a source location not equal to σ_f, there is an edge to every other location (but not itself), while location σ_f has no outgoing edges.

5.3.1 Semantics

The semantics are the same as in Section 2.2, but we require a few additional definitions. A *hybrid control* is a finite or infinite sequence of labels $\omega = \omega_1 \omega_2 \ldots$, with $\omega_i \in \Sigma \cup \mathbb{R}^+$. $\omega_i \in \mathbb{R}^+$ is the duration of the t-step at step i. The set of hybrid controls is denoted $\mathcal{S}$. A *hybrid trajectory* π over $\omega \in \mathcal{S}$ is a finite or infinite sequence $\pi : (\sigma_0, x_0) \xrightarrow{\omega_1} (\sigma_1, x_1) \xrightarrow{\omega_2} (\sigma_2, x_2) \xrightarrow{\omega_3} \ldots$ where $(\sigma_i, x_i) \in \Sigma \times \mathbb{R}^n$. Trajectory π is *accepted* by H iff $\forall i$, $(\sigma_i, x_i) \xrightarrow{\omega_{i+1}} (\sigma_{i+1}, x_{i+1})$ is either a t-step or σ-step of H. Let π be the trajectory (not necessarily accepted by H) starting at $(\sigma, x) \in \Sigma \times \Omega$ and defined over $\omega \in \mathcal{S}$. We say ω is *admissible* for (σ, x) on interval $[0, T]$ if (1) π remains in $\Sigma \times \Omega$ for $t \in [0, T]$, and (2) corresponding to ω is a piecewise constant control $\mu_\omega(t)$ (with a finite number of discontinuities in finite time). Let $\mathcal{S}_{(\sigma,x)}$ be the set of admissible controls for (σ, x).

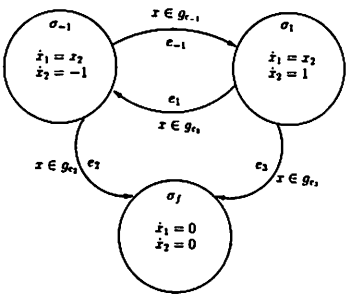

Figure 5.1: Hybrid automaton for time optimal control of a double integrator system

Example 5.3.1. Consider a time optimal control problem for

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= u. \end{aligned}$$

We select $\Omega = (-1,1) \times (-1,1)$ and $\Omega_f = \overline{B}_\epsilon(0)$, the closed epsilon ball centered at 0. The cost-to-go function is $J(x,\mu) = \int_0^{T(x,\mu)} dt$ and $U = \{u \ : \ |u| \leq 1\}$. We select $\Sigma_\delta = \{-1,1\}$, so that $\delta = 1$. The hybrid system is show in Figure 5.1. The state set is $\{\sigma_{-1} = -1, \sigma_1 = 1, \sigma_f\} \times \mathbb{R}^n$. $g_{e_{-1}}$ and g_{e_1} are unknown and must be synthesized, while $g_{e_2} = g_{e_3} = \Omega_f$.

5.3.2 Hybrid optimal synthesis

We want to synthesize enabling conditions so that for each $y \in \mathcal{R}$, the cost-to-go from y well-approximates the viscosity solution at y of HJB. This requires posing a hybrid optimal synthesis problem. We define a *hybrid cost-to-go function* $J_H : \Sigma \times \mathbb{R}^n \times \mathcal{S} \to \mathbb{R}$ as follows. For $\omega \in \mathcal{S}_{(\sigma,x)}$,

$$J_H((\sigma,x),\omega) = J(x,\mu_\omega).$$

The *hybrid value function* $V_H : \Sigma \times \mathbb{R}^n \to \mathbb{R}$ is

$$V_H((\sigma,x)) = \inf_{\omega \in \mathcal{S}_{(\sigma,x)}} J_H((\sigma,x),\omega).$$

Hybrid optimal synthesis problem:
Given H and $0 < \epsilon^1 < \epsilon^2$, synthesize g_e, $e \in E_h$, subject to:

1. $g_e = \Omega_f$ *if* $e = (\sigma,\sigma_f)$, $\sigma \in \Sigma_\delta$.

2. *For each* $e \in E_h$, $g_e \subseteq \Omega$.

3. *For all* $\omega \in \mathcal{S}$ *and* $(\sigma, x) \in \Sigma \times \Omega$ *such that* $V_H((\sigma, x)) < \infty$, $\pi_{(\sigma,x)}$ *is accepted by* H *if* ω *is admissible and* ϵ^1*-optimal for* (σ, x).

4. *For all* $\omega \in \mathcal{S}$ *and* $(\sigma, x) \in \Sigma \times \Omega$, $\pi_{(\sigma,x)}$ *is not accepted by* H *if either* ω *is not admissible for* (σ, x), ω *is not* ϵ^2*-optimal for* (σ, x), *or* $V_H((\sigma, x)) = \infty$.

Remark 3.1. Condition 1 says that the enabling condition for edges going to the final location is Ω_f. Condition 2 corresponds to trajectories remaining in Ω. Conditions 3 and 4 say the hybrid automaton "does the right thing".

5.4 Quotienting by the bisimulation

We propose to solve the hybrid optimal control problem using the bisimulation of H. In this section we define some parameters of this process, assuming that the bisimulation $\simeq$ is available using the method of Chapter 3.

First, since the dynamics are restricted to the set Ω, the set of interesting equivalence classes of $\simeq$, denoted Q, are those that intersect $\Sigma_\delta \times cl(\Omega)$. For each $q \in Q$ we define a distinguished point $(\sigma, \xi) \in q$. We associate q with its distinguished point by the notation $q = [(\sigma, \xi)]$. It is now possible to define the enabling and reset conditions of H in terms of Q. In particular, the enabling conditions of H are synthesized as subsets of Q while the reset conditions are defined as follows. For $e = (\sigma, \sigma')$

$$r_e(x) = \{\ y \mid \exists \xi.[(\sigma, x)] = [(\sigma, \xi)] \wedge [(\sigma', \xi)] = [(\sigma', y)]\ \}. \tag{5.4.1}$$

That is, $r_e(x)$ is the projection to $\mathbb{R}^n$ of the set of equivalence classes $[(\sigma', y)]$ such that the projection to $\mathbb{R}^n$ of $[(\sigma', y)]$ and $[(\sigma, x)]$ have nonempty intersection. This definition in effect gives an over-approximation of the identity map in terms of the equivalence classes of $\simeq$ and will introduce non-determinacy in the finite automaton. Notice also that (5.4.1) encodes information about the bisimulation in H. This sequence of steps is not typical; it is characteristic of our synthesis procedure. We define a mesh size on Q by

$$\delta_Q = \max_{q \in Q} \sup_{(\sigma,x),(\sigma,y) \in q} \{\|x - y\|\}.$$

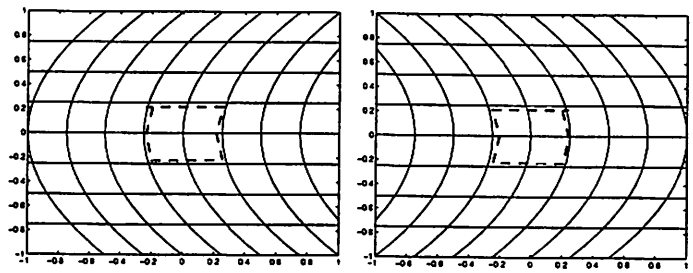

Figure 5.2: Partitions for states σ_1 and σ_{-1} of the hybrid automaton of Figure 5.1

Finally, for each $q = [(\sigma, \xi)] \in Q$ we associate the duration τ_q, the maximum time to traverse q using constant control σ. That is,

$$\tau_q = \sup_{(\sigma,x),(\sigma,y)\in q} \{\, t \mid y = \phi_t(x,\sigma) \,\}.$$

Example 5.4.1. Continuing example 5.3.1, a first integral for vector field $\dot{x}_1 = x_2$, $\dot{x}_2 = 1$ is $x_1 - \frac{1}{2}x_2^2 = c_1$, $c_1 \in \mathbb{R}$. For $\dot{x}_1 = x_2$, $\dot{x}_2 = -1$ a first integral is $x_1 + \frac{1}{2}x_2^2 = c_2$, $c_2 \in \mathbb{R}$. We select a transverse foliation for each vector field, given by $x_2 = c_3$. A possible set of partitions for locations σ_1 and σ_{-1} and $\Omega = (-1,1) \times (-1,1)$ are shown in Figure 5.2. The equivalence classes of $\simeq$ are pairs consisting of a control label in Σ_δ and the interiors of regions, open line segments and curves forming the boundaries of two regions, and the points at the corners of regions. $\tau = 0$ for the segments transverse to the flow and the corner points. $\tau = \Delta$ for the interiors of regions and segments tangential to the flow, where $\Delta = .25$ in Figure 5.2.

5.5 Discrete problem

In this section we transform the hybrid optimal control problem to a dynamic programming problem on a non-deterministic finite automaton, for which an algorithmic solution may be found. Consider the class of non-deterministic automata with cost structure represented by the tuple

$$A = (Q, \Sigma_\delta, E, obs, Q_f, \hat{L}, \hat{h}).$$

Q is the state set, as above, and Σ_δ is the set of control labels as before. $obs : E \to \Sigma_\delta$ is a map that assigns a control label to each edge and is given by $obs(e) = \sigma'$, where $e = (q, q')$, $q = [(\sigma, \xi)]$ and $q' = [(\sigma', \xi')]$. Q_f is the target set given by the over-approximation of Ω_f,

$$Q_f = \{q \in Q \mid \exists x \in \Omega_f \,.\, (\sigma, x) \in q \,\}. \tag{5.5.1}$$

$E \subseteq Q \times Q$ is the transition relation encoding t-steps and σ-steps of H. A will be used to synthesize g_e of H, so, in the spirit of [83], E includes all possible edges between locations. The synthesis procedure on A will involve trimming undesirable edges. Thus, $(q, q') \in E$, where $q, q' \in Q$, $q = [(\sigma, \xi)]$ and $q' = [(\sigma', \xi')]$ if either (a) $\sigma = \sigma'$, there exists $x \in \Omega$ such that $(\sigma, x) \in q$, and there exists $\tau > 0$ such that $\forall t \in [0, \tau]$, $(\sigma, \phi_t(x, \sigma)) \in q$ and $(\sigma, \phi_{\tau+\epsilon}(x, \sigma)) \in q'$ for arbitrarily small $\epsilon > 0$, or (b) $\sigma = \sigma'$, there exists $x \in \Omega$ such that $(\sigma, x) \in q$, and there exists $\tau > 0$ such that $\forall t \in [0, \tau)$, $(\sigma, \phi_t(x, \sigma)) \in q$ and $(\sigma, \phi_\tau(x, \sigma)) \in q'$, or (c) $\sigma \neq \sigma'$ and there exists $x \in \Omega$ such that $(\sigma, x) \in q$ and $(\sigma', x) \in q'$. Cases (a) and (b) say that from a point in q, q' is the first state (different from q) reached after following the flow of $f(x, \sigma)$ for some time. Case (c) says that an edge exists between q and q' if their projections to $\mathbb{R}^n$ have non-empty intersection.

Let $e = (q, q')$ with $q = [(\sigma, \xi)]$ and $q' = [(\sigma', \xi')]$. $\hat{L} : E \to \mathbb{R}$ is the *discrete instantaneous cost* given by

$$\hat{L}(e) := \begin{cases} \tau_q L(\xi, \sigma) & \text{if } \sigma = \sigma' \\ 0 & \text{if } \sigma \neq \sigma'. \end{cases} \tag{5.5.2}$$

This definition reflects that no cost is incurred for control switches. $\hat{h} : Q \to \mathbb{R}$ is the *discrete terminal cost* given by

$$\hat{h}(q) := h(\xi).$$

The domain of $\hat{h}$ can be extended to Ω, with a slight abuse of notation, by

$$\hat{h}(x) := \hat{h}(q) \tag{5.5.3}$$

where $q = \arg\min_{q'} \{\|x - \xi'\| \mid q' = [(\sigma', \xi')]\}$.

5.5.1 Semantics

A transition or *step* of A from $q = [(\sigma, \xi)] \in Q$ to $q' = [(\sigma', \xi')] \in Q$ with observation $\sigma' \in \Sigma_\delta$ is denoted $q \xrightarrow{\sigma'} q'$. If $\sigma \neq \sigma'$ the transition is referred to as a *control switch*; otherwise, it is

referred to as a *time step*. If $E(q)$ is the set of edges that can be enabled from $q \in Q$, then for $\sigma \in \Sigma_\delta$,

$$E_\sigma(q) = \{e \in E(q) \mid obs(e) = \sigma\}.$$

If $|E_\sigma(q)| > 1$, then we say that $e \in E_\sigma(q)$ is *unobservable* in the sense that when control event σ is issued, it is unknown which edge among $E_\sigma(q)$ is taken. If $\sigma = \sigma'$, then $|E_\sigma(q)| = 1$, by the uniqueness of solutions of ODE's and by the definition of bisimulation.

A *control policy* $c : Q \to \Sigma_\delta$ is a map assigning a control event to each state; $c(q) = \sigma$ is the control event issued when the state is at q. A *trajectory* π of A over c is a sequence $\pi = q_0 \overset{\sigma_1}{\to} q_1 \overset{\sigma_2}{\to} q_2 \overset{\sigma_3}{\to} \ldots$, $q_i \in Q$. A trajectory is *non-Zeno* if between any two non-zero duration time steps there are a finite number of control switches and zero duration time steps. Let $\Pi_c(q)$ be the set of trajectories starting at q and applying control policy c, and let $\tilde{\Pi}_c(q)$ be the set of trajectories starting at q, applying control policy c, and eventually reaching Q_f. If for every $q \in Q$, $\pi \in \Pi_c(q)$ is non-Zeno then we say c is an *admissible control policy*. The set of all admissible control policies for A is denoted $\mathcal{C}$.

A control policy c is said to have a *loop* if A has a trajectory $q_0 \overset{c(q_0)}{\to} q_1 \overset{c(q_1)}{\to} \ldots \overset{c(q_{m-1})}{\to} q_m = q_0$, $q_i \in Q$. A control policy has a *Zeno loop* if it has a loop made up of control switches and/or zero duration time steps (i.e. $\tau_q = 0$) only.

Lemma 5.5.1. *A control policy c for non-deterministic automaton A is admissible if and only if it has no Zeno loops.*

Proof. First we show that a non-deterministic automaton with non-Zeno trajectories has a control policy without Zeno loops. For suppose not. Then a trajectory starting on a state belonging to the loop can take infinitely many steps around the loop before taking a non-zero duration time step. This trajectory is not non-Zeno, a contradiction. Second, we show that a control policy without Zeno loops implies non-Zeno trajectories. Suppose not. Consider a Zeno trajectory that takes an infinite number of control switches and/or zero duration time steps between two non-zero duration time steps. Because there are a finite number of states in Q, by the Axiom of Choice, one of the states must be repeated in the sequence of states visited during the control switches and/or zero duration time steps. This implies the existence of a loop in the control policy. By the construction of the bisimulation partition a trajectory spends zero time in a state q iff $\tau_q = 0$. This implies a Zeno loop, a contradiction. □

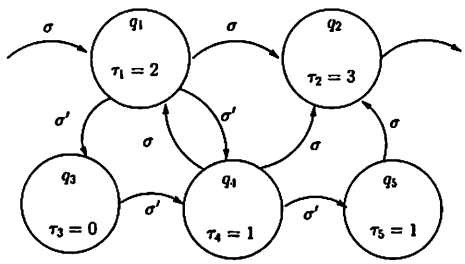

Figure 5.3: Fragment of automaton with a zero duration time step.

Example 5.5.1. Consider the automaton in Figure 5.3. If we are at q_1 and the control $\sigma'\sigma'\sigma$ is issued, then three possible trajectories are $q_1 \xrightarrow{\sigma'} q_3 \xrightarrow{\sigma'} q_4 \xrightarrow{\sigma} q_2$, $q_1 \xrightarrow{\sigma'} q_4 \xrightarrow{\sigma'} q_5 \xrightarrow{\sigma} q_2$, or $q_1 \xrightarrow{\sigma'} q_3 \xrightarrow{\sigma'} q_4 \xrightarrow{\sigma} q_1$. The first trajectory has a zero duration time step. The control is inadmissible since the last trajectory has a Zeno loop.

5.5.2 Dynamic programming

In this section we formulate the dynamic programming problem on A. This involves defining a cost-to-go function and a value function that minimizes it over control policies suitable for non-deterministic automata.

Let $\pi = q_0 \xrightarrow{\sigma_1} q_1 \to \ldots \to q_{N-1} \xrightarrow{\sigma_N} q_N$, where $q_i = [(\sigma_i, \xi_i)]$ and π takes the sequence of edges $e_1 e_2 \ldots e_N$. We define a *discrete cost-to-go* $\hat{J} : Q \times C \to \mathbb{R}$ by

$$\hat{J}(q,c) = \begin{cases} \max_{\pi \in \tilde{\Pi}_c(q)} \left\{ \sum_{j=1}^{N_\pi} \hat{L}(e_j) + \hat{h}(q_{N_\pi}) \right\} & \text{if } \Pi_c(q) = \tilde{\Pi}_c(q) \\ \infty & \text{otherwise} \end{cases}$$

where $N_\pi = \min\{j \geq 0 \mid q_j \in Q_f\}$. We take the maximum over $\tilde{\Pi}_c(q)$ because of the non-determinacy of A: it is uncertain which among the (multiple) trajectories allowed by c will be taken so we must assume the worst-case situation. The *discrete value function* $\hat{V} : Q \to \mathbb{R}$ is

$$\hat{V}(q) = \min_{c \in C} \hat{J}(q,c)$$

for $q \in Q \setminus Q_f$ and $\hat{V}(q) = \hat{h}(q)$ for $q \in Q_f$. We show in Proposition 5.5.2 that $\hat{V}$ satisfies a DPP that takes into account the non-determinacy of A and ensures that optimal control policies are admissible. This DPP describes the accumulation of cost over one step to be

the worst case cost among edges that have the same label. Let $\mathcal{A}_q$ be the set of control assignments $c(q) \in \Sigma_\delta$ at q such that c is admissible.

Proposition 5.5.2. *$\hat{V}$ satisfies*

$$\hat{V}(q) = \min_{c(q)\in\mathcal{A}_q} \Big\{ \max_{e=(q,q')\in E_{c(q)}(q)} \{\hat{L}(e) + \hat{V}(q')\} \Big\}, \quad q \in Q \setminus Q_f \tag{5.5.4}$$

$$\hat{V}(q) = \hat{h}(q), \quad q \in Q_f. \tag{5.5.5}$$

Proof. Fix $q \in Q$. By definition of $\hat{J}$

$$\hat{J}(q,c) = \max_{e=(q,q')\in E_{c(q)}(q)} \{\hat{L}(e) + \hat{J}(q',c)\}. \tag{5.5.6}$$

By definition of $\hat{V}$

$$\hat{J}(q,c) \geq \max_{e=(q,q')\in E_{c(q)}(q)} \{\hat{L}(e) + \hat{V}(q')\}.$$

Since $c(q) \in \mathcal{A}_q$ is arbitrary

$$\hat{V}(q) \geq \min_{c(q)\in\mathcal{A}_q} \Big\{ \max_{e=(q,q')\in E_{c(q)}(q)} \{\hat{L}(e) + \hat{V}(q')\} \Big\}.$$

To prove the reverse inequality suppose, by way of contradiction, there exists $\sigma' \in \Sigma_\delta$ such that

$$\hat{V}(q) > \max_{e=(q,q')\in E_{\sigma'}(q)} \{\hat{L}(e) + \hat{V}(q')\} := \hat{L}(e) + \hat{V}(\overline{q}). \tag{5.5.7}$$

Suppose the optimal admissible policy for $\overline{q}$ is $\overline{c}$. Define $c = \overline{c}$ on $Q \setminus \{q\}$ and $c(q) = \sigma'$. Then $\hat{J}(q,c) = \hat{L}(e) + \hat{V}(\overline{q}) < \hat{V}(q)$. This gives rise to a contradiction if we can show c is admissible. Suppose not. Then there exists a loop of control switches and zero duration time steps containing q and $\overline{q}$, implying $\hat{V}(\overline{q}) \geq \hat{V}(q)$, which contradicts hypothesis (5.5.7).

□ □

Remark 5.1. The DPP for $\hat{V}$ is a prescription for synthesizing admissible control policies, but we have not indicated how, in practice, this can be achieved. One possibility is to introduce a fictitious switching cost in the formulation of $\hat{V}$. Capuzzo-Dolcetta and Evans [27] introduce a small switching cost which tends to zero as $\delta \to 0$. Alternatively, admissible controls can be obtained through a device introduced in implementation. For example, a counter of the number of switches could be used or we may select an algorithmic solution which is guaranteed not to generate Zeno controls.

5.5.3 Synthesis of enabling conditions

The synthesis of enabling conditions or *controller synthesis* is typically a post-processing step of a backward reachability analysis (see, for example, [103]). This situation prevails here as well: equations (5.5.4)-(5.5.5) describe a backward analysis to construct an optimal policy $c \in \mathcal{C}$. Once c is known the enabling conditions of H are extracted as follows.

Consider each $e = (\sigma, \sigma') \in E$ of H with $\sigma \neq \sigma'$. There are two cases. If $\sigma' \neq \sigma_f$ then $g_e = \{x \mid (\sigma, x) \in q, q \in Q \ \wedge \ c(q) = \sigma'\}$. That is, if the control policy designates switching from $q \in Q$ with label σ to $q' \in Q$ with label σ', then the corresponding enabling condition in H includes the projection to $\mathbb{R}^n$ of q. The second case when $\sigma' = \sigma_f$ is for edges going to the terminal location of H. Then $g_e = \{x \mid (\sigma, x) \in q, q \in Q_f\}$.

5.6 Main Result

We will prove that $\hat{V}$ converges to V, the viscosity solution of the HJB equation, as $\delta_Q, \delta \to 0$. The proof will be carried out in three steps. In the first step we consider restricting the set of controls to piecewise constant functions, whose constant intervals are a function of the state. In the second step we introduce the discrete approximations of L and h. In the last step we introduce the discrete states Q and consider the non-determinacy of A.

In the sequel we make use of a filtration of control sets $\Sigma_k \equiv \Sigma_{\delta_k}$ corresponding to a sequence $\delta_k \to 0$ as $k \to \infty$, in such a manner that $\Sigma_k \subset \Sigma_{k+1}$. Considering (3.2.3), we define a filtration of families of submanifolds such that $\mathcal{W}_k^\sigma \subset \mathcal{W}_{k+1}^\sigma$, for each $\sigma \in \Sigma_k$.

Step 1: piecewise constant controls.

In the first step we define a class of piecewise constant functions that depend on the state and show that the value function which minimizes the cost-to-go over this class converges to the viscosity solution of HJB as $\delta_k \to 0$. The techniques of this step are based on those in Bardi and Capuzzo-Dolcetta [14] and are related to those in [27].

We consider the optimal control problem (5.2.2)-(5.2.4) when the set of admissible controls is $\mathcal{U}_k^1$, piecewise constant functions consisting of finite sequences of control labels $\sigma \in \Sigma_k$ and each σ is applied for a time $\tau(\sigma, x)$. Let $(\sigma, x) \in q$ for some $q \in Q$ and define $\tau(\sigma, x)$ to be the minimum of the time it takes the trajectory starting at x and using control $\sigma \in \Sigma_k$ to reach (ta) $\partial\Omega_f$, and (tb) some x' such that $(\sigma, x') \notin q$. If a trajectory is at x_i at the

start of the $(i+1)$th step, then the control σ_{i+1} is applied for time $\tau_{i+1} := \tau(\sigma_{i+1}, x_i)$ and $x_{i+1} = \phi_{\tau_{i+1}}(x_i, \sigma_{i+1})$.

Let

$$\mathcal{R}_k^1 := \{\, x \in \mathbb{R}^n \mid \exists \mu \in \mathcal{U}_k^1 \,.\, T(x,\mu) < \infty \,\}.$$

We define the cost-to-go function $J_k^1 : \Omega \times \mathcal{U}_k^1 \to \mathbb{R}$ as follows. For $x \in \Omega$ and $\mu = \sigma_1\sigma_2\ldots \in \mathcal{U}_k^1$, if $T(x,\mu) < \infty$ then

$$J_k^1(x,\mu) = \sum_{j=1}^{N} \int_0^{\tau(\sigma_j, x_{j-1})} L(\phi_s(x_{j-1},\sigma_j),\sigma_j)ds + h(x_N)$$

where $N = \min\{j \geq 0 \mid x_j \in \partial\Omega_f\}$. $J_k^1(x,\mu) = \infty$, otherwise. We define the value function $V_k^1 : \mathbb{R}^n \to \mathbb{R}$ as follows. For $x \in \Omega \setminus \Omega_f$,

$$V_k^1(x) = \inf_{\mu \in \mathcal{U}_k^1} J_k^1(x,\mu) \tag{5.6.1}$$

and for $x \in \Omega_f$, $V_k^1(x) = h(x)$.

Proposition 5.6.1. *V_k^1 satisfies, for all $x \in \mathcal{R}_k^1$,*

$$V_k^1(x) = \min_{\sigma \in \Sigma_k} \left\{ \int_0^{\tau(\sigma,x)} L(\phi_s(x,\sigma),\sigma)ds + V_k^1(\phi_{\tau(\sigma,x)}(x,\sigma)) \right\}. \tag{5.6.2}$$

Proof. Fix $x \in \mathcal{R}_k^1$ and $\mu = \sigma\sigma_1\sigma_2\ldots \in \mathcal{U}_k^1$. Using the semigroup property of flows and the definition of J_k^1

$$J_k^1(x,\mu) = \int_0^{\tau(\sigma,x)} L(\phi_s(x,\sigma),\sigma)ds + J_k^1(\phi_{\tau(\sigma,x)}(x,\sigma),\overline{\mu}) \tag{5.6.3}$$

where $\overline{\mu} = \sigma_1\sigma_2\ldots \in \mathcal{U}_k^1$. By definition of V_k^1

$$J_k^1(x,\mu) \geq \int_0^{\tau(\sigma,x)} L(\phi_s(x,\sigma),\sigma)ds + V_k^1(\phi_{\tau(\sigma,x)}(x,\sigma)).$$

Hence,

$$V_k^1(x) \geq \min_{\sigma \in \Sigma_k} \left\{ \int_0^{\tau(\sigma,x)} L(\phi_s(x,\sigma),\sigma)ds + V_k^1(\phi_{\tau(\sigma,x)}(x,\sigma)) \right\}.$$

To prove the reverse inequality fix $\sigma \in \Sigma_k$, set $z = \phi_{\tau(\sigma,x)}(x,\sigma)$, and fix $\epsilon > 0$ and $\mu_z \in \mathcal{U}_k^1$ such that

$$V_k^1(z) \geq J_k^1(z,\mu_z) - \epsilon.$$

Define the control

$$\overline{\mu}(s) = \begin{cases} \sigma & s \leq \tau(\sigma, x) \\ \mu_z(s-t) & s > \tau(\sigma, x). \end{cases}$$

Then

$$\begin{aligned} V_k^1(x) \leq J_k^1(x, \overline{\mu}) &= \int_0^{\tau(\sigma,x)} L(\phi_s(x,\sigma),\sigma)ds + J_k^1(z, \mu_z) \\ &\leq \int_0^{\tau(\sigma,x)} L(\phi_s(x,\sigma),\sigma)ds + V_k^1(z) + \epsilon. \end{aligned}$$

Since $\sigma \in \Sigma_k$ and $\epsilon > 0$ are arbitrary

$$V_k^1(x) \leq \min_{\sigma \in \Sigma_k} \left\{ \int_0^{\tau(\sigma,x)} L(\phi_s(x,\sigma),\sigma)ds + V_k^1(\phi_{\tau(\sigma,x)}(x,\sigma)) \right\}.$$

□ □

We would like to show that V_k^1 is uniformly bounded and locally uniformly continuous. Considering uniform continuity of V_k^1, let C_k be as in (3.2.2) and γ_n^σ the transversal foliation of $\dot{x} = f(x, \sigma)$. For each $\sigma \in \Sigma_k$ we define the regions in $\mathbb{R}^n$

$$\begin{aligned} M_c^\sigma &:= \{\, x \in (\gamma_n^\sigma)^{-1}(c) \mid c \in C_k \,\} \\ M_{c-}^\sigma &:= \{\, x \in (\gamma_n^\sigma)^{-1}((-1,c)) \mid c \in C_k \,\}. \end{aligned}$$

Remark 6.1.

(a) Let $x \in \mathcal{R}_k^1$ and $\mu = \sigma_1\sigma_2 \ldots \in \mathcal{U}_k^1$. Suppose that $x_{j-1} \in M_c^{\sigma_j}$ for some $c \in C_k$ so that $\tau_j = 0$ and $\sigma_{j+1} \neq \sigma_j$. Let $\tilde{\mu} = \ldots\sigma_{j-1}\sigma_{j+1}\ldots$. Then $J(x,\mu) = J(x,\tilde{\mu})$. Therefore, whenever we construct an ϵ-optimal control for x we may assume that if $\tau_j = 0$ then $\sigma_{j+1} = \sigma_j$.

(b) If $x, y \in M_{c-}^\sigma$ for some $c \in C_k$ and $\tau(\sigma, x)$ and $\tau(\sigma, y)$ are defined using (tb) then $|\tau(\sigma,x) - \tau(\sigma,y)| \to 0$ and $\|\phi_{\tau(\sigma,x)}(x,\sigma) - \phi_{\tau(\sigma,y)}(y,\sigma)\| \to 0$ as $\|x - y\| \to 0$ in M_{c-}^σ, since M_c^σ is a smooth submanifold. For the details, see Theorem 6.1, p. 91-94, [43]. If instead $\tau(\sigma, x)$ and $\tau(\sigma, y)$ are defined using (ta) and σ is an ϵ-optimal control for x, then by Assumption 2.2 the same results hold.

(c) For each $x \in \cup_k \mathcal{R}_k^1$ and $\epsilon > 0$ there exists $m \in \mathbb{Z}^+$ and $\mu \in \mathcal{U}_m^1$ such that μ is an ϵ-optimal control for x w.r.t. V^1 satisfying Assumptions 2.2. This follows from Assumptions 2.2, $V_k^1(x) \geq V(x)$, and the fact that we can well-approximate an ϵ-optimal control for V by a control in $\mathcal{U}_m^1$, for large enough m.

Lemma 5.6.2. *For each $y \in \cup_k \mathcal{R}_k^1$ and $\epsilon > 0$, there exists $m_\epsilon \in \mathbb{Z}^+$ and $\eta_\epsilon > 0$ such that*

$$|V_k^1(x) - V_k^1(y)| < 2\epsilon$$

for all $|x - y| < \eta_\epsilon$ and $k > m_\epsilon$.

Proof. Fix $y \in \cup_k \mathcal{R}_k^1$. By Remark 6.1(c) there exists $m_1 > 0$ and $\mu \in \mathcal{U}_{m_1}^1$ such that μ is an ϵ-optimal control for y satisfying Assumptions 2.2. Let $x \in \mathcal{R}_{m_1}^1$. Then $V_k^1(x) - V_k^1(y) \leq J_k^1(x, \mu_x) - J_k^1(y, \mu) + \epsilon$ for any $\mu_x \in \mathcal{U}_{m_1}^1$ and $k > m_1$. If we can show that for fixed y and μ there exists $\mu_x \in \mathcal{U}_{m_1}^1$ such that

$$J_k^1(x, \mu_x) - J_k^1(y, \mu) < \epsilon \tag{5.6.4}$$

for all $x \in \mathcal{R}_{m_1}^1$ sufficiently close to y, then $V_k^1(x) - V_k^1(y) \leq 2\epsilon$ for all $k \geq m_1$.

Conversely, by Remark 6.1(c) there exists $m_2 > 0$ and $\mu_x \in \mathcal{U}_{m_2}^1$ such that μ_x is an ϵ-optimal control for x satisfying Assumptions 2.2. Then $V_k^1(y) - V_k^1(x) \leq J_k^1(y, \mu) - J_k^1(x, \mu_x) + \epsilon$ for any $\mu \in \mathcal{U}_{m_2}^1$ and $k > m_2$. If we can show that for fixed y there exists $\mu \in \mathcal{U}_{m_2}^1$ such that

$$J_k^1(y, \mu) - J_k^1(x, \mu_x) < \epsilon \tag{5.6.5}$$

for all $x \in \mathcal{R}_{m_2}^1$ sufficiently close to y, then $V_k^1(x) - V_k^1(y) \geq -2\epsilon$ for all $k \geq m_2$. The result follows by letting $m_\epsilon = \min\{m_1, m_2\}$. Thus, we must show (5.6.4) and (5.6.5).

Consider first (5.6.4). Let $\overline{\mu} = \overline{\sigma}_1 \overline{\sigma}_2 \ldots \in \mathcal{U}_k^1$ be an ϵ-optimal control for y such that $y_N \in \partial\Omega_f$ and Remark 6.1(a) holds. By redefining indices, we can associate with $\overline{\mu}$ the open-loop control $\tilde{\mu} = (\sigma_1, \tilde{\tau}_1)(\sigma_2, \tilde{\tau}_2) \ldots$, where τ_i is the time σ_i is applied. We claim there exists $\tilde{\mu}^x = (\sigma_1, \tilde{\tau}_1^x)(\sigma_2, \tilde{\tau}_2^x) \ldots$ such that as $x \to y$, (a) $x_j \to y_j$, (b) $\tilde{\tau}_j^x \to \tilde{\tau}_j$, and (c)

$x_N \in \partial\Omega_f$. Then we have

$$\begin{aligned} J_k^1(x,\tilde{\mu}^x) - J_k^1(y,\tilde{\mu}) &\leq \sum_{j=1}^{N} \int_0^{\tilde{\tau}_j} |L(\phi_s(x_{j-1},\sigma_j),\sigma_j) - L(\phi_s(y_{j-1},\sigma_j),\sigma_j)| ds \\ &\quad + \sum_{j=1}^{N} \Big| \int_{\tilde{\tau}_j}^{\tilde{\tau}_j^x} L(\phi_s(x_{j-1},\sigma_j),\sigma_j) ds \Big| + |h(y_N) - h(x_N)| \\ &\leq L_L T_K \exp(L_f T_K) \sum_{j=1}^{N} \|x_{j-1} - y_{j-1}\| \\ &\quad + M_L \sum_{j=1}^{N} |\tilde{\tau}_j^x - \tilde{\tau}_j| + L_h |x_N - y_N|. \end{aligned}$$

By the claim the r.h.s. can be made less than ϵ. Thus, we need only show there exists $\tilde{\mu}^x = (\sigma_1, \tilde{\tau}_1^x)(\sigma_2, \tilde{\tau}_2^x)\ldots$ which satisfies the claim and $\mu^x \in \mathcal{U}_k^1$ can be reconstructed from it, based on the discrete states in Q visited by $\phi_t(x, \tilde{\mu}^x)$. We argue by induction. Suppose (a)-(c) hold at $j-1$. We show they hold at j. By Remark 6.1(a) we need only consider the case when $y_{j-1} \in M_{c-}^{\sigma_j}$ and $y_j \in M_c^{\sigma_j}$ for some $c \in C_k$. For x_{j-1} sufficiently close to y_{j-1} $x_{j-1} \in M_{c-}^{\sigma_j}$. By Remark 6.1(b) there exists $\tilde{\tau}_j^x$ such that $x_j = \phi_{\tilde{\tau}_j^x}(x_{j-1}, \sigma_j) \in M_c^{\sigma}$ and $\tilde{\tau}_j^x \to \tilde{\tau}_j$ and $x_j \to y_j$ as $x_{j-1} \to y_{j-1}$. The case $y_{j-1} \in M_{c-}^{\sigma_j}$ and $y_j \in \partial\Omega_f$ follows in the same way from Remark 6.1(a) and Assumption 2.2. Proving (5.6.5) follows along the same lines as the proof for (5.6.4). □ □

To show boundedness of V_k^1, let

$$T(x) := \inf_{\mu \in \mathcal{U}_k^1} T(x,\mu).$$

In light of Assumption 2.1(2), we have that for all $x \in \mathbb{R}^n$, $|V_k^1(x)| \leq T(x) \cdot M_L + M_h$. Consider the set

$$K_a := \{x \in \mathcal{R}_k^1 \mid T(x) < a\}.$$

Then $|V_k^1(x)| \leq a \cdot M_L + M_h$, $\forall x \in K_a$.

We have shown that on each $K_a \subseteq \mathbb{R}^n$, $\{V_k^1\}$ forms a family of equibounded, locally equicontinuous functions. It follows by Arzela-Ascoli Theorem that along some subsequence k_n, $V_{k_n}^1$ converges to a continuous function V_*.

Proposition 5.6.3. *V_* is the unique viscosity solution of HJB.*

Proof. We show that V_* solves HJB in the viscosity sense. Let $\psi \in C^1(\mathbb{R}^n)$ and suppose $x_0 \in \Omega$ is a strict local maximum for $V_* - \psi$. There exists a closed ball B centered at x_0 such that $(V_* - \psi)(x_0) > (V_* - \psi)(x)$, for all $x \in B$. Let $x_{0\delta_k}$ be a maximum point for $V_k^1 - \psi$ over B. Since $V_k^1 \to V_*$ locally uniformly it follows that $x_{0\delta_k} \to x_0$ as $\delta_k \to 0$. Then, for any $\sigma \in \Sigma_k$, the point $\phi_\tau(x_{0\delta_k}, \sigma)$ is in B (using boundedness of f), for sufficiently small δ_k and $0 \leq \tau \leq \tau(x_{0\delta_k}, \sigma)$, since $\tau(x_{0\delta_k}, \sigma) \to 0$ as $\delta_k \to 0$. Therefore,

$$V_k^1(x_{0\delta_k}) - \psi(x_{0\delta_k}) \geq V_k^1(\phi_\tau(x_{0\delta_k}, \sigma)) - \psi(\phi_\tau(x_{0\delta_k}, \sigma)).$$

Considering Equation 5.6.2, we have

$$\begin{aligned} 0 &= -\min_{\sigma \in \Sigma_k} \left\{ V_k^1(\phi_\tau(x_{0\delta_k}, \sigma)) - V_k^1(x_{0\delta_k}) + \int_0^\tau L(\phi_s(x_{0\delta_k}, \sigma), \sigma) ds \right\} \\ &\geq -\min_{\sigma \in \Sigma_k} \left\{ \psi(\phi_\tau(x_{0\delta_k}, \sigma)) - \psi(x_{0\delta_k}) + \int_0^\tau L(\phi_s(x_{0\delta_k}, \sigma), \sigma) ds \right\}. \end{aligned}$$

Since $\psi \in C^1(\mathbb{R}^n)$, we have by the Mean Value Theorem,

$$0 \geq -\min_{\sigma \in \Sigma_k} \left\{ \frac{\partial \psi}{\partial x}(y) \cdot \int_0^\tau f(\phi_s(x_{0\delta_k}, \sigma), \sigma) ds + \int_0^\tau L(\phi_s(x_{0\delta_k}, \sigma), \sigma) ds \right\}$$

where $y = \alpha x_{0\delta_k} + (1 - \alpha)\phi_\tau(x_{0\delta_k}, \sigma)$ for some $\alpha \in [0, 1]$. Dividing by $\tau > 0$ on each side and taking the limit as $\delta_k \to 0$, we have $V_k^1 \to V_*$, $x_{0\delta_k} \to x_0$, $\tau \to 0$, and $y \to x_{0\delta_k}$. By the Fundamental Theorem of Calculus, the continuity of f and L, and the uniform continuity in u of the expression in brackets, we obtain

$$0 \geq -\inf_{u \in U} \left\{ \frac{\partial \psi}{\partial x}(x_0) \cdot f(x_0, u) + L(x_0, u) \right\}.$$

This confirms part (i) of the viscosity solution definition. Part (ii) is proved in an analogous manner. □ □

Step 2: approximate cost functions.

In this step we keep the semantics on piecewise constant controls of Step 1 but replace cost functions L and h by approximations L^2 and $\hat{h}$. We define the cost-to-go function $J_k^2 : \Omega \times \mathcal{U}_k^1 \to \mathbb{R}$ as follows. First, we define an approximate instantaneous cost $L^2 : \Omega \times \Sigma_k \to \mathbb{R}$ given by

$$L^2(x, \sigma) := \hat{L}(q) \tag{5.6.6}$$

where $(\sigma, x) \in q$. For $x \in \Omega$ and $\mu = \sigma_1\sigma_2 \ldots \in \mathcal{U}_k^1$, if $T(x,\mu) < \infty$ then

$$J_k^2(x,\mu) = \sum_{j=1}^{N} L^2(x_{j-1}, \sigma_j) + \hat{h}(x_N)$$

where $N = \min\{j \geq 0 \mid x_j \in \partial\Omega_f\}$.

We define a value function $V_k^2 : \mathbb{R}^n \to \mathbb{R}$ as follows. For $x \in \Omega \setminus \Omega_f$,

$$V_k^2(x) = \inf_{\mu \in \mathcal{U}_k^1} J_k^2(x,\mu) \tag{5.6.7}$$

and for $x \in \Omega_f$, $V_k^2(x) = \hat{h}(x)$. For $x \in \Omega$ such that $V_k^2(x) < \infty$, V_k^2 satisfies the DPP

$$V_k^2(x) = \min_{\sigma \in \Sigma_k} \{L^2(x,\sigma) + V_k^2(\phi_{\tau(\sigma,x)}(x,\sigma))\}.$$

The proof is along the same lines as that of Proposition 5.5.2.

The following facts are useful for the subsequent result.

Fact 1. *If $\delta_k < \frac{m_f}{L_f}$, then for all $q \in Q$,*

$$\tau_q \leq \frac{\delta_k}{m_f - L_f\delta_k}. \tag{5.6.8}$$

Proof. Let $q \in Q$. Fix $x \in \Omega$ and $\sigma \in \Sigma_k$ such that $(\sigma, x) \in q$ and $\|\phi_{\tau_q} - x\| \leq \delta_k$. We have

$$\begin{aligned}
\delta_k \geq \|\phi_{\tau_q} - x\| &= \left\| \int_0^{\tau_q} f(\phi_s(x,\sigma),\sigma) ds \right\| \\
&\geq \left\| \int_0^{\tau_q} f(x,\sigma) ds \right\| - \left\| \int_0^{\tau_q} [f(\phi_s(x,\sigma),\sigma) - f(x,\sigma)] ds \right\| \\
&\geq \tau_q \|f(x,\sigma)\| - \tau_q L_f \delta_k.
\end{aligned}$$

Therefore,

$$\tau_q \leq \frac{\delta_k}{\|f(x,\sigma)\| - L_f\delta_k}.$$

Using Assumption 4.1(2) the result follows. □ □

Fact 2. *Let $x, x' \in M_c^\sigma$ for some $c \in C_k$ and $\sigma \in \Sigma_k$ such that $\|x - x'\| \leq \delta_k$. Let τ, τ' be times such that $\phi_\tau(x,\sigma), \phi_{\tau'}(x',\sigma) \in M_{c+\Delta}^\sigma$. Then $|\tau - \tau'| \leq c_\gamma \tau \delta_k$ for some $c_\gamma > 0$.*

Proof. We have

$$\int_0^\tau \frac{d}{ds}(\gamma_n^\sigma(\phi_s(x,\sigma)))ds = \int_0^{\tau'} \frac{d}{ds}(\gamma_n^\sigma(\phi_s(x',\sigma)))ds.$$

Let $f = f(\phi_s(x,\sigma),\sigma)$, $f' = f(\phi_s(x',\sigma),\sigma)$, $d\gamma = d\gamma_n^\sigma(\phi_s(x,\sigma))$ and $d\gamma' = d\gamma_n^\sigma(\phi_s(x',\sigma))$. Then rearranging terms

$$\int_0^\tau (f' \cdot d\gamma')ds - \int_0^\tau (f \cdot d\gamma)ds = \int_{\tau'}^\tau (f' \cdot d\gamma')ds.$$

Let L_1 be the Lipschitz constant of $f \cdot d\gamma$ (using the fact that γ_n^σ is smooth). Then

$$\int_{\tau'}^\tau f' \cdot d\gamma' \leq L_1 \tau \|x - x'\| \leq L_1 \tau \delta_k.$$

Since γ_n^σ defines a transversal foliation to vector field $f(\cdot,\sigma)$, $f \cdot d\gamma > 0$. Let $c = \min_{s\in[\tau,\tau']}\{f' \cdot d\gamma'\} > 0$. Letting $c_\gamma = \frac{L_1}{c}$ we obtain the result. □ □

Proposition 5.6.4. *Let $k_0 \in \mathbb{Z}^+$ be arbitrary, $x \in \mathcal{R}_{k_0}^1$, and $\mu \in \mathcal{U}_{k_0}^1$ be an ϵ-optimal control for x. Then $|J_k^1(x,\mu) - J_k^2(x,\mu)| \to 0$ as $k \to \infty$.*

Proof. We have

$$\begin{aligned} \left|J_k^1(x,\mu) - J_k^2(x,\mu)\right| \;\leq\; & \left|\sum_{j=1}^N \Big[\int_0^{\tau(\sigma_j,x_{j-1})} L(\phi_s(x_{j-1},\sigma_j),\sigma_j)ds\Big] + h(x_N)\right. \\ & \left. - \sum_{j=1}^N [\tau_{q_{j-1}} L(\xi_{j-1},\sigma_j)] - \hat{h}(x_N)\right| \end{aligned}$$

where $(x_{j-1},\sigma_j) \in q_{j-1}$ and $q_{j-1} = [(\xi_{j-1},\sigma_j)]$. There exists ξ_N such that $\hat{h}(x_N) = h(\xi_N)$ and $\|x_N - \xi_N\| \leq \delta_k$. Also, using the Mean Value Theorem, there exists $\tilde{t}$ with $\tilde{x} = \phi_{\tilde{t}}(x_{j-1},\sigma_j)$ and $\|\tilde{x} - \xi_{j-1}\| \leq \delta_k$ such that

$$\begin{aligned} \left|J_k^1(x,\mu) - J_k^2(x,\mu)\right| \;&\leq\; \sum_{j=1}^N \left|\tau(\sigma_j,x_{j-1})L(\tilde{x},\sigma_j) - \tau_{q_{j-1}} L(\xi_{j-1},\sigma_j)\right| + \left|h(x_N) - \hat{h}(x_N)\right| \\ &\leq\; \sum_{j=1}^N \tau_{q_{j-1}} L_L \delta_k + \sum_{j=1}^N [\tau_{q_{j-1}} - \tau(\sigma_j,x_{j-1})]L(\tilde{x},\sigma_j) + L_h\delta_k. \end{aligned}$$

Using Fact 1 the first term on the r.h.s. decreases linearly as δ_k. Call the second term on the r.h.s. "B". Splitting B into sums over control switches and time steps, we have

$$\begin{aligned} B \;&\leq\; M_L \sum_{j=2}^N [\tau_{q_{j-1}} - \tau(\sigma_j,x_{j-1})]\mathbb{I}(\sigma_j = \sigma_{j-1}) + M_L \sum_{j=1}^N [\tau_{q_{j-1}} - \tau(\sigma_j,x_{j-1})]\mathbb{I}(\sigma_j \neq \sigma_{j-1}) \\ &\leq\; M_L \sum_{j=2}^N c_{j-1}\tau_{q_{j-1}}\delta_k + M_L \sum_{j=1}^N \tau_{q_{j-1}} \mathbb{I}(\sigma_j \neq \sigma_{j-1}) \end{aligned}$$

for some $c_{j-1} \in \mathbb{R}$. In the second line we used Fact 2 and the fact that $\tau_{q_{j-1}} \geq \tau(\sigma_j, x_{j-1})$. Using Fact 1 the first term on the r.h.s. decreases linearly as δ_k. The second term on the r.h.s. goes to zero since μ has a fixed number of control switches for all $k \geq k_0$. □ □

Step 3: discrete states and non-determinacy.

We define

$$\hat{V}_k(x) := \min_{\sigma \in \Sigma_k} \{ \hat{V}_k(q) \mid (\sigma, x) \in q \}.$$

Also let $\hat{\mathcal{R}}_k = \{x \in \Omega \mid \hat{V}_k(x) < \infty\}$ and $\hat{\mathcal{R}} = \cup_k \hat{\mathcal{R}}_k$.

Remark 6.2.

(a) By Remark 6.1(c) and $V_k^1(x) \leq V_k^2(x)$, for each $x \in \cup_k \mathcal{R}_k^1$ and $\epsilon > 0$ there exists $m_\epsilon \in \mathbb{Z}^+$ and $\mu \in \mathcal{U}_{m_\epsilon}^1$ such that μ is an ϵ-optimal control for x w.r.t. V^2 satisfying Assumptions 2.2.

(b) $\hat{\mathcal{R}} \subset \cup_k \mathcal{R}_k^1$, but the converse is not true, in general.

(c) If μ is an ϵ-optimal control for x w.r.t. V_k^2, then we can assume $\phi_t(x, \mu)$ does not self-intersect, for if it did we can find $\tilde{\mu}$, also ϵ-optimal, which eliminates loops in $\phi_t(x, \mu)$.

(d) $\|x - y\| \to 0$ as $k \to \infty$ for all $y \in r_e(x)$ and all edges e of H_k, the hybrid automaton defined using Σ_k and C_k given in (3.2.2).

Proposition 5.6.5. *For all* $x \in \hat{\mathcal{R}}$, $|\hat{V}_k(x) - V_k^2(x)| \to 0$ *as* $k \to \infty$.

Proof. Fix $\epsilon > 0$ and $x \in \hat{\mathcal{R}}$. By Remark 6.2(a) there exists $m_\epsilon > 0$ and an ϵ-optimal control $\mu \in \mathcal{U}_{m_\epsilon}^1$ for x w.r.t. $V_{m_\epsilon}^2$. Denote $\mu = ((\sigma_1, \tau_1), \ldots, (\sigma_N, \tau_N))$, where τ_i is the time σ_i is applied. If c is a policy derived using δ_k and C_k, for $k \geq m_\epsilon$, then $0 \leq \hat{V}_k(q) - V_k^2(x) \leq \hat{J}_k(q, c) - J_k^2(x, \mu) + \epsilon$, where $q = [(\sigma_1, x)]$. If we can show there exists $\overline{k} \geq m_\epsilon$ such that for $k > \overline{k}$, there exists a policy $\overline{c}$ such that $\hat{J}_k(q, \overline{c}) - J_k^2(x, \mu) < \epsilon$ then the result follows.

We can find $\overline{k} \geq m_\epsilon$ such that, by Remark 6.2(d) and the transversality of $\phi_t(x, \mu)$ with the submanifolds where it switches controls and with Ω_f, there exists $\tilde{\mu} \in \mathcal{U}_k$, $k > \overline{k}$, such that each trajectory $\phi_t(x, \tilde{\mu})$ of H_k switches controls on the same (transversal) submanifolds as $\phi(x, \mu)$ and reaches Ω_f. Let Ψ_k be this set of trajectories of H_k starting at x. Let

$W_k(\phi) = \sum_{j=1}^{N} L^2(x_{j-1}, \sigma_j) + \hat{h}(x_N)$ where $\tilde{\mu} = ((\sigma_1, \tilde{\tau}_1, \ldots, (\sigma_N, \tilde{\tau}_N))$, $x_j^- = \phi_{\tilde{\tau}_j}(x_{j-1}, \sigma_j)$, and $x_j \in r_e(x_j^-)$, where $e = (\sigma_j, \sigma_{j+1})$ is an edge of H_k.

We observe that for $\phi, \phi' \in \Psi_k$, $\tilde{\mu} \in \mathcal{U}_k^1$, $k > \overline{k}$, $|W_k(\phi) - W_k(\phi')| \to 0$ as $k \to \infty$, using Lipschitz continuity of L and h, Remark 6.2(d), and the fact that $\tilde{\mu}$ is fixed for $k > \overline{k}$. Notice that $\phi(x, \mu) \in \Psi_k$, $k > \overline{k}$. We can define the control policy $\overline{c}$ such that automaton A accepts the time abstract trajectory starting at q corresponding to each trajectory of Ψ_k and with all other control assignments of $\overline{c}$ as time steps. $\overline{c}$ is admissible because otherwise some $\phi' \in \Psi_k$ would have a Zeno loop. Since ϕ' approaches $\phi_t(x, \mu)$ as $k \to \infty$, this would imply $\phi_t(x, \mu)$ has a loop, contradicting Remark 6.2(c). Now we observe that $\hat{J}(q, \overline{c}) = \max_{\phi \in \Psi_k} W_k(\phi) := W_k(\overline{\phi})$. Thus, $\hat{J}_k(q, \overline{c}) - J_k^2(x, \mu) \leq |W_k(\overline{\phi}) - W_k(\phi(x, \mu))| \to 0$ as $k \to \infty$. □ □

Combining Propositions 5.6.3, 5.6.4, and 5.6.5, we have

Theorem 5.6.6. *For all $x \in \hat{\mathcal{R}}$, $\hat{V}_k(x) \to V(x)$ as $k \to \infty$.*

5.7 Implementation

So far we have developed a discrete method for solving an optimal control problem based on hybrid systems and bisimulation. We showed that the solution of the discrete problem converges to the solution of the continuous problem as a discretization parameter δ goes to zero. Now we focus on the pragmatic question of how the discretized problem can be efficiently solved.

5.7.1 Motivation

Following the introduction of the concept of viscosity solution [62, 35], Capuzzo-Dolcetta [28] introduced a method for obtaining approximations of viscosity solutions based on a time discretization of the Hamilton-Jacobi-Bellman (HJB) equation. The approximations of the value function correspond to a discrete time optimal control problem, for which an optimal control can be synthesized which is piecewise constant. Finite difference approximations were also introduced in [36] and [90]. In general, the time discretized approximation of the HJB equation is solved by finite element methods. Gonzales and Rofman [46] introduced a discrete approximation by triangulating the domain of the finite horizon problem they

considered, while the admissible control set is approximated by a finite set. Gonzales and Rofman's approach is adapted in several papers, including [40].

Our work was inspired by the ideas of [96] which uses the special structure of an optimal control problem to obtain a single-pass algorithm to solve the discrete problem, thus bypassing the expensive iterations of a finite element method. The key property to find a single pass algorithm is to obtain a partition of the domain so that the cost-to-go function from any equivalence class of the partition is determined from knowledge of the cost-to-go function from those equivalence classes with strictly smaller cost-to-go functions. In our approach, we start with a triangulation of the domain provided by a bisimulation partition. *The combination of the structure of the bisimulation partition and the requirement of non-Zeno trajectories enables us reproduce the key property of [96], so that we obtain a Dijkstra-like algorithmic solution.* Our approach has the same complexity as that reported in [96] of $O(N \log N)$ if suitable data structures are used, where N is the number of locations of the finite automaton.

5.8 Non-deterministic Dijkstra algorithm

The dynamic programming solution (5.5.4)-(5.5.5) can be viewed as a shortest path problem on a non-deterministic graph subject to all optimal paths satisfying a non-Zeno condition. It is useful to consider an example to motivate the differences between the deterministic and non-deterministic cases.

Example 5.8.1. Consider the automaton of Figure 5.4. Suppose that $obs(e) = \sigma$ for $e = \{e_1, e_2, e_5, e_7\}$, $obs(e) = \sigma'$ for $e = \{e_3, e_4, e_6, e_8, e_9, e_{10}\}$, and $obs(e_{11}) = \sigma''$. Also, $\hat{L}(e_1) = 1$, $\hat{L}(e_4) = 4$, $\hat{L}(e_5) = 2$, $\hat{L}(e_8) = 1$, and $\hat{L}(e_{11}) = 1$, while $\hat{L}$ is zero for the other edges. If the automaton were interpreted as deterministic, one obtains

$$\begin{aligned}
\hat{V}(q_1) &= \min\{\ \hat{L}(e_1) + \hat{h}(q_f), \hat{V}(q_2), \hat{V}(q_3)\ \} \\
\hat{V}(q_2) &= \min\{\ \hat{L}(e_4) + \hat{h}(q_f), \hat{V}(q_1), \hat{V}(q_4)\ \} \\
\hat{V}(q_5) &= \min\{\ \hat{L}(e_{11}) + \hat{h}(q_f), \hat{V}(q_2), \hat{V}(q_3)\ \}.
\end{aligned}$$

These equations resolve to $\hat{V}(q_1) = \hat{V}(q_2) = \hat{V}(q_5) = 1 + \hat{h}(q_f)$, and the control policy is $c(q_1) = c(q_2) = \sigma$, and $c(q_5) = \sigma'$. If the automaton is non-deterministic, then the control

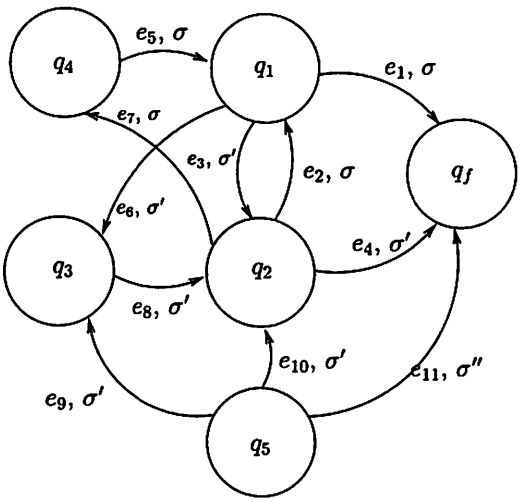

Figure 5.4: Nondeterministic automaton

policy is deduced as follows. Using (5.5.4) we have

$$\begin{aligned}
\hat{V}(q_1) &= \min\{\hat{L}(e_1) + \hat{h}(q_f), \max\{\hat{V}(q_2), \hat{V}(q_3)\}\} \\
\hat{V}(q_2) &= \min\{\hat{L}(e_4) + \hat{h}(q_f), \max\{\hat{V}(q_4), \hat{V}(q_1)\}\} \\
\hat{V}(q_5) &= \min\{\hat{L}(e_{11}) + \hat{h}(q_f), \max\{\hat{V}(q_3), \hat{V}(q_2)\}\}.
\end{aligned}$$

Substituting known quantities we find

$$\begin{aligned}
\hat{V}(q_1) &= \min\{1 + \hat{h}(q_f), 1 + \hat{V}(q_2)\} \\
\hat{V}(q_2) &= \min\{4 + \hat{h}(q_f), 2 + \hat{V}(q_1)\} \\
\hat{V}(q_5) &= \min\{5 + \hat{h}(q_f), 1 + \hat{V}(q_2)\}.
\end{aligned}$$

When solved simultaneously, these equations yield $\hat{V}(q_1) = 1 + \hat{h}(q_f)$, $\hat{V}(q_2) = 3 + \hat{h}(q_f)$, $\hat{V}(q_5) = 4 + \hat{h}(q_f)$, and $c(q_1) = c(q_2) = \sigma$, and $c(q_5) = \sigma'$. Notice that all trajectories are non-Zeno inspite of the fact that a trajectory starting from q_5 may take two consecutive control switches.

5.8.1 Description

The algorithm is a modification of the Dijkstra algorithm for deterministic graphs [38] and synthesizes an optimal, memoryless, admissible control policy that takes the states of a non-deterministic graph to a target set. As in the deterministic case, the algorithm is greedy: if

a step can be taken into a set of states whose controls have already been assigned and have a minimum cost, the step is assigned.

First, we define the notation. F_n is the set of states that have been assigned a control and are deemed "finished" at iteration n, while U_n are the unfinished states. At each n, $Q = U_n \cup F_n$. $\Sigma_n(q)$ is the set of control events at iteration n that take state q to finished states exclusively. $\tilde{U}_n$ is the set of states for which there exists a control event that can take them to finished states exclusively. $\tilde{V}_n(q)$ is a tentative cost-to-go value at iteration n. B_n is the set of "best" states among $\tilde{U}_n$.

The non-deterministic Dijkstra (NDD) algorithm first determines $\tilde{U}_n$ by checking if any q in U_n can take a step to states belonging exclusively to F_n. For states belonging to $\tilde{U}_n$, an estimate of the value function $\tilde{V}$ following the prescription of (5.5.4) is obtained: among the set of control events constituting a step into states in F_n, select the event with the lowest worst-case cost. Next, the algorithm determines B_n, the states with the lowest $\tilde{V}$ among $\tilde{U}_n$, and these are added to F_{n+1}. The iteration counter is incremented until it reaches $N = |Q|$. It is assumed in the following description that initially $\hat{V}(q) = \infty$ and $c(q) = \emptyset$ for all $q \in Q$.

Procedure NDD:

$F_1 = Q_f$; $U_1 = Q - Q_f$;
for each $q \in Q_f$, $\hat{V}(q) = \hat{h}(q)$;

for $n = 1$ to N, do
  for each $q \in U_n$,
    $\Sigma_n(q) = \{\sigma' \in \Sigma_\delta \mid \text{if } q \xrightarrow{\sigma'} q', \text{then } q' \in F_n\}$;
  $\tilde{U}_n = \{q \in U_n \mid \Sigma_n(q) \neq \emptyset\}$;
  for each $q \in \tilde{U}_n$,
    $\tilde{V}_n(q) = \min_{\sigma' \in \Sigma_n(q)}\{\max_{e=(q,q') \in E_{\sigma'}(q)}\{\hat{L}(e) + \hat{V}(q')\}\}$;
  $B_n = \text{argmin}_{q \in \tilde{U}_n}\{\tilde{V}_n(q)\}$;
  for each $q \in B_n$,
    $\hat{V}(q) = \tilde{V}_n(q)$;
    $c(q) = \text{argmin}_{\sigma' \in \Sigma_n(q)}\{\max_{e=(q,q') \in E_{\sigma'}(q)}\{\hat{L}(e) + \hat{V}(q')\}\}$;
  endfor
  $F_{n+1} = F_n \cup B_n$; $U_{n+1} = Q - F_{n+1}$;
endfor

The algorithm is opportunistic in assigning control switches. At the first iteration, say n, that a state can take a control switch to finished states, it will be assigned the control switch by the algorithm. This is because control switches have zero instantaneous cost, so the state will have a minimum $\tilde{V}$ and will be included in B_n. In fact, B_n can include either states that can take control switches and zero cost time steps to F_n, or states that can take a non-zero cost time step to F_n. The opportunistic assignment of control switches is intuitively what we expect: waiting for a later iteration to assign them does not make sense because states that finish later have a higher or equal cost-to-go.

5.8.2 Justification

In this section we show that the control policy synthesized by algorithm NDD allows non-Zeno trajectories only and is optimal in the required worst-case sense.

Lemma 5.8.1. *Algorithm NDD synthesizes a control policy with no Zeno loops.*

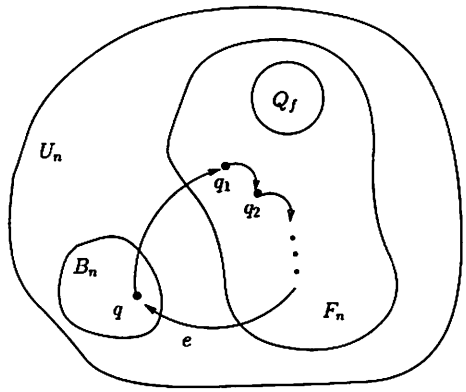

Figure 5.5: A loop of control switches

Proof. We argue by induction. The claim is obviously true for F_1. Suppose that the states of F_n have been assigned controls forming no Zeno loops. Consider F_{n+1}. Each state of B_n takes either a time step or a control switch to F_n so there cannot be a Zeno loop in B_n. The only possibility is for some $q \in B_n$ to close a Zeno loop with states in F_n, as shown in Figure 5.5. This implies there exists a control assignment that allows an edge from F_n to q to be taken; but this is not allowed by NDD. Thus, F_{n+1} has no Zeno loops. □

Next we prove that the algorithm is *optimal* in the sense that it synthesizes a control policy such that each $q \in Q$ reaches Q_f with the best worst-case cost. We observe a few properties of the algorithm. First, if all states of Q can reach Q_f then $Q - Q_f = \cup_n B_n$. Second, as in the deterministic case, the algorithm computes $\hat{V}$ in order of level sets of $\hat{V}$. In particular, $\hat{V}(B_n) \leq \hat{V}(B_{n+1})$. Finally, we need the following property.

Lemma 5.8.2. *For all $q \in Q$ and $\sigma' \in \Sigma_\delta$,*

$$\hat{V}(q) \leq \max_{e=(q,q') \in E_{\sigma'}(q)} \{\hat{L}(e) + \hat{V}(q')\}.$$

Proof. Fix $q \in Q$ and $\sigma' \in \Sigma_\delta$. There are two cases.
Case 1.

$$\hat{V}(q) \leq \max_{e=(q,q') \in E_{\sigma'}(q)} \{\hat{V}(q')\}.$$

In this case the result is obvious.

Case 2.

$$\hat{V}(q) > \max_{e=(q,q')\in E_{\sigma'}(q)} \{\hat{V}(q')\}. \tag{5.8.1}$$

We observed above that q belongs to some B_n. Suppose w.l.o.g. that $q \in B_j$. Together with (5.8.1) this implies $q' \in F_j$ for all q' such that $q \xrightarrow{\sigma'} q'$. This, in turn, means that $\sigma' \in \Sigma_j(q)$ and according to the algorithm

$$\hat{V}(q) = \tilde{V}_n(q) \leq \max_{e=(q,q')\in E_{\sigma'}(q)} \{\hat{L}(e) + \hat{V}(q')\}$$

which proves the result. □

The main result is the following.

Theorem 5.8.3. *Algorithm NDD is optimal.*

Proof. Let $V(q)$ be the optimal (best worst-case) cost-to-go for $q \in Q$ and $\overline{Q} = \{q \in Q \mid V(q) < \hat{V}(q)\}$. Let $l(\pi_q)$ be the number of edges taken by the shortest optimal (best worst-case) trajectory π_q from q. Define $\overline{q} = \arg\min_{q\in\overline{Q}}\{l(\pi_q)\}$. Suppose that the best worst-case trajectory starting at $\overline{q}$ is $\pi_{\overline{q}} = \overline{q} \xrightarrow{\sigma'} \overline{\overline{q}} \to \ldots$. We showed in the previous lemma that

$$\hat{V}(\overline{q}) \leq \max_{e=(\overline{q},q')\in E_{\sigma'}(\overline{q})} \{\hat{L}(e) + \hat{V}(q')\} \leq \hat{L}(e) + \hat{V}(\overline{\overline{q}}).$$

Since $\pi_{\overline{q}}$ is the best worst-case trajectory from $\overline{q}$ and by the optimality of $V(\overline{q})$

$$V(\overline{q}) = \max_{e=(\overline{q},q')\in E_{\sigma'}(\overline{q})} \{\hat{L}(e) + V(q')\} = \hat{L}(e) + \hat{V}(\overline{\overline{q}}).$$

Since $\pi_{\overline{q}}$ is the shortest best worst-case trajectory, we know that $\overline{\overline{q}} \notin \overline{Q}$, so $V(\overline{\overline{q}}) = \hat{V}(\overline{\overline{q}})$. This implies $\hat{V}(\overline{q}) \leq \hat{L}(e) + V(\overline{\overline{q}}) = V(\overline{q})$, a contradiction. □

Remarks:

1. It is intuitively reasonable that the algorithm cannot synthesize a controller with Zeno loops. This worst-case behavior would show up in the value function, forcing it to be infinite for states that can reach the loop.

2. When we say that the algorithm is optimal, we mean the algorithm determines the best worst-case cost to take each state to the target set. In fact, (see remark below) the hybrid system or continuous system using the synthesized controller may perform better than worst case.

3. The non-deterministic automaton predicts more trajectories than what either the continuous system or the hybrid system can exhibit. Indeed, the automaton may exhibit a trajectory that reaches the target set using only control switches, and thus accruing zero cost. This is not of concern. Such a trajectory is an artifact of the non-determinacy of the automaton, and is not used in the determination of the value function, which accounts only for worst-case behavior, nor is it exhibited in either the hybrid system or the continuous system when the control policy synthesized by Algorithm NDD is used.

4. Related to the previous remark is that the non-deterministic automaton may also predict worst-case behavior which is not exhibited by the continuous system. It would appear that a discrepancy will develop between the cost-to-go obtained by applying the synthesized controller to the continuous system and the cost-to-go predicted by the nondeterministic automaton. This error is incurred every time a control switch is taken and is effectively an error in predicting the state and has an upper bound of δ at each iteration. This error was accounted for in our proof of convergence of the method, and the convergence result essentially depends on the fact that only a finite number of control switches occur.

Example 5.8.2. Consider the example of Figure 5.6. The states are labeled q_i and the number in the lower, left corner is the instantaneous cost of a time step. States can take a time step to the state immediately to the right, and they can take a control switch to states with a different σ_i value and overlapping vertically. (Edges are not drawn to keep the figure readable.) For example, state q_3 can take a time step to q_2 and a control switch to q_{12} and q_{13} using control σ_2, and to q_{17} and q_{20} using control σ_3. The algorithm generates the following data:

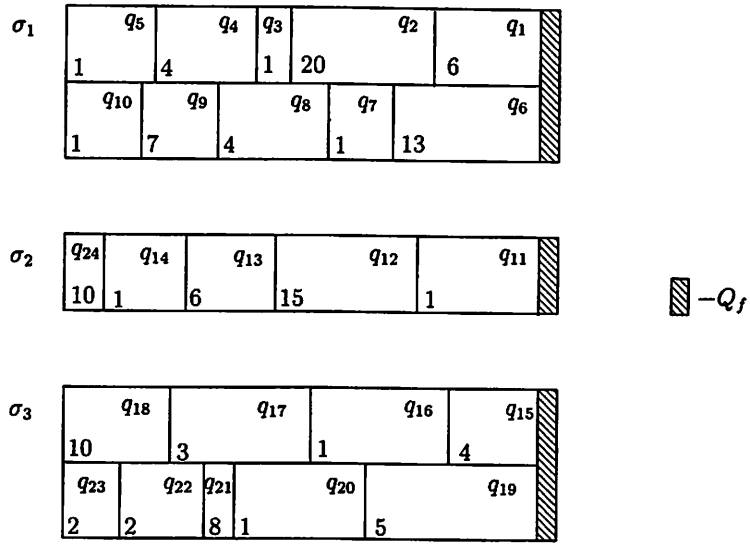

Figure 5.6: Example of algorithm NDD

n	B_n	$\hat{V}(B_n)$	control
1	$\{q_{11}\}$	1	σ_2
2	$\{q_{15}, q_1\}$	1	σ_2
3	$\{q_{16}\}$	2	σ_3
4	$\{q_{17}, q_{19}\}$	5	σ_3
5	$\{q_6\}$	5	σ_3
6	$\{q_7, q_{20}\}$	6	$c(q_7) = \sigma_1$, $c(q_{20}) = \sigma_3$
7	$\{q_2, q_3, q_{12}\}$	6	σ_3
8	$\{q_4, q_8\}$	10	σ_1
9	$\{q_5\}$	11	σ_1
10	$\{q_{13}\}$	12	σ_2
11	$\{q_{21}\}$	12	σ_2
12	$\{q_{14}\}$	13	σ_2
13	$\{q_9, q_{22}\}$	13	σ_2
14	$\{q_{10}\}$	14	σ_1
15	$\{q_{24}, q_{18}, q_{23}\}$	14	σ_1

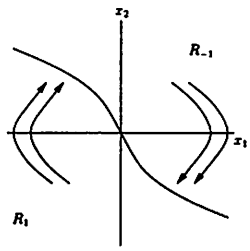

Figure 5.7: The switching curve for the double integrator system.

5.9 Examples

5.9.1 Double integrator system

We apply our method to the time optimal control problem of the rocket car. Given the equations of motion

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= u \end{aligned}$$

and the set of admissible controls $U = \{u \ : \ |u| \leq 1\}$. We select $\Omega = (-1,1) \times (-1,1)$ and $\Omega_f = \overline{B}_\epsilon(0)$, the closed epsilon ball centered at 0. The cost-to-go function is $J(x,\mu) = \int_0^{T(x,\mu)} dt$. The bang-bang solution obtained using Pontryagin's maximum principle is well known to involve a single switching curve shown in Figure 5.7. In region R_1, the control $u = 1$ is applied. When the switching curve is reached, the control is switched to $u = -1$. In region R_{-1}, the control $u = -1$ is applied, and when the switching curve is reach, the control is switched to $u = 1$. The continuous value function V is shown in Figure 5.8.

To construct the hybrid automaton H we select $\Sigma_\delta = \{-1, 1\}$, so that $\delta = 1$. H is show in Figure 5.1. The state space is $\{\sigma_{-1} = -1, \sigma_1 = 1, \sigma_f\} \times \mathbb{R}^n$. $g_{e_{-1}}$ and g_{e_1} are unknown and must be synthesized, while $g_{e_2} = g_{e_3} = \Omega_f$.

A first integral for vector field $\dot{x}_1 = x_2$, $\dot{x}_2 = 1$ is $x_1 - \frac{1}{2}x_2^2 = c_1$, $c_1 \in \mathbb{R}$. For $\dot{x}_1 = x_2$, $\dot{x}_2 = -1$ a first integral is $x_1 + \frac{1}{2}x_2^2 = c_2$, $c_2 \in \mathbb{R}$. We select a transverse foliation for each vector field, given by $x_2 = c_3$.

We define Q, Q_f, E, $\hat{L}$ and $\hat{h}$ for automaton A derived from H in Figure 5.1. Q can be visualized using Figure 5.3. The states $q \in Q$ are of the form $(\sigma, [x])$ with $\sigma \in \{\sigma_{-1}, \sigma_1\}$.

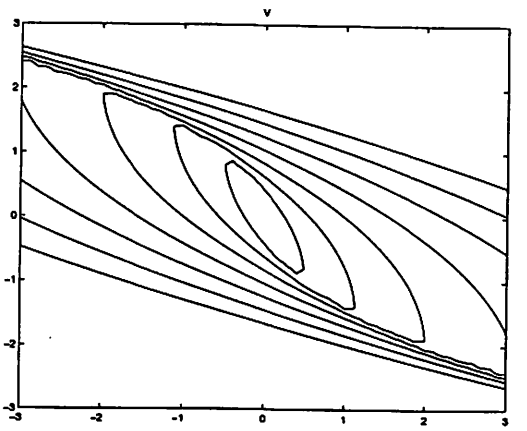

Figure 5.8: Value function for the continuous problem.

For the case $\sigma = \sigma_1$ with $c_1, c_2 \in \mathbb{R}$, $[x]$ is either an open subset of $\mathbb{R}^2$ bounded by the leaves $c_1 < x_1 - \frac{1}{2}x_2^2 < c_1 + \Delta$ and $c_2 < x_2 < c_2 + \Delta$; or an open interval in a horizontal leaf $x_1 - \frac{1}{2}x_2^2 = c_1$, $c_2 < x_2 < c_2 + \Delta$; or an open interval in a vertical leaf $c_1 < x_1 - \frac{1}{2}x_2^2 < c_1 + \Delta$, $x_2 = c_2$; or a point $x_1 - \frac{1}{2}x_2^2 = c_1$, $x_2 = c_2$. Analogous expressions can be written for $\sigma = \sigma_{-1}$. In Figure 5.3, $\Delta = 0.25$, $c_1 \in [-1, 1]$ and $c_2 \in [-1, 1]$. If we identify equivalence classes $(\sigma, [x])$ by their Euclidean coordinates (c_1, c_2) directly, then Q_f, shown in Figure 5.3 as the regions inside the dotted lines, includes states $(\sigma, [x])$, where $[x]$ satisfies $c_1, c_2 \in (-\Delta, \Delta)$.

Let us consider the edges corresponding to control switches of A. $q = (\sigma_1, [x]) \in Q$ has an outgoing edge to $q' = (\sigma_{-1}, [y]) \in Q$ if $[x] \cap [y] \neq \emptyset$. For example, for $q = (\sigma_1, [x])$ and $[x]$ satisfying $c_1 \in (-.25, -.5)$ and $c_2 = .25$, there are three outgoing edges from q to q_i, $i = 1, \ldots, 3$, with $[y]$ satisfying $c_2 = .25$ and $c_1 \in (-.5, -.25)$, $c_1 = -.25$, and $c_1 \in (-.25, 0)$, respectively. Similarly, for $q = (\sigma_1, [x])$ and $[x]$ satisfying $c_1 \in (-.5, -.25)$ and $c_2 \in (.75, 1)$, there are five outgoing edges from q to q_i, $i = 1, \ldots, 3$, with $[y]$ satisfying $c_2 \in (.75, 1)$ and $c_1 \in (-.25, 0)$, $c_1 = 0$, $c_1 \in (0, .25)$, $c_1 = .25$ and $c_1 \in (.25, .5)$, respectively. Edges corresponding to time steps of A can be determined from visual inspection of Figure 5.3. For example, for $q = (\sigma_1, [x])$ with $[x]$ satisfying $c_1 \in (-.25, -.5)$ and $c_2 = .25$, there is an outgoing edge from q to $q' = (\sigma_1, [y])$ with $[y]$ satisfying $c_1 \in (-.25, -.5)$ and $c_2 \in (.25, .5)$.

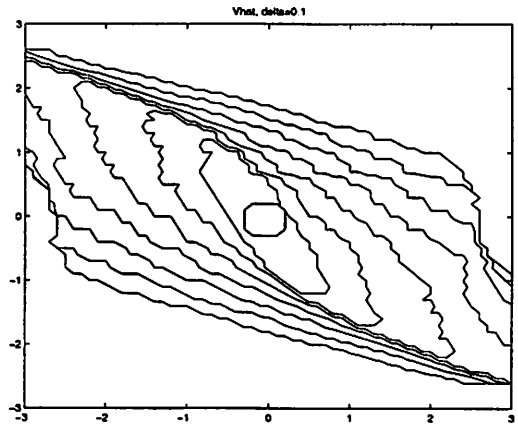

Figure 5.9: $\hat{V}$ for $\Delta = 0.1$.

Finally, we define $\hat{L}$ and $\hat{h}$. Let $e = (q, q')$ with $q = (\sigma, [x])$ and $q' = (\sigma', [y])$. Then

$$\hat{L}(e) = \begin{cases} \Delta & \sigma = \sigma' \ \wedge \ [x] \text{ satisfies } c_2 \in (a, a + \Delta), \text{ some } a \in \mathbb{R} \\ 0 & \sigma = \sigma' \ \wedge \ [x] \text{ satisfies } c_2 = a, \text{ some } a \in \mathbb{R} \\ 0 & \sigma \neq \sigma' \end{cases} .$$

In this example, $\hat{h}(q) = 0$ for all $q \in Q$.

The results of algorithm NDD are shown in Figures 5.9, 5.10, and 5.11. Figure 5.9 shows $\hat{V}$ for $\Delta = 0.1$. The enabling conditions $g_{e_{-1}}$ and g_{e_1} are shown in Figures 5.10 and 5.11, respectively. The roughness in the boundaries of the enabling conditions is caused both by the discretization of the state space and by the non-determinism of the finite automaton.

5.9.2 Fuller's problem

In this example we discuss how our method can be applied in the canonically difficult situation of Fuller's problem. Fuller's problem is of interest because all of its trajectories are Zeno. We propose an ad hoc method to avoid the Zeno behavior.

Consider the optimal control problem (5.1.2) with $|u| \leq 1$ and the cost function $J(x, \mu) = \int_0^{T(x,\mu)} x_1^2(s)ds$. Let $\xi \in (0, \frac{1}{2})$ be a constant. It was shown in [44] that the optimal switching

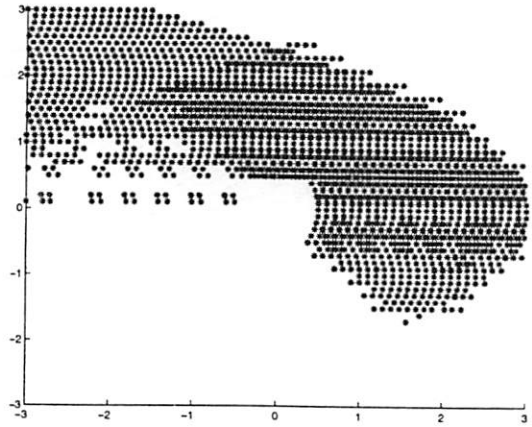

Figure 5.10: Enabling condition $g_{e_{-1}}$.

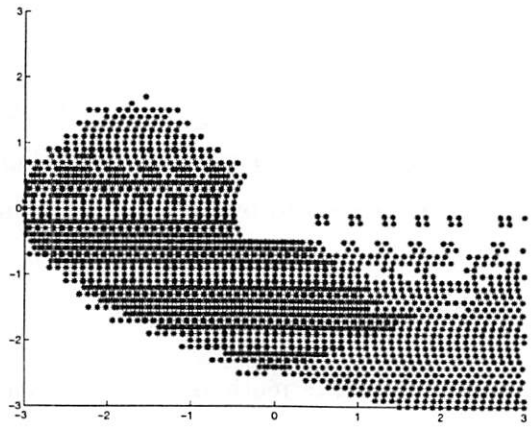

Figure 5.11: Enabling condition g_{e_1}.

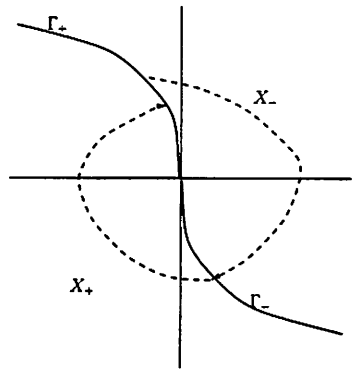

Figure 5.12: Vector fields and switching curves for Fuller's example

curves Γ_- and Γ_+ are given by

$$\begin{aligned} \Gamma_+ : \quad & x_i = -\xi x_2^2 && x_2 > 0 \\ \Gamma_- : \quad & x_i = \xi x_2^2 && x_2 < 0. \end{aligned}$$

The situation is depicted in Figure 5.12. The upper vector field X_- uses $u = -1$ while the lower vector field X_+ uses $u = 1$. The combined vector field is denoted X.

Solutions of X_- are parabolic curves $x_1 - \frac{1}{2}x_2^2 = c$, $c \in \mathbb{R}$. The parabola meets Γ_+ at $x_1 = -\xi x_2^2 = c + \frac{1}{2}x_2^2$ or

$$\left(\frac{-\xi c}{\frac{1}{2} - \xi}, \sqrt{\frac{c}{\frac{1}{2} - \xi}} \right). \tag{5.9.1}$$

The parabola meets Γ_- when $x_1 = \xi x_2^2 = c - \frac{1}{2}x_2^2$ or

$$\left(\frac{\xi c}{\frac{1}{2} + \xi}, -\sqrt{\frac{c}{\frac{1}{2} + \xi}} \right). \tag{5.9.2}$$

Let the X trajectory cross Γ_+ at $p^n = (x_1^n, x_2^n)$ and Γ_- at $\overline{p}^n = (\overline{x}_1^n, \overline{x}_2^n)$. (5.9.1) and (5.9.2) given

$$\overline{x}_2^n = \sqrt{\frac{\frac{1}{2} - \xi}{\frac{1}{2} + \xi}} x_2^n. \tag{5.9.3}$$

Since the picture is symmetric with respect to x_1 and $-x_1$ and by (5.9.3)

$$x_2^{n+1} = \frac{\frac{1}{2} - \xi}{\frac{1}{2} + \xi} x_2^n.$$

Hence $x_1^n, x_2^n \to 0$ as $n \to \infty$. The time it takes the X trajectory to go from p^n to $\overline{p}^n$ to p^{n+1} is

$$\begin{aligned} t^n &= x_2^n + 2|\overline{x}_2^n| + x_2^{n+1} \\ &= \frac{1 + 2\sqrt{\frac{1}{4} - \xi^2}}{\frac{1}{2} + \xi} x_2^n. \end{aligned}$$

The total time elapsed for an X trajectory to reach the origin is

$$\begin{aligned} T &= \sum_{n=1}^{\infty} t^n \\ &= \frac{1 + 2\sqrt{\frac{1}{4} - \xi^2}}{\frac{1}{2} + \xi} \sum_{n=0}^{\infty} \left(\frac{\frac{1}{2} - \xi}{\frac{1}{2} + \xi} \right)^n x_{20} \\ &= \frac{1 + 2\sqrt{\frac{1}{4} - \xi^2}}{2\xi} x_{20}. \end{aligned}$$

Thus, every trajectory takes an infinite number of switches in finite time. The origin is called a *Zeno point.* It was shown in [87] that Zeno points are stationary points but not equilibrium points of either vector field X_- or X_+..

To avoid Zeno behavior in this example, we propose the ad hoc fix of enlarging the target set to be a closed ball around the origin. We can obtain a switching strategy and approximate value function using the same methods as in the double integrator example.

Chapter 6

Strategies without Bisimulation

For us there is only the trying. The rest is not our business.
- T.S. Eliot.

In Section 3.4.2 we introduced symbolic model checking. The question addressed in this chapter is whether the symbolic reachability algorithm for rectangular automata terminates in a finite number of iterations. We study this problem because it has the interesting feature that no finite bisimulation for rectangular automata is available; nevertheless the reachability problem for initialized rectangular automata terminates. It serves as an example that bisimulation may be too strong a requirement on a hybrid system to perform symbolic model checking.

The first result on decidability of rectangular automata was reported in [79] and it was quickly followed by an alternative proof in [50]. The first proof approach involved mapping the rectangular automaton to a discrete-time automaton while the second proof approach used a mapping from a rectangular automaton with n variables to a timed automaton with $2n$ variables. This chapter provides a third proof approach, which is based on a direct analysis of the symbolic model checking algorithm. This method has the benefit that it can be extended to other decidability questions such as decidability of controller synthesis. For example in controller synthesis an operator called *unavoidable predecessor*, $\tilde{Pre}$, is needed. Proving decidability using $\tilde{Pre}$ involves proving closure properties of a class of formulas associated with the class of hybrid automata (in this case rectangular automata) under $\tilde{Pre}$. The results in this chapter show how this is done for the operators required in symbolic reachability analysis.

Notation. x' refers to the updated value of a variable x after a transition is taken. $\neg S$ is

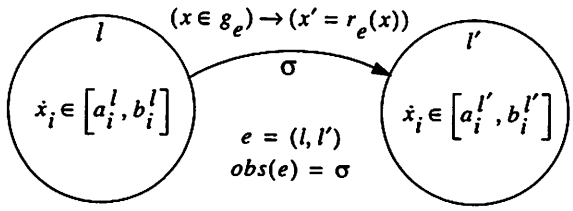

Figure 6.1: Fragment of a rectangular automaton.

the complement of set S. The notation $x \models \gamma$ means "x satisfies formula γ". $\mathcal{F}(\mathbb{R}^n)$ is the set of convex-valued maps on $\mathbb{R}^n$.

6.1 Rectangular automata

A rectangular automaton H is a hybrid automaton as defined in Section 2.2 where each component M_l is a (compact) integer-bounded rectangular subset of $\mathbb{R}^n$, and $X : L \rightarrow \mathcal{F}(\mathbb{R}^n)$ is a rectangular-valued differential inclusion on $L \times \mathbb{R}^n$. Let $Q = \cup_{l \in L}\{l\} \times M_l$. The inclusion restricted to l is $X^l = \Pi_{i=1}^n [a_i^l, b_i^l]$; that is, for each $l \in L$, the dynamics are given by $\dot{x}_i \in [a_i^l, b_i^l]$. $g_e \subset \mathbb{R}^n$ is a rectangular region of the form $g_e = \Pi_{i=1}^n [c_i, d_i]$. For each $x \in g_e$, $r_e(x)$ is a rectangular region of the form $(r_e(x))_i := [r_i, s_i]$, if the ith component is reset, and $(r_e(x))_i := x_i$, if not. We define a map $obs : E \rightarrow \Sigma$ which gives the control event associated to each edge. We will assume that

1. for $e_1, e_2 \in E$, if $e_1 \neq e_2$ and $obs(e_1), obs(e_2) \in \Sigma_c$, then $obs(e_1) \neq obs(e_2)$, and for simplicity $\Sigma_u = \{env\}$,

2. H is *compact*; that is, for each $l \in L$, X^l defines a compact rectangle, and for each $e \in E$, g_e is compact, and for each $x \in g_e$, $r_e(x)$ is compact.

3. H is *initialized*; that is, for every $e = (l, \sigma, l') \in E$, if the ith component of the reset map is identity, then the ith component of the inclusion does not change, or $(r_e(x))_i = x_i$ implies $X_i^l = X_i^{l'}$.

For the remainder of the chapter we consider only compact, initialized rectangular automata (CIRA).

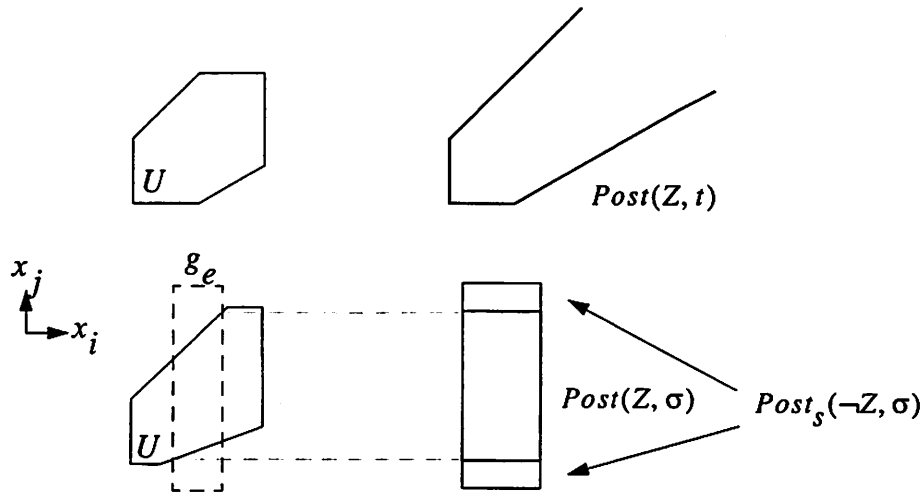

Figure 6.2: Weak Post.

6.1.1 *Post* and *Pre* operators

Building on the definitions of Section 3.4.2, a region $U \subset \mathbb{R}^n$ is a *polyhedral region* if it is a polyhedron. A zone is called a *polyhedral zone* (respectively, rectangular,bounded,compact zone) if $U^l = \bigcup_k U_k^l$, where each $U_k^l \subset \mathbb{R}^n$ is a polyhedral (respectively, rectangular, bounded, compact) region. Z is a *simple polyhedral zone* if $Z = \{l\} \times U$, where U is a polyhedral region. We define the set of all polyhedral zones to be $\mathcal{Z}$. For region U and $e \in E$, define $\neg_e U = g_e \setminus U$ and $\neg_{r_e} U = r_e(g_e) \setminus U$.

Let $Z \in \mathcal{Z}$ be a simple polyhedral zone, $\sigma \in \Sigma$, $t \in \mathbb{R}^+$, and $\Sigma' \subseteq \Sigma$.

We define two post operators called weak and strong post, which are required to distinguish the following two situations: (1) there exists a trajectory originating from the initial zone that reaches a target point, and (2) all trajectories that reach a target point originate in the initial zone.

We define the weak post operator $Post : \mathcal{Z} \times (2^\Sigma \cup \mathbb{R}^+) \to \mathcal{Z}$ to be

$$Post(Z,\sigma) = \{q \in Q \mid \exists q' \in Z \,.\, q' \xrightarrow{\sigma} q\} \tag{6.1.1}$$

$$Post(Z,t) = \{q \in Q \mid \exists q' \in Z, \exists t \in \mathbb{R}^+ \,.\, q' \xrightarrow{t} q\} \tag{6.1.2}$$

$$Post(Z,\Sigma') = \bigcup_{\sigma \in \Sigma'} Post(Z,\sigma). \tag{6.1.3}$$

$Post(Z,\sigma)$ is the zone of states reachable in one σ-step from Z. $Post(Z,t)$ is the zone of states that can be reached in a t-step, where $t \in \mathbb{R}^+$. $Post(Z,\Sigma')$ is the zone of states

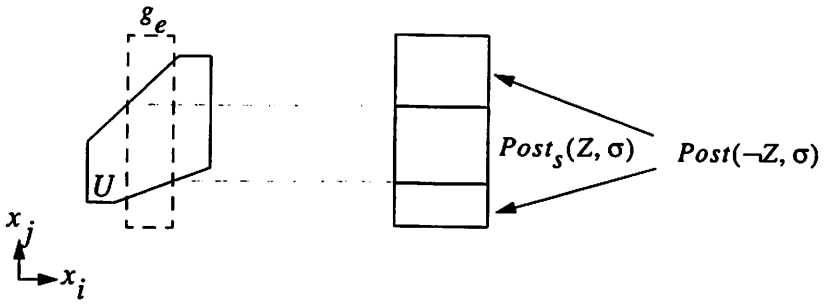

Figure 6.3: Strong Post.

reachable in one σ-step for $\sigma \in \Sigma'$. Figure 6.2 shows weak post in time, and weak post on a σ-step in which x_i is reset, but x_j is not.

Strong post, $Post_s : \mathcal{Z} \times 2^{\Sigma} \to \mathcal{Z}$ is defined to be

$$Post_s(Z, \sigma) = \{q \in Q \mid \forall q' \,.\, q' \xrightarrow{\sigma} q, q' \in Z\} \tag{6.1.4}$$

$$Post_s(Z, \Sigma') = \bigcup_{\sigma \in \Sigma'} Post_s(Z, \sigma). \tag{6.1.5}$$

$Post_s(Z, \sigma)$ is the zone of states reachable in one σ-step from Z only. $Post_s(Z, \Sigma')$ is the zone of states reachable in one σ-step for $\sigma \in \Sigma'$, from Z only. Figure 6.3 shows strong post on a σ-step in which x_i is reset, but x_j is not.

We define two predecessor operators called weak and strong pre, in order to distinguish two situations: (1) there exists a trajectory originating in a zone that reaches a target zone, or (2) all trajectories originating in a zone reach a target zone.

We define weak pre, $Pre : \mathcal{Z} \times (2^{\Sigma} \cup \mathbb{R}^+) \to \mathcal{Z}$ to be

$$Pre(Z, \sigma) = \{q \in Q \mid \exists q' \in Z \,.\, q \xrightarrow{\sigma} q'\} \tag{6.1.6}$$

$$Pre(Z, t) = \{q \in Q \mid \exists q' \in Z, \exists t \in \mathbb{R}^+ \,.\, q \xrightarrow{t} q'\} \tag{6.1.7}$$

$$Pre(Z, \Sigma') = \bigcup_{\sigma \in \Sigma'} Pre(Z, \sigma). \tag{6.1.8}$$

$Pre(Z, \sigma)$ is the zone of states that can reach Z in one σ-step. $Pre(Z, t)$ is the zone of states that can reach Z in a t-step, where $t \in \mathbb{R}^+$. $Pre(Z, \Sigma')$ is the zone of states that can reach Z in one σ-step for $\sigma \in \Sigma'$. Figure 6.4 shows weak pre in time, and weak pre on a σ-step in which x_i is reset, but x_j is not.

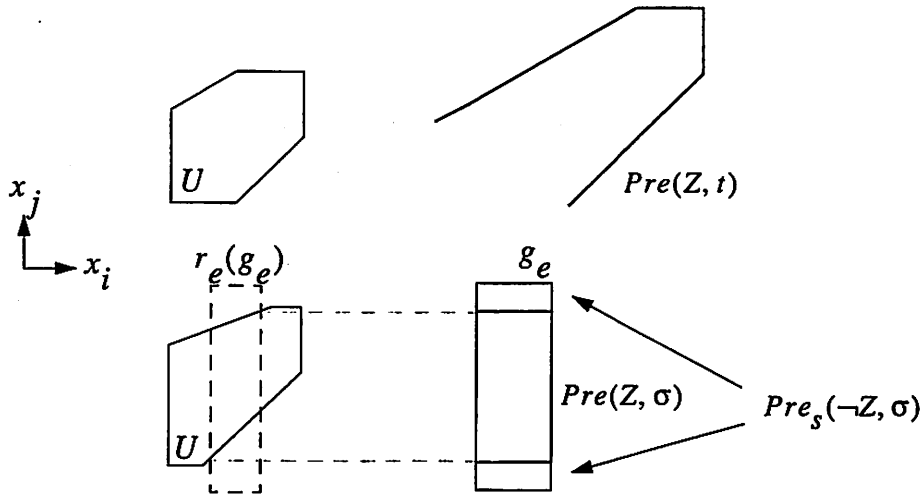

Figure 6.4: Weak Pre.

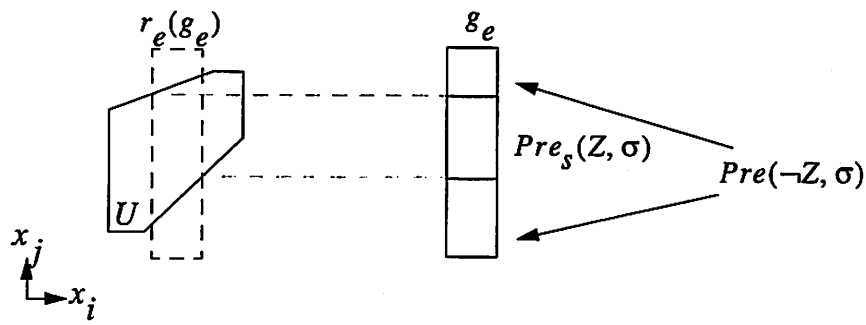

Figure 6.5: Strong Pre.

Strong pre, $Pre_s : \mathcal{Z} \times 2^{\Sigma} \to \mathcal{Z}$ is defined to be

$$Pre_s(Z,\sigma) = \{q \in Q \mid \forall q' \,.\, q \xrightarrow{\sigma} q', q' \in Z\} \tag{6.1.9}$$

$$Pre_s(Z,\Sigma') = \bigcup_{\sigma \in \Sigma'} Pre_s(Z,\sigma). \tag{6.1.10}$$

$Pre_s(Z,\sigma)$ is the zone of states that must reach Z in one σ-step. Figure 6.5 shows strong pre on a σ-step in which x_i is reset, but x_j is not. $Pre_s(Z,\Sigma')$ is the zone of states that must reach Z in one σ-step for $\sigma \in \Sigma'$.

Several useful facts about the dual nature of Pre/Pre_s and $Post/Post_s$ are summarized in the following Lemma.

Lemma 6.1.1. *Given a CIRA H with edge $e \in E$, $obs(e) = \sigma$, and a simple polyhedral zone Z, we have*

$$\begin{aligned} Pre(Z,\sigma) &= \neg_e Pre_s(\neg Z,\sigma), \\ Pre_s(Z,\sigma) &= \neg_e Pre(\neg Z,\sigma), \\ Post(Z,\sigma) &= \neg_{r_e} Post_s(\neg Z,\sigma), \\ Post_s(Z,\sigma) &= \neg_{r_e} Post(\neg Z,\sigma). \end{aligned}$$

Proof. Let $q = (l,x) \in Pre(Z,\sigma)$. Necessarily $x \in g_e$. Because $q \xrightarrow{\sigma} q'$ where $q' \in Z$, $q \notin Pre_s(\neg Z,\sigma)$. Hence $q \in \neg_e Pre_s(\neg Z,\sigma)$. Let $q = (l,x) \in Pre_s(Z,\sigma)$. Necessarily $x \in g_e$. Because $q \xrightarrow{\sigma} q'$ implies $q' \in Z$, there does not exist $q'' \in \neg Z$ such that $q \xrightarrow{\sigma} q''$. Hence $q \notin Pre(\neg Z,\sigma)$, so $q \in \neg_e Pre(\neg Z,\sigma)$. Let $q' = (l',x') \in Post(Z,\sigma)$. Necessarily $x' \in r_e(g_e)$. There exists $q \in Z$ such that $q \xrightarrow{\sigma} q'$. Hence $q' \notin Post_s(\neg Z,\sigma)$, so $q' \in \neg_{r_e} Post_s(\neg Z,\sigma)$. Let $q' = (l',x') \in Post_s(Z,\sigma)$. Necessarily $x' \in r_e(g_e)$. Because $q \xrightarrow{\sigma} q'$ implies $q \in Z$, there does not exist $q'' \in \neg Z$ such that $q'' \xrightarrow{\sigma} q'$. Hence $q' \notin Post(\neg Z,\sigma)$, so $q' \in \neg_{r_e} Post(\neg Z,\sigma)$. □

6.2 Symbolic reachability analysis

In this section we prove that reachability for CIRA is decidable. The idea is to syntactically restrict the expressions used in the symbolic implementation of the iterative reachability algorithm. If there are a finite number of expressions that can be generated, then the iterations must terminate.

The class of formulas that form a symbolic execution theory for rectangular automata are linear inequalities, denoted Ω. We define a *linear formula* to be the finite conjunction of linear inequalities. A linear formula defines a polyhedron in $\mathbb{R}^n$. The notation $\langle U \rangle$ refers to a (non-unique) set of formulas that generate a region U, and if ρ is a formula, then $[\rho]$ is the set of states that satisfy the formula. If $Z = \{l\} \times U$, a simple polyhedral zone, we abuse notation and also refer to a set of formulas that generate Z by $\langle Z \rangle$. For a polyhedral zone $Z = \cup_k \{l^k\} \times U^k$, $\langle Z \rangle$ denotes a disjunction of linear formulas ρ^k, such that each ρ^k generates the polyhedral region U^k.

Example 6.2.1. We will define two classes of formulas whose selection is motivated by a simple observation in $\mathbb{R}^2$. We assume the inclusion satisfies $a_i, b_i > 0, i = 1, 2$. Suppose an initial rectangular zone $Z = \{l\} \times U$ is defined by formulas $c_i \leq x_i \leq d_i$ where $c_i, d_i \in \mathbb{Z}$ and $i = 1, 2$. Then the zone $Pre(Z, t)$ is generated by formulas

$$\begin{aligned} x_i &\leq a_i^l \overline{\xi}_i \\ \frac{x_2}{a_2^l} - \frac{x_1}{b_1^l} &\leq \frac{d_2}{a_2^l} - \frac{c_1}{b_1^l} \\ \frac{x_2}{b_2^l} - \frac{x_1}{a_1^l} &\geq \frac{c_2}{b_2^l} - \frac{d_1}{a_1^l}. \end{aligned}$$

where $\overline{\xi}_i = \frac{d_i}{a_i^l}$ and the formulas $x_i \geq c_i$ have been removed. The second equation defines an *upper envelope* for the region and the third equation is a *lower envelope*. This idea generalizes to higher dimensions and captures the essence of what is to follow.

Assumption 6.2.1. We will assume in what follows that $a_i, b_i > 0$ for $i = 1, \ldots, n$, in order to simplify the exposition. The other cases can be dealt with analogously so we defer the details.

6.2.1 Formulas on a Mesh

We restrict consideration to linear inequalities defined on a mesh of points lying in the union of the rectangular regions N_l. First, define the mesh interval Δ by

$$\frac{1}{\Delta} = LCM\{a_i^l, b_i^l \mid l \in L, 1 \leq i \leq n\}.$$

The mesh of points N on the invariant regions is given by

$$N = \{x \mid x_i = m_i \Delta, m_i \in \mathbb{Z}. x \in \cup_{l \in L} M_l\}.$$

The projection of N on the ith coordinate is

$$N_i = \{x_i \mid x \in N\}.$$

Also let

$$I = \{(i,j) \mid i = 1,\ldots,n,\ j = i+1,\ldots,n\}.$$

In what follows, we refer to a formula defining a region U as tight if the formula "touches" the region. That is, a linear inequality satisfied by all points of U is *tight* if a point of U satisfies the formula obtained by converting the linear inequality to equality.

6.2.2 Formulas for Pre

We define a class of formulas $\mathcal{S}_{pre}$ suitable for zones reached by Pre operations. A simple polyhedral zone $Z = \{l\} \times U$ is generated by formulas given by

$$b_k^l \eta_k \ \%_l \ x_k \ \%_l \ a_k^l \overline{\eta}_k \tag{6.2.1}$$

$$\frac{x_j}{a_j^l} - \frac{x_i}{b_i^l} \ \%_l \ \frac{\overline{\xi}_{ji}}{a_j^l} - \frac{\xi_{ij}}{b_i^l} \tag{6.2.2}$$

$$\frac{x_j}{b_j^l} - \frac{x_i}{a_i^l} \ \%_g \ \frac{\xi_{ji}}{b_j^l} - \frac{\overline{\xi}_{ij}}{a_i^l} \tag{6.2.3}$$

where $\%_l = \{\leq, <\}$ and $\%_g = \{\geq, >\}$. Equation (6.2.1) defines $2n$ tight rectangular constraints, where $k = 1,\ldots,n$, and $\eta_k, \overline{\eta}_k \in N_k$. Equations (6.2.2)-(6.2.3) define $n(n-1)$ tight envelope constraints for Pre, where $\frac{\overline{\xi}_{ij}}{a_i^l}, \frac{\xi_{ij}}{b_i^l} \in N_i$ and $\frac{\overline{\xi}_{ji}}{a_j^l}, \frac{\xi_{ji}}{b_j^l} \in N_j$. $\tilde{\mathcal{S}}_{pre}$ is the class of formulas defined by taking the conjunction of the $n(n+1)$ formulas (6.2.1)-(6.2.3). No formulas can be excluded (even if they are redundant) and all formulas are tight.

We define $\mathcal{S}_{pre}$ to be the class of formulas defined by taking finite disjunctions of formulas in $\tilde{\mathcal{S}}_{pre}$. In this manner, non-simple polyhedral zones are generated by $\mathcal{S}_{pre}$. Note that $\tilde{\mathcal{S}}_{pre} \subset \mathcal{S}_{pre}$.

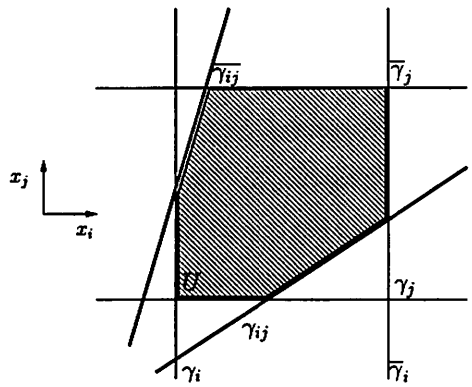

Figure 6.6: Formulas for Post.

6.2.3 Formulas for *Post*

We can define a class of expressions $\mathcal{S}_{post}$ suitable for zones reached by weak post operations. A simple polyhedral zone $Z = \{l\} \times U$ is generated by the formulas

$$a_k^l \eta_k \ \%_l \ x_k \ \%_l \ b_k^l \overline{\eta}_k \tag{6.2.4}$$

$$\frac{x_j}{b_j^l} - \frac{x_i}{a_i^l} \ \%_l \ \frac{\overline{\xi}_{ji}}{b_j^l} - \frac{\xi_{ij}}{a_i^l} \tag{6.2.5}$$

$$\frac{x_j}{a_j^l} - \frac{x_i}{b_i^l} \ \%_g \ \frac{\xi_{ji}}{a_j^l} - \frac{\overline{\xi}_{ij}}{b_i^l} \tag{6.2.6}$$

where $\%_l = \{\leq, <\}$ and $\%_g = \{\geq, >\}$. Equation (6.2.4) for $k = 1, \ldots, n$ defines $2n$ tight rectangular constraints, where $\eta_k, \overline{\eta}_k \in N_k$. Equations (6.2.5)-(6.2.6) define $n(n-1)$ tight envelope constraints for the weak post operation for rectangular inclusions, where $\frac{\overline{\xi}_{ij}}{b_i^l}, \frac{\xi_{ij}}{a_i^l} \in N_i$ and $\frac{\overline{\xi}_{ji}}{b_j^l}, \frac{\xi_{ji}}{a_j^l} \in N_j$. $\tilde{\mathcal{S}}_{post}$ is the class of formulas defined by taking the finite conjunction of the $n(n+1)$ formulas (6.2.4)-(6.2.6). No formulas can be excluded (even if they are redundant) and all formulas are tight.

We define $\mathcal{S}_{post}$ to be the class of formulas defined by taking all finite disjunctions of formulas in $\tilde{\mathcal{S}}_{post}$. In this manner, non-simple polyhedral zones are generated by $\mathcal{S}_{post}$.

We will adopt the following notation. $\overline{\gamma}_j(\gamma_j) \in \langle Z \rangle$ denote the upper (lower) rectangular constraint on component x_j and $\overline{\gamma}_{ij}(\gamma_{ij}) \in \langle Z \rangle$ denote the upper (lower) envelope constraint involving components x_j and x_i. See Figure 6.6.

Example 6.2.2. It is necessary to include all of the linear constraints in the appropriate

forms. Suppose the inclusion dynamics in location l are $\dot{x} \in [2,2], \dot{y} \in [5,7], \dot{z} \in [1,1]$. The initial zone $Z = \{l\} \times U$ is generated by formulas $z = 0 \ \wedge \ x \geq 0 \ \wedge \ x \leq 2 \ \wedge \ 7x = 2y$. Then $Post(Z,t)$ yields the formulas $7x \leq 2y + 4z \ \wedge \ 2y \leq 7x \ \wedge \ 2z \leq x \ \wedge \ x \leq 2z + 2$. The first formula in not in the class $\mathcal{S}_{post}$. The problem arises because region U does not have a valid lower constraint for the x, y pair: the formula $7x = 2y$ has the correct slope for an upper constraint, but cannot be used as a lower constraint. The situation is remedied by adding either a lower rectangular constraint or a lower envelope constraint.

Suppose we add a lower rectangular constraint so that U is generated by the formulas $z = 0 \ \wedge \ x \geq 0 \ \wedge \ x \leq 2 \ \wedge \ 2y \leq 7x \ \wedge y \geq 0$. Now $Post(Z,t)$ is generated by the formulas $x \geq 0 \ \wedge \ y \geq 0 \ \wedge \ z \geq 0 \ \wedge \ \frac{y}{7} - \frac{x}{2} \leq 0 \ \wedge \ \frac{y}{5} - \frac{x}{2} \geq -5 \ \wedge \ z - \frac{x}{2} \leq 0 \ \wedge \ z - \frac{x}{2} \geq -1 \ \wedge \ z - \frac{y}{5} \leq 0 \ \wedge \ z - \frac{y}{7} \geq -1$. Because the inclusion for x and z have the same lower and upper limits, some of these formulas are redundant. In general, however, they will be independent.

Alternately, suppose we add a lower envelope constraint so that U is generated by the formulas $z = 0 \ \wedge \ x \geq 0 \ \wedge \ x \leq 2 \ \wedge \ 2y \leq 7x \ \wedge 2y \geq 5x$. In this case, $Post(Z,t)$ is generated by the formulas $x \geq 0 \ \wedge \ y \geq 0 \ \wedge \ z \geq 0 \ \wedge \ \frac{y}{7} - \frac{x}{2} \leq 0 \ \wedge \ \frac{y}{5} - \frac{x}{2} \geq 0 \ \wedge \ z - \frac{x}{2} \leq 0 \ \wedge \ z - \frac{x}{2} \geq -1 \ \wedge \ z - \frac{y}{5} \leq 0 \ \wedge \ z - \frac{y}{7} \geq -1$.

Example 6.2.3. The requirement that the formulas are tight is essential. For example, suppose we have the inclusion $\dot{x}_1 = 1$, $\dot{x}_2 \in [1,2]$. Thus, $\Delta = \frac{1}{2}$. Suppose we have a region $U \subset \mathbb{R}^2$ generated by the formulas

$$\begin{aligned} 0 \leq x_1 &\leq 5 \\ \frac{1}{2} \leq x_2 &\leq 1 \\ \frac{x_2}{2} - x_1 &\leq 0 \\ x_2 - x_1 &\geq 0. \end{aligned}$$

$\langle U \rangle \notin \mathcal{S}_{post}$ because the constraint $x_1 \geq 0$ is not tight. The tight lower constraint is $x_1 \geq \frac{1}{4}$ obtained from $\frac{x_2}{2} - x_1 \leq 0$ and $x_2 \geq \frac{1}{2}$.

6.3 Transformations on Formulas

In this section we define transformations on the formulas defining simple polyhedral zones for *Post* operations. To minimize the notational overhead we use $\leq, \geq$ rather than $\%_l, \%_g$ in linear inequalities, but the proofs extend naturally when the latter syntax is substituted.

6.3.1 $Post(\cdot,\sigma)$ transformations

We give the transformation on *Post* formulas defining a simple polyhedral zone under the $Post(\cdot,\sigma)$ operator.

For $e \in E$, let I_e be the set of indices of components that are reset by r_e.

Lemma 6.3.1. *Given a simple, polyhedral zone $Z = \{l\} \times U$ and a simple integer-valued rectangular zone, $Y = \{l\} \times R$, if $\langle Z \rangle \in \mathcal{S}_{post}$, then $\langle Z \cap Y \rangle \in \mathcal{S}_{post}$.*

Proof. Let γ_i, $\overline{\gamma}_i$, γ_{ij}, and $\overline{\gamma}_{ij}$ be the formulas that generate Z and $x_i \in [c_i, d_i]$, $c_i, d_i \in \mathbb{Z}$ be the formulas that generate Y. $Z \cap Y$ is generated by the conjunction of these formulas. From this conjunction we must construct the new tight formulas and show that they belong to $\mathcal{S}_{post}$. First, we construct the tight rectangular constraints of the form $x_j \in [\alpha_j, \beta_j]$ where $\alpha_j, \beta_j \in \mathbb{R}$. Once the α_j's and β_j's are known, the tight upper envelope constraint is found by taking the tighter of $\overline{\gamma}_{ij}$ and

$$\frac{x_j}{b_j^l} - \frac{x_i}{a_i^l} \leq \frac{\beta_j}{b_j^l} - \frac{\alpha_i}{a_i^l}.$$

The tight lower envelope constraint is found by taking the tighter of γ_{ij} and

$$\frac{x_j}{a_j^l} - \frac{x_i}{b_i^l} \geq \frac{\alpha_j}{a_j^l} - \frac{\beta_i}{b_i^l}.$$

Claim: α_j and β_j, $j = 1, \ldots, n$ are computed by

$$\alpha_j = \max\left\{ c_j,\ a_j^l \eta_j,\ \max_{i \neq j}\left\{ \min_{\lambda \in \mathbb{R}}\{(\lambda, c_i) \models \gamma_{ij}\} \right\} \right\} \tag{6.3.1}$$

$$\beta_j = \min\left\{ d_j,\ b_j^l \overline{\eta}_j,\ \min_{i \neq j}\left\{ \max_{\lambda \in \mathbb{R}}\{(\lambda, d_i) \models \overline{\gamma}_{ij}\} \right\} \right\}. \tag{6.3.2}$$

The first formula is found be considering that α_j is determined by (1) γ_j, (2) $x_j \geq c_j$, and (3) the intersection of γ_{ij} and $x_i \geq c_i$ for all $i \neq j$. The second formula is found by considering that β_j is determined by (1) $\overline{\gamma}_j$, (2) $x_j \leq d_j$, and (3) the intersection of $\overline{\gamma}_{ij}$ and $x_i \leq d_i$ for all $i \neq j$.

Assuming the claim is true, we see that β_j takes the forms

$$\beta_j = \begin{cases} b_j^l \overline{\eta}_j \\ b_j^l \frac{d_j}{b_j^l} \\ b_j^l \left[\frac{\xi_{ji}}{b_j^l} - \frac{\xi_{ij}}{a_i^l} + \frac{d_i}{a_i^l} \right] \end{cases} \tag{6.3.3}$$

while α_j takes the forms

$$\alpha_j = \begin{cases} a_j^l \eta_j \\ a_j^l \frac{c_j}{a_j^l} \\ a_j^l [\frac{\xi_{ji}}{a_j^l} - \frac{\overline{\xi}_{ij}}{b_i^l} + \frac{c_i}{b_i^l}]. \end{cases} \tag{6.3.4}$$

Now we observe that $\frac{c_j}{a_j^l} \in N_j$ since $c_j \in \mathbb{Z}$, $\eta_j \in N_j$ by assumption, and $\frac{\xi_{ji}}{a_j^l} - \frac{\overline{\xi}_{ij}}{b_i^l} + \frac{c_i}{b_i^l} \in N_j$ since $c_i \in \mathbb{Z}$. The same observations show that $\frac{\alpha_j}{a_j^l} \in N_j$. Making analogous observations for β_j we obtain $\langle Z \cap Y \rangle \in \mathcal{S}_{post}$.

It remains only to prove the claim. Let W be the region generated by the transformed formulas. Let $(l, x) \in W$. A quick check confirms that x satisfies the conjunction of formulas $\langle Z \cap Y \rangle$. Conversely, let $(l, x) \in Z \cap Y$. Suppose $(l, x) \notin W$. One can enumerate the possible conjunctions of formulas violated by x to arrive at the required contradiction. □

In light of Lemma 6.3.1, when taking $Post(Z, \sigma)$ on edge $e = (l, l')$, where $Z = \{l\} \times U$ and $U \cap g_e \neq \emptyset$, it suffices to consider $Post(Z', \sigma)$, where $Z' = \{l\} \times U'$ and $U' \subseteq g_e$.

Lemma 6.3.2. *Given a CIRA H and a simple, polyhedral zone $Z = \{l\} \times U$ with $\langle Z \rangle \in \mathcal{S}_{post}$, suppose H has an edge $e = (l, l'), obs(e) = \sigma$ such that $U \subseteq g_e$. Then $\langle Post(Z, \sigma) \rangle = \mathcal{T}\langle Z \rangle$, where $\mathcal{T} : \mathcal{S}_{post} \to \Omega$ is a transformation on formulas consisting of the following steps:*

1. *for each $i \in I_e$, replace $\overline{\gamma}_i$, and γ_i by $x_i \in [r_i, s_i]$.*

2. *for each $(i, j) \in I$, $i, j \in I_e$, remove $\overline{\gamma}_{ij}$ and γ_{ij} and add the (tight) envelope constraints*

$$\frac{x_j}{b_j^{l'}} - \frac{x_i}{a_i^{l'}} \quad \%_l \quad \frac{s_j}{b_j^{l'}} - \frac{r_i}{a_i^{l'}} \tag{6.3.5}$$

$$\frac{x_j}{a_j^{l'}} - \frac{x_i}{b_i^{l'}} \quad \%_g \quad \frac{r_j}{a_j^{l'}} - \frac{s_i}{b_i^{l'}}. \tag{6.3.6}$$

3. *for each $(i, j) \in I$, $i, j \notin I_e$ retain the tight constraints $\overline{\gamma}_{ij}$ and γ_{ij}.*

4. *for each $(i, j) \in I$ such that $j \notin I_e$ and $i \in I_e$, remove $\overline{\gamma}_{ij}$ and γ_{ij}, retain the constraints $\overline{\gamma}_j$, γ_j, and add tight envelope constraints*

$$\frac{x_j}{b_j^l} - \frac{x_i}{a_i^l} \quad \%_l \quad \frac{b_j^l \overline{\eta}_j}{b_j^{l'}} - \frac{r_i}{a_i^l} \tag{6.3.7}$$

$$\frac{x_j}{a_j^l} - \frac{x_i}{b_i^l} \quad \%_g \quad \frac{a_j^l \eta_j}{a_j^{l'}} - \frac{s_i}{b_i^l}. \tag{6.3.8}$$

Proof. We will show that $q \in Post(Z,\sigma)$ implies $q \in [\mathcal{T}\langle Z\rangle]$, $q \in Post_s(\neg Z,\sigma)$ implies $q \in \neg_{r_e}[\mathcal{T}\langle Z\rangle]$, and finally observe that $Post_s(\neg Z,\sigma) \subseteq \neg_{r_e}[\mathcal{T}\langle Z\rangle] \iff [\mathcal{T}\langle Z\rangle] \subseteq Post(Z,\sigma)$. Observe that $\mathcal{T}\langle Z\rangle$ consists of the formulas:

a. $x_i \in [r_i, s_i]$, $i \in I_e$,

b. $\overline{\gamma}_{ij}$, γ_{ij}, $i,j \notin I_e$.

c. $\overline{\gamma}_j$, γ_j, $j \notin I_e$

where we have not included the redundant envelope constraints. Then $\neg_{r_e}[\mathcal{T}\langle Z\rangle]$ is generated by the formulas

sa. $x \in r_e(g_e)$,

sb. $(\neg\overline{\gamma}_j, j \notin I_e) \quad \vee \quad (\neg\gamma_j, j \notin I_e) \quad \vee \quad (\neg\gamma_{ij}, i,j \notin I_e) \quad \vee \quad (\neg\overline{\gamma}_{ij}, i,j \notin I_e)$,

again omitting redundant envelope constraints.

Let $(l',y) \in Post(Z,\sigma)$, i.e. $\exists\, x \in U$ such that $y \in r_e(x)$. We will show that $(l',y) \in [\mathcal{T}\langle Z\rangle]$. Since $y \in r_e(x)$ formulas *a.* are satisfied. Formulas *b.* are satisfied because $y_i = x_i$, $y_j = x_j$ for $i,j \notin I_e$ and $(x_i,x_j) \models \gamma_{ij}, \overline{\gamma}_{ij}$, for $x \in U$. Considering formulas *c.*, $x \in U$ and $y_j = x_j$, so $y_j \models \overline{\gamma}_j, \gamma_j$.

Next, let $(l',y) \in Post_s(\neg Z,\sigma)$. Call $Y = \neg_{r_e}[\mathcal{T}\langle Z\rangle]$. We will show $(l',y) \in Y$. By definition of $Post_s$, for all $x \in g_e$ such that $y \in r_e(x)$, $x \in \neg U$. Since $y \in r_e(x)$, formulas *sa.* are satisfied. Since $x \in \neg U$ either

1. $x_j = y_j \models \neg\gamma_j$ or $x_j = y_j \models \neg\overline{\gamma}_j$, for $j \notin I_e$, implying $y \in Y$; or
2. $(x_i,x_j) \models \neg\overline{\gamma}_{ij}$ or $(x_i,x_j) \models \neg\gamma_{ij}$, for $i,j \notin I_e$, but $y_j = x_j$, $y_i = x_i$ implies $y \in Y$; or
3. $(x_i,x_j) \models \neg\gamma_{ij}(\overline{\gamma}_{ij})$ for $i \in I_e$, $j \notin I_e$ and no other formulas of U are violated by x (for if one is, to go its case). Then $y_j = x_j \models \neg\gamma_j(\neg\overline{\gamma}_j)$, implying $y \in Y$. For suppose not. Then there exists x' with $x'_k = x_k$, $k \neq i$ and $x'_i \in [a^l_i\eta_i, b^l_i\overline{\eta}_i]$ such that $x' \in U$. Then $y \in r_e(x) = r_e(x')$, contradicting $y \in Post_s(\neg Z,\sigma)$; or
4. $(x_i,x_j) \models \neg\gamma_{ij}$, for $i,j \in I_e$. Let $x'_k = x_k$ for $k \neq i,j$. Then for all $x'_i \in [c_i,d_i]$, $x'_j \in [c_j,d_j]$ $y \in r_e(x')$ and since $y \in Post_s(\neg Z,\sigma)$, $g_e \subseteq \neg U$. This contradicts the

assumption that $U \subseteq g_e$. A similar contradiction is reached for $\neg\overline{\gamma}_{ij}$, $i,j \in I_e$. Thus, these last two cases do not arise.

□

6.3.2 $Post(\cdot,t)$ transformations

We give the transformation on *Post* formulas defining a simple polyhedral zone under the $Post(\cdot,t)$ operator. This requires some convexity properties of the post sets of a rectangular inclusion.

Let U be a non-empty convex set in $\mathbb{R}^n$. U *recedes* in direction $y \neq 0$, iff $x + \lambda y \in U$, for every $\lambda \geq 0$, $x \in U$. The set of all such y's is called the *recession cone* of U, denoted $O^+(U)$.

Theorem 6.3.3 (Rockafellar [84]). *Let U be a non-empty convex set. The recession cone $O^+(U)$ is a convex cone containing the origin, and given by*

$$O^+(U) = \{y \mid U + y \subset U\}.$$

Lemma 6.3.4. *Suppose a non-empty convex set U is the set of solutions to a system of linear inequalities on $\mathbb{R}^n$:*

$$U = \{x \mid Ax \geq b\}.$$

Then

$$O^+(U) = \{x \mid Ax \geq 0\}.$$

Proof. Suppose y is such that $U + y \subseteq U$. Then for all $x \in U$, $Ax \geq b$ and $A(x+y) \geq b$. In particular, there exists x such that $Ax = b$, from which it follows $Ay \geq 0$. Conversely, suppose y is such that $Ay \geq 0$. Then for all $x \in U$, $A(x+y) = Ax + Ay \geq b$, implying $x + y \in U$, or $U + y \subseteq U$. □

Lemma 6.3.5. *Given a constant, convex inclusion $\dot{x} \in F$, and a convex zone $Z = \{l\} \times U$, $Post(Z,t)$ is convex.*

Proof. Let $x, y \in Post(Z,t)$. Then there exists $x_0, y_0 \in U$ and $s_1, t_1 \in \mathbb{R}^+$ such that

$$x(s) = x_0 + \int_0^s \dot{x}(\tau)d\tau \qquad x(s_1) = x,$$

$$y(t) = y_0 + \int_0^t \dot{y}(\tau)d\tau \qquad x(t_1) = y$$

and s and t are related by $s = \frac{s_1}{t_1}t$. Let $z(u)$ be the convex combination of $x(s)$ and $y(t)$

$$z(u) = (1-\theta)x(s) + \theta y(t)$$

where u is a time defined by

$$u = (1-\theta)s + \theta t$$

and $u_1 = (1-\theta)s_1 + \theta t_1$. Thus,

$$z(u) = (1-\theta)x\Big(\frac{s_1}{(1-\theta)s_1 + \theta t_1}u\Big) + \theta y\Big(\frac{t_1}{(1-\theta)s_1 + \theta t_1}u\Big).$$

Then

$$\begin{aligned} z(u_1) &= (1-\theta)x_0 + \theta y_0 + \\ &\int_0^{u_1}\Big[(1-\theta)\dot{x}(s(u))\cdot\Big(\frac{s_1}{(1-\theta)s_1+\theta t_1}\Big) + \theta\dot{y}(t(u))\cdot\Big(\frac{t_1}{(1-\theta)s_1+\theta t_1}\Big)\Big]du. \end{aligned}$$

Since U is convex $z_0 = (1-\theta)x_0 + \theta y_0 \in U$. Let $\gamma = \frac{\theta t_1}{(1-\theta)s_1+\theta t_1}$. Then

$$z(u_1) = z_0 + \int_0^{u_1}\Big[(1-\gamma)\dot{x}(s(u)) + \gamma\dot{y}(t(u))\Big]du.$$

By convexity of F, $z(u_1) \in Post(Z,t)$. Therefore, $Post(Z,t)$ is convex. □

Given a region U, $x \in U$ is an *extreme point* of U if x is not an interior point of any line segment in U.

Lemma 6.3.6. *Given a constant, convex inclusion $\dot{x} \in F$ and a convex region $Z = \{l\} \times U$, the extreme points of $Post(Z,t)$ are reached from extreme points of U by extreme trajectories only.*

Proof. Let $x_0 \in U$ be a non-extreme point of U (if no such x_0 exists then we proceed to examining extreme and non-extreme trajectories below). Suppose $\phi_t(x_0)$ is a trajectory of $\dot{x} \in F$ starting from x_0. We can write $x_0 = \sum_{i=1}^{m}\lambda u_i$ where $\sum_i \lambda_i = 1$, $\lambda_i < 1$ and $u_1, \ldots, u_m$ are extreme points of U. Define trajectories $\phi_t(u_i)$, starting from u_i such that $\dot{\phi}_t(u_i) = \dot{\phi}_t(x_0), \forall t > 0$. Then,

$$\begin{aligned} \phi_t(x_0) &= x_0 + \int_0^t \dot{\phi}_s(x_0)ds \\ &= \sum_i \lambda_i\Big[u_i + \int_0^t \dot{\phi}_s(u_i)ds\Big] \\ &= \sum_i \lambda_i\phi_t(u_i). \end{aligned}$$

Therefore, $\phi_t(x_0)$ cannot reach an extreme point of $Post(Z,t)$.

Next, suppose that $\dot{\phi}_s(x_0)$ is non-extreme on an interval $[0,t]$. We can write

$$\dot{\phi}_s(x_0) = \sum_{i=1}^{q} \lambda_i(s) f_i$$

where $f_1, \ldots, f_q$ are extreme points of F and $\sum_i \lambda_i(s) = 1$, $\lambda_i < 1$ for all $s \in [0,t]$. Let

$$\overline{\lambda}_i = \frac{1}{t} \int_0^t \lambda_i(s) ds$$

and observe that $\sum_i \overline{\lambda}_i = 1$. Then,

$$\begin{aligned} \phi_t(x_0) &= x_0 + \int_0^t \dot{\phi}_s(x_0) ds \\ &= \sum_{i=1}^{q} \overline{\lambda}_i \Big[x_0 + \int_0^t f_i ds \Big]. \end{aligned}$$

Thus, $\phi_t(x_0)$ is a non-extreme point, and by the previous argument, cannot reach an extreme point. Therefore, trajectories with non-extreme rates cannot reach extreme points. □

The following lemma relies on the fact that all formulas of (6.2.4)-(6.2.6) appear in $\langle Z \rangle$ for a simple polyhedral zone Z. In particular, redundant formulas (6.2.5)-(6.2.6) are included in $\langle Z \rangle$ even if Z is rectangular.

Lemma 6.3.7. *Given a simple, polyhedral zone $Z = \{l\} \times U$ with $\langle Z \rangle \in \mathcal{S}_{post}$, $\langle Post(Z,t) \rangle = \mathcal{T}\langle Z \rangle$, where $\mathcal{T} : \mathcal{S}_{post} \to \Omega$ is a transformation on formulas consisting of the step: remove $\overline{\gamma}_k$, $k = 1, \ldots, n$.*

Proof. Let $Y = [\mathcal{T}\langle Z \rangle]$ and $\langle Y \rangle = \mathcal{T}\langle Z \rangle$. First we show that $Post(Z,t) \subseteq \{l\} \times Y$. Let $(l,y) \in Post(Z,t)$. First, observe that the lower rectangular constraints (6.2.4) are satisfied by y, since the derivative of each component is positive $(l,y) \in Post(Z,t)$ implies there exists $x \in U$ and a trajectory $\phi_t(x)$ such that for some $\tau \geq 0$, $y = \phi_\tau(x)$ and the components of y satisfy

$$\begin{aligned} y_j \quad &\%_l \quad b_j^l \tau + x_j \\ y_j \quad &\%_g \quad a_j^l \tau + x_j \end{aligned}$$

for $j = 1, \ldots, n$. Taking any (i,j) pair and combining these relations we find

$$\frac{y_j}{b_j^l} - \frac{y_i}{a_i^l} \%_l \frac{x_j}{b_j^l} - \frac{x_i}{a_i^l}$$

and similarly for the lower envelope constraint. Thus, formulas (6.2.5)-(6.2.6) are satisfied by y, so $y \in Y$.

Next we must show $\{l\} \times Y \subseteq Post(Z,t)$. Consider $x \in U$. Since $x \in Y$, for any $v \in O^+(Y)$, we have $x + v \in Y$. By Lemma 6.3.4 v satisfies

$$\frac{v_j}{b_j^l} - \frac{v_i}{a_i^l} \quad \%_l \quad 0 \tag{6.3.9}$$

$$\frac{v_j}{a_j^l} - \frac{v_i}{b_i^l} \quad \%_g \quad 0. \tag{6.3.10}$$

Let $ex(O^+(Y)) = \{v \in O^+(Y) \mid v_i = \{a_i^l, b_i^l, i = 1,2\}\}$, the extreme rates of $O^+(Y)$. Taking any $w \in ex(U)$, and $v \in ex(O^+(Y))$, we have $y = w + \lambda v \in Y$, $\lambda \in \mathbb{R}^+$. From Lemma 6.3.6 we know that the extreme rays of the region defined by $Post(Z,t)$ are reached from extreme points of U using extreme rates. Thus, y is an extreme ray of (the region) $Post(Z,t)$, implying $(l,y) \in Post(Z,t)$. Since y is an arbitrary extreme ray of Y and the region defined by $Post(Z,t)$, and Y and $Post(Z,t)$ are convex by Lemma 6.3.5, the result follows. □

6.3.3 $\mathcal{S}_{post}$ closed under *Post*

The main result we will need to show that reachability is decidable is that $\mathcal{S}_{post}$ is closed under *Post*.

Lemma 6.3.8. *Given simple polyhedral zone Z, if $\langle Z \rangle \in \mathcal{S}_{post}$, then $\langle Post(Z,\sigma) \rangle \in \mathcal{S}_{post}$.*

Proof. Considering each of the steps in Lemma 6.3.2 we observe that Step 1 and Step 2 constraints belong to $\mathcal{S}_{post}$ because $r_i, s_i \in \mathbb{Z}$. Step 3 constraints belong to $\mathcal{S}_{post}$ automatically. Finally, Step 4 constraints belong to $\mathcal{S}_{post}$ since $a_j^{l'} = a_j^l$, $b_j^{l'} = b_j^l$ for $j \notin I_e$. It follows that $\langle Post(Z,\sigma) \rangle \in \mathcal{S}_{post}$. □

Lemma 6.3.9. *Given simple polyhedral zone Z, if $\langle Z \rangle \in \mathcal{S}_{post}$, then $\langle Post(Z,t) \rangle \in \mathcal{S}_{post}$.*

Proof. From Lemma 6.3.7, $Post(Z,t)$ can be computed by replacing the existing upper rectangular constraints with those defining M_l. We are finished, since the removal of rectangular constraints and intersection with an integer-valued rectangular region was shown in Lemma 6.3.1 not to affect membership in $\mathcal{S}_{post}$. □

Lemma 6.3.10. *Given a non-simple polyhedral zone Z, if $\langle Z \rangle \in \mathcal{S}_{post}$, then $\langle Post(Z, \sigma) \rangle \in \mathcal{S}_{post}$.*

Proof. Every non-simple polyhedral zone Z can be written as $Z = \cup_k Z_k$, where Z_k is a simple polyhedral zone. Then use $Post(Z, \sigma) = \bigcup_k Post(Z_k, \sigma)$, and Lemma 6.3.8. □

Lemma 6.3.11. *Given a non-simple polyhedral zone Z, if $\langle Z \rangle \in \mathcal{S}_{post}$, then $\langle Post(Z, t) \rangle \in \mathcal{S}_{post}$.*

Theorem 6.3.12 (Reachability). *Reachability is decidable for CIRA.*

Proof. The initial (rectangular) region is generated by formulas of $\mathcal{S}_{post}$. Using Lemmas 6.3.8-6.3.9, every step of the reachability analysis generates formulas in $\mathcal{S}_{post}$. Since there are a finite number of formulas in $\mathcal{S}_{post}$, the reachability analysis terminates in a finite number of iterations. □

Chapter 7

Conclusion

And the end of all our exploring
Will be to arrive where we started
And know the place for the first time.
- T.S. Eliot.

In this chapter we say our final words. Mainly we try to convey our excitement about what lies ahead for hybrid systems in the form of new frontiers where hybrid systems can make a difference and questions about hybrid systems that are unresolved. First, we must mention two ominous threats.

Ominous threats

No work has appeared giving an indication of the performance we can expect from model checking of hybrid systems. Will the performance be as explosive as in hardware verification? An analysis of the complexity of the algorithms combined with experiments with real models needs to be done to ensure that exhaustive searches of hybrid state spaces are practically feasible.

There has been theoretical work on hybrid systems and important application domains we discussed in the introduction. There still is a gap between these two worlds, and this gap needs to be filled in the near future. This can best be achieved by developing software tools.

Implementation and Applications

We presented a new methodology for model checking of hybrid systems under natural compatibility conditions of the enabling and reset conditions. We have entered a brave new world for model checking, and it is imperative that we carry through to software implementation and applications before we can claim that the paradigm-shifts that motivated the

research were meaningful.

Because model checking based on bisimulation is not a numerical black-box approach, the best way to demonstrate it's potential impact is to select an application area that has a pre-existing need for the hybrid systems framework. Coordinated autonomous agent problems and embedded systems are the two strongest candidates. We desire a model checking tool based on bisimulation that handles a suite of reachability and controller synthesis problems that are currently not solvable using simulation-based methods. At that point we could certainly argue that the effort has been worthwhile. Fortunately, this goal has moved beyond the state of wishful thinking.

Also because model checking as proposed here is not a black-box approach, we are interested in developing black box approaches that do not necessarily rely on bisimulation. Indeed, the basic idea is to form a *cover* rather than a partition of the hybrid state space.

Theory

As well as attention to implementation and applications, we have seen over the course of the thesis specific theoretical and practical questions that reach out to be solved. Let us review those questions.

In Chapter 2 we presented a local geometric theory of bisimulation. Perhaps it could be argued that this theory was not so local, and we showed examples where indeed the bisimulation partition was global. But we are left with a need to know when is the partition local in the assumed sense and when is it global, and how can the domain of a partition be expanded, even by some *inspired adhoccery*, if need be. These questions lead to several promising research avenues.

We plan to study global bisimulations arising from systems with symmetries. We also know that reductions of quotient systems are obtained from group symmetries at the automaton level [33, Ch. 14]. It is natural to try to see how these symmetries are related, whether they can be understood within a unified mathematical framework, and what benefits do we get from such a bird's eye view. A second approach to global bisimulation is to study particular classes of vector fields such as Morse-Smale systems. An understanding of which vector fields admit finite bisimulations will give new insight to both continuous and hybrid dynamics, and we hope that this will lead to a cascade of small revelations.

In Chapter 5 we defined a hybrid optimal synthesis problem, but this problem was not

directly solved. This problem needs to be readdressed in a separate investigate on hybrid optimal synthesis problems. We examined Zeno behavior in Fuller's problem. The synthesis of controls in the presence of Zeno phenomena requires further exploration which should be tied into the older work on regular synthesis in optimal control.

In Chapter 6 we studied decidability of reachability for initialized rectangular automata. The next question to be explored using the same proof method is decidability of safety controller synthesis for rectangular automata.

Beneficiaries

So much effort in control theory has been placed on extracting precise models and developing (sometimes computationally intractible) algorithms to modify a limited set of features of those models. Control theory may work too hard at producing models which must then be whittled down to some familiar form so that anything can be done. Witness the success of fuzzy logic and one realizes that one can go very far with simpler models and a greater emphasis on efficient algorithmic solutions.

Hybrid automata provide a framework in which more of the "burden of control" can be placed at the logic level, for the performance of model checking is relatively unaffected by the number of states of the automaton. We are lead to envision a new research direction based on hybrid systems: *logic synthesis for control.*

Appendix A

Differential Inclusions

In this chapter we review some necessary background on differential inclusions used in Chapter 2. We follow closely [8] but also present some results from [41].

A.1 Set-valued maps

Let X and Y be two Hausdorff topological spaces. A set valued map F from X to Y is a map that associates with any $x \in X$ a subset $F(x)$ of Y. The domain of F is $Dom(F) := \{x \in X \mid F(x) \neq \emptyset\}$. The range of F is $Range(F) := \bigcup_{x \in X} F(x)$. A set-valued map is compact (bounded) if its range is compact (bounded). We say that a map F is *locally compact* if for each point in $Dom(F)$, there exists a neighborhood which is mapped into a compact subset. The *graph* of F is $Graph(F) := \{(x, y) \in X \times Y \mid y \in F(x)\}$. We say that F is *upper semicontinuous* (u.s.c.) at $x \in X$ if for any open N such that $F(x) \subset N$, there exists a neighborhood of x, M such that $F(M) \subset N$.

Proposition A.1.1. *The graph of an u.s.c. set-valued map with closed values from X to Y is closed.*

We say that F is *lower semicontinuous* (l.s.c.) at $x \in X$ if for any $y \in F(x)$ and any neighborhood $N(y)$ of y, there exists a neighborhood $N(x)$ of x such that $\forall x \in N(x)$ $F(x) \cap N(y) \neq \emptyset$. A set valued map F from X to Y is continuous at $x \in X$ if it is both u.s.c. and l.s.c. at x.

Let $B(S, r) := \{x \in X \mid d(x, S) \leq r\}$ be the ball of radius r around the subset S. We say

the set valued map $F : X \to Y$, (X, d_1) and (Y, d_2) are metric spaces, is *locally Lipschitz* if for any $x_0 \in X$, there exists a neighborhood $N(x_0) \subset X$ and a constant $L \geq 0$ such that $\forall\, x, x' \in N(x_0),\ F(x) \subset B(F(x'),\ Ld_1(x, x'))$. F is *Lipschitz* if there exists $L \geq 0$ such that $\forall\, x, x' \in X,\ F(x) \subset B(F(x'),\ Ld_1(x, x'))$.

A.2 The selection problem

Given a family of sets $\{F_\alpha : \alpha \in A\}$, a *selection* is a map $\alpha \to f_\alpha$ in F_α. We are interested in obtaining continuous selections of F, which need not always exist.

Example A.2.1. Consider the set valued map $F : \mathbb{R} \to \mathbb{R}$ given by

$$F(x) = \begin{cases} \{-1\} & x < 0 \\ [-1, 1] & x = 0 \\ \{1\} & x > 0 \end{cases}$$

This map does not have a continuous selection.

Example A.2.2. Consider $F : (-1, 1) \to \mathbb{R}^2$ given by

$$F(t) = \begin{cases} (cos\theta, tsin\theta) & \text{and } \frac{1}{t} \leq \theta \leq \frac{1}{t} + 2\pi - |t| \quad t \neq 0 \\ (x, y) & \text{and } -1 \leq x \leq 1, y = 0 \quad t = 0 \end{cases}$$

For $t \neq 0$, $F(t)$ is a subset of an ellipse in $\mathbb{R}^2$, whose small axis shrinks to zero as $t \to 0$, so that the ellipse collapses to a segment, $F(0)$. The subset of the ellipse given by $F(t)$ is obtained by removing from it a section, from the angle $\frac{1}{t} - |t|$ to the angle $\frac{1}{t}$. As t gets smaller, the arclength of this hole decreases while the initial angle increases as $\frac{1}{t}$, i.e. it spins around the origin with increasing angular speed. The map is Hausdorff continuous at the origin while any continuous selection $f(t)$ defined on $(-1, 0)$ or $(0, 1)$, such as $f(t) = (cos\frac{1}{t}, tsin\frac{1}{t})$ could not be continuously extended to $(-1, 1)$. The hole in the ellipse would force the selection to rotate around the origin with an angle between $\frac{1}{t}$ and $\frac{1}{t} + 2\pi - |t|$, so $\lim_{t \to 0} f(t)$ cannot exist.

Minimum Selection. The *minimum selection* is given by $m(x) = \min F(x)$, for which we have

Theorem A.2.1. *Let X be a metric space, Y a Hilbert space, and F, from X to the closed, convex subsets of Y, is continuous. Then the mapping $x \mapsto m(F(x))$ is a continuous selection from F.*

Barycentric Selection. Let X be a metric space and $F : X \to 2^{\mathbf{R}^n}$ be compact, convex-valued, Lipschitz, and globally bounded, i.e. there exists M such that $F(x) \subset MB, \forall x \in X$. Let $A \subset \mathbb{R}^n$ be a compact, convex set and m the Lebesgue measure. The barycenter of A is

$$b(A) = \frac{1}{m(A)} \int_A x dm.$$

One can show that $b(A) \in A$. To ensure the set has posiitive measure we also consider $b(A + B) \in A$. The *barycentric selection* of F is

$$f(x) = b(F(x) + B).$$

Theorem A.2.2. *f is Lipschitz continuous.*

Michael's Selection.

Theorem A.2.3. *Let X be a metric space, Y a Banach space. Let F from X into the closed convex subsets of Y be lower semicontinuous. Then there exists $f : X \to Y$, a continuous selection from F.*

A.3 Solutions of differential inclusions

Denote by $L^p(I, \mathbb{R}^n)$ the space of functions $f : [0, T] \to \mathbb{R}^n$ such that $\int_0^T |f|^p < \infty$. L^1 consists of the Lebesgue integrable functions on $[0, T]$. $L^\infty(I, \mathbb{R}^n)$ is the space of all bounded, measurable functions on $[0, T]$.

Consider the differential inclusion

$$\dot{x} \in F(t, x). \tag{A.3.1}$$

The selection theorems of the previous section give means to obtain existence of solutions of (A.3.1). If F is lower semicontinuous, with closed, convex values, we can apply Michael's Selection Theorem A.2.3 to obtain a continuous vector field which is a selection of F. For F continuous with closed, convex values, the minimal selection gives a continuous vector field

corresponding to "slow" solutions. For the case of upper semicontinuous maps with closed, convex values, it is possible to prove an analog of Peano's theorem for ordinary differential equations. Other existence results also exist. See [8, Ch 2].

The following two results are useful when working with sequences of solutions of a differential inclusion.

Lemma A.3.1. *[41, p. 78] Suppose that in a domain D F is nonempty, compact, convex-valued and upper-semicontinuous in t, x. Then the limit of a uniformly convergent sequence of solutions of* (A.3.1) *is a solution of the inclusion.*

Lemma A.3.2. *[41, p. 77] Suppose F satisfies the assumptions of the previous lemma in a compact domain D. Then all the solutions of* (A.3.1) *that lie in D are equicontinuous.*

A.3.1 Filippov theorem

Filippov's theorem [42] is the analog for differential inclusions of the Gronwall lemma and is used to construct continuous (w.r.t. the initial condition) selections of solutions of Lipschitz inclusions.

Theorem A.3.3. *Given the interval I, an absolutely continuous function $y : I \to \mathbb{R}^n$, and constant $\beta > 0$, define $Q = \{(t,x) : t \in I, |x - y(t)| \leq \beta\}$. For the differential inclusion*

$$\dot{x} \in F(t,x)\,, \qquad x(0) = x_0, \tag{A.3.2}$$

assume $F : Q \to 2^{\mathbb{R}^n}$ is non-empty, closed-valued, and continuous with Lipschitz constant $K(t) \in \mathcal{L}^1(I)$. Assume also that

$$|y(0) - x_0| = \delta \leq \beta,$$
$$d(\dot{y}(t), F(t, y(t))) \leq p(t)\,, \quad a.e.$$

with $p \in \mathcal{L}^1(I)$. Set

$$\xi(t) = \delta e^{\int_0^t K(s)ds} + \int_0^t e^{\int_s^t K(u)du} p(s)ds\,.$$

Let $J \subseteq I$, nonempty such that $t \in J$ implies $\xi(t) \leq \beta$. Then there exists a solution x on J of (A.3.2) *such that*

$$|x(t) - y(t)| \leq \xi(t)$$

and

$$|\dot{x}(t) - \dot{y}(t)| \leq K(t)\xi(t) + p(t)\,, \quad a.e.$$

Remark A.3.1. If $y(t)$ is a solution of (A.3.2), with $y(0) = y_0$ and $K(t) \equiv K$, a constant, then there exists a solution x of (A.3.2) with $x(0) = x_0$ and

$$|x(t) - y(t)| \leq |x_0 - y_0|e^{Kt}. \tag{A.3.3}$$

A.4 Continuous selections of Filippov solutions

In this section we give a condensed version of the results obtained in [30] providing continuous selections of solutions of differential inclusions. The result refines the proof of the Filippov theorem to obtain continuity in the initial condition.

Consider the problem

$$\dot{x} \in F(t,x), \qquad x(0) = \xi\,, \tag{A.4.1}$$

on a time interval $I = [0,T]$, where ξ ranges over a compact $X_0 \subset \mathbb{R}^n$ with diameter D. In addition, we assume the following.

Assumption A.4.1. The set-valued map F satisfies:

(a) The values of F are compact, nonempty subsets of $\mathbb{R}^n$.

(b) there exists $K \in \mathbb{R}$ such that $d_H(F(x), F(x')) \leq K|x - x'|$, for all $x, x' \in \mathbb{R}^n$.

(c) $t \mapsto F(t,x)$ is measurable.

Under Assumption 2.4.1, an absolutely continuous solution to (A.4.1) exists for each $\xi \in X_0$ [41].

Theorem A.4.1. *Suppose F satisfies Assumption A.4.1. Let $\xi_0 \in X_0$ and $x(t)$ be a solution of* (A.4.1) *such that $x(0) = \xi_0$. Then there exists a continuous $\psi : X_0 \to AC$, a selection of solutions of* (A.4.1) *such that $\psi_t(\xi_0) = x(t)$.*

To prove the theorem we need the following proposition from [30].

Proposition A.4.2. *Let $v_0, \ldots v_q$ be in $\mathcal{L}^1$, and let $\{I_i(\xi)\}$ be a partition of I into a finite*

number of subintervals with endpoints depending continuously on ξ. Consider the map

$$\varphi : \xi \mapsto \xi + \int_0^t \sum_{i=0}^{q} \chi_{I_i(\xi)}(s) v_i(s) ds.$$

Then there exists $\alpha \in \mathcal{L}^1(I)$ such that for every $\epsilon > 0$ there exists $\delta > 0$ such that

$$|\xi' - \xi| < \delta \text{ implies } |\dot{\varphi}_t(\xi') - \dot{\varphi}_t(\xi)| \leq \alpha(t)\chi_E(t),$$

for some set E with measure $(E) \leq \epsilon$.

Theorem A.4.1 follows from the following result in [30]. We present the relevant parts of the proof.

Theorem A.4.3. *Suppose F satisfies Assumption A.4.1. Then there exists a sequence $\{y^j\}$ of approximate solutions of* (A.4.1) *which satisfy, at the jth iteration*
(i)

$$\int_0^t |\dot{y}_s^j(\xi) - \dot{y}_s^{j-1}(\xi)| ds \leq D\Big[\frac{(Kt)^j}{j!} + 2^{-j-1}\Big[2^{-2} + \sum_{i=1}^{j} \frac{(2Kt)^i}{i!}\Big]\Big], \tag{A.4.2}$$

(ii)

$$d[\dot{y}_t^j(\xi), F(t, y_t^{j-1}(\xi))] \leq KD2^{-j-2},$$

(iii)

$$d[\dot{y}_t^j(\xi), F(t, y_t^j(\xi))] \leq KD\Big[\frac{(Kt)^j}{j!} + 2^{-j-1} \sum_{i=0}^{j} \frac{(2Kt)^i}{i!}\Big]$$

(iv) there exists α^j in $\mathcal{L}^1$ such that for every $\epsilon > 0$, there exists $\delta > 0$ such that $|\xi - \xi'| < \delta$ implies

$$|\dot{y}_t^j(\xi') - \dot{y}_t^j(\xi)| \leq \alpha^j(t)\chi_E(t)$$

for some $E \subset I$ with measure$(E) \leq \epsilon$.

Proof. The proof is by induction on j.

We first show (i)-(iv) hold for $j = 1$. Define a cover $B(\xi, \delta^0(\xi))$ of X^0. Let $\{B(\xi_i^0, \delta^0(\xi_i^0))\}_{i=1}^{n^0}$ be a finite subcover where $\delta(\xi) \leq \min\{D2^{-3}, |\xi - \xi_0|/2\}$. Define a partition of $I = [0, T]$ by $\{I_i^0(\xi)\}_{i=1}^{n^0}$ where

$$I_i^0(\xi) = [T \sum_{i=1}^{i-1} \psi_i^0(\xi), T \sum_{i=1}^{i} \psi_i^0(\xi)] \tag{A.4.3}$$

and $\{\psi_i^0\}$ is a partition of unity subordinate to $\{B(\xi_i^0, \delta^0(\xi_i^0))\}_{i=1}^{n^0}$.

Now define the initial guesses

$$y_t^0(\xi) := \xi + \int_0^t \dot{x}(s)ds \tag{A.4.4}$$

$$y_t^1(\xi) := \xi + \int_0^t \sum_{i=1}^{n^0} \chi_{I_i^0(\xi)}(s) v_s^0(\xi_i^0) ds \tag{A.4.5}$$

where $v_t^0(\xi) \in F(t, y_t^0(\xi))$ is a measurable selection such that

$$|\dot{y}_t^0(\xi) - v_t^0(\xi)| = d[y_t^0(\xi), F(t, y_t^0(\xi))] \leq K|\xi - \xi_0|.$$

Then we have

$$\begin{aligned}
\int_0^t |\dot{y}_s^1(\xi) - \dot{y}_s^0(\xi)|ds &\leq \int_0^t \sum_{i=1}^{n^0} |v_s^0(\xi_i^0) - \dot{x}(s)|ds \\
&\leq \int_0^t \sum_{i=1}^{n^0} \chi_{I_i^0(\xi)} K|\xi_i^0 - \xi_0|ds \\
&\leq DKt.
\end{aligned}$$

This proves (i). Fix t and let i be such that $t \in I_i^0(\xi)$. Then we have

$$\begin{aligned}
d[\dot{y}_t^1(\xi), F(t, y_t^0(\xi))] &= d[v_t^0(\xi_i^0), F(t, y_t^0(\xi))] \\
&\leq d_H[F(t, y_t^0(\xi_i^0)), F(t, y_t^0(\xi))] \\
&\leq K|\xi_i^0 - \xi| \\
&\leq KD2^{-3}.
\end{aligned}$$

This proves (ii). Also,

$$\begin{aligned}
d[\dot{y}_t^1(\xi), F(t, y_t^1(\xi))] &\leq d[\dot{y}_t^1(\xi), F(t, y_t^0(\xi))] + d_H[F(t, y_t^0(\xi)), F(t, y_t^1(\xi))] \\
&\leq K\frac{D}{2^3} + KDKt \\
&\leq KD\big[Kt + 2^{-1}[1 + 2Kt]\big].
\end{aligned}$$

This proves (iii).

Next we assume (i)-(iv) hold for $j-1$, and show they hold for j. Choose $v_t^{j-1}(\xi) \in F(t, y_t^{j-1}(\xi))$ such that

$$\begin{aligned}
|\dot{y}_t^{j-1}(\xi) - v_t^{j-1}(\xi)| &= d[\dot{y}_t^{j-1}(\xi), F(t, y_t^{j-1}(\xi))] \\
&\leq DK\Big[\frac{(Kt)^{j-1}}{(j-1)!} + 2^{-j}\sum_{i=0}^{j-1}\frac{(2Kt)^i}{i!}\Big].
\end{aligned}$$

By (iv) of the recursive hypothesis there exists $\delta^j > 0$ such that $|\xi' - \xi| < \delta^j$ implies

$$|\dot{y}_t^{j-1}(\xi') - \dot{y}_t^{j-1}(\xi)| \leq \alpha^{j-1}(t)\chi_E(t)$$

for some $E \subset I$ such that $\int_E \alpha^{j-1}(t)dt \leq KD2^{-j-3}$. Let $\delta^j(\xi) = \min\{\delta^j, D2^{-j-3}, |\xi - \xi_0|/2\}$. Define the subcover $\{B(\xi_i^j, \delta^j(\xi_i^j))\}_{i=1}^{n^j}$ and the partition $\{I_i^j(\xi)\}_{i=1}^{n^j}$ of I, as in (A.4.3). Set the jth approximate solution to

$$y_t^j(\xi) := \xi + \int_0^t \sum_{i=1}^{n^j} \chi_{I_i^j(\xi)}(s) v_s^{j-1}(\xi_i^j) ds.$$

Note that $y_t^j(\xi_0) = x(t)$ since $I_0^j(\xi_0) = [0, T]$. Then we have

$$\begin{aligned}
&\int_0^t |\dot{y}_s^j(\xi) - \dot{y}_s^{j-1}(\xi)| ds \\
&\leq \int_0^t \sum_i \chi_{I_i^j(\xi)} |v_s^{j-1}(\xi_i^j) - \dot{y}_s^{j-1}(\xi)| ds \\
&\leq \int_0^t \sum_i \chi_{I_i^j(\xi)} |v_s^{j-1}(\xi_i^j) - \dot{y}_s^{j-1}(\xi_i^j)| ds \\
&+ \int_0^t \sum_i \chi_{I_i^j(\xi)} |\dot{y}_s^{j-1}(\xi_i^j) - \dot{y}_s^{j-1}(\xi)| ds \\
&\leq \int_0^t (\sum_i \chi_{I_i^j(\xi)}) \Big[DK \Big[\frac{(Ks)^{j-1}}{(j-1)!} + 2^{-j} \sum_{i=0}^{j-1} \frac{(2Ks)^i}{i!} \Big] \Big] ds \\
&+ \int_0^t (\sum_i \chi_{I_i^j(\xi)}) \alpha^{j-1}(s) \chi_E(s) ds \\
&\leq D \Big[\frac{(Kt)^j}{j!} + 2^{-j-3} + 2^{-j-1} \sum_{i=1}^{j} \frac{(2Kt)^i}{i!} \Big].
\end{aligned}$$

This proves (i). Now fix t and let i be such that $t \in I_i^j(\xi)$. Then,

$$\begin{aligned}
d[\dot{y}_t^j(\xi), F(t, y_t^{j-1}(\xi))] &= d[v_t^{j-1}(\xi_i^j), F(t, y_t^{j-1}(\xi))] \\
&\leq d_H[F(t, y_t^{j-1}(\xi_i^j)), F(t, y_t^{j-1}(\xi))] \\
&\leq K \Big| \xi_i^j - \xi + \int_0^t (\dot{y}_s^{j-1}(\xi_i^j) - \dot{y}_s^{j-1}(\xi)) ds \Big| \\
&\leq KD[2^{-j-3} + 2^{-j-3}] = KD2^{-j-2}.
\end{aligned}$$

This proves (ii). Finally, we prove (iii).

$$\begin{aligned} d[\dot{y}_t^j(\xi), F(t, y_t^j(\xi))] &\le d[\dot{y}_t^j(\xi), F(t, y_t^{j-1}(\xi))] + d_H[F(t, y_t^{j-1}(\xi)), F(t, y_t^j(\xi))] \\ &\le KD2^{-j-2} + K|y_t^{j-1}(\xi) - y_t^j(\xi)| \\ &\le KD\Big[\frac{(Kt)^j}{j!} + 2^{-j-1}\sum_{i=0}^{j}\frac{(2Kt)^i}{i!}\Big]. \end{aligned}$$

□

Corollary A.4.4. *Suppose F satisfies Assumption A.4.1. Then the approximate solutions $\{y^j\}$ of Theorem A.4.3 satisfy*

$$|\dot{y}_t^j(\xi) - \dot{y}_t^0(\xi_i^0)| \le DK\Big[e^{Kt} + e^{2Kt}\Big] \le 2DKe^{2Kt}, \tag{A.4.6}$$

a.e. on interval $I_i(\xi)$.

Proof. From the proof of Theorem A.4.3 at every iteration j we select $v_t^j(\xi) \in F(t, y_t^j(\xi))$, a measurable selection such that

$$|\dot{y}_t^j(\xi) - v_t^j(\xi)| \le DK\Big[\frac{(Kt)^j}{j!} + 2^{-j-1}e^{2Kt}\Big].$$

Given ξ and t, at every j we can find an ℓ^j such that $t \in I_{\ell^j}^j(\xi_{\ell^j}^j)$ and this means $\dot{y}_t^m(\xi) = v_t^{m-1}(\xi_{\ell^m}^m)$. Thus,

$$\begin{aligned} |\dot{y}_t^j(\xi) - \dot{y}_t^{j-1}(\xi_{\ell^j}^{j-1})| &\le DK\Big[\frac{(Kt)^{j-1}}{(j-1)!} + 2^{-j}e^{2Kt}\Big], \\ |\dot{y}_t^j(\xi_{\ell^{j+1}}^{j+1}) - \dot{y}_t^{j-1}(\xi_{\ell^j}^j)| &\le DK\Big[\frac{(Kt)^{j-1}}{(j-1)!} + 2^{-j}e^{2Kt}\Big]. \end{aligned} \tag{A.4.7}$$

From (A.4.7), using a triangle inequality, we obtain the result. □

Bibliography

[1] R. Alur, C. Courcoubetis, D. Dill, N. Halbwachs, and H. Wong-Toi. An implementation of three algorithms for timing verification based on automata emptiness. In *Real-Time Systems Symposium*, IEEE Comput. Soc. Press, p. 157-66, 1992.

[2] R. Alur, C. Courcoubetis, T. A. Henzinger, and P. H. Ho. Hybrid Automaton: An algorithmic approach to the specification and verification of hybrid systems. *Hybrid Systems I*, LNCS 736, pp. 209-229, Springer-Verlag, 1993.

[3] R. Alur, C. Courcoubetis, N. Halbwachs, T. Henzinger, P. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, no. 138, pp. 3-34, 1995.

[4] R. Alur, D. L. Dill. A theory of timed automata. *Theoretical Computer Science*, no. 126, pp. 183-235, 1994.

[5] R. Alur and T.A. Henzinger. *Computer-Aided Verification. An Introduction to Model Building and Model Checking for Concurrent Systems.* Draft, 1998.

[6] V.I. Arnol'd. *Mathematical methods of classical mechanics.* Springer-Verlag, 2nd edition, 1989.

[7] K.J. Astrom, K. Furuta. Swinging up a pendulum by energy control. *Automatica*, vol. 36, no. 2, pp. 287-295, February 2000.

[8] J. Aubin and A. Cellina. *Differential inclusions: set-valued maps and viability theory.* Springer-Verlag, Berlin, 1984.

[9] F. Bacchus and F. Kabanza. Planning for Temporally Extended Goals. *Proc. National Conference on Artificial Intelligence (AAAI '96)*, 1996.

[10] A. Balluchi, L. Benvenuti, M.D. Di Benedetto, C. Pinello, A. Sangiovanni-Vincentelli. Automotive engine control and hybrid systems: challenges and opportunities. *Proceedings of the IEEE Special Issue on Hybrid Systems*, to appear 2000.

[11] A. Balluchi, M.D. Di Benedetto, C. Pinello, et.al. Hybrid control in automotive applications: the cut-off control. *Automatica*, vol. 35, pp. 519-535, March 1999.

[12] A. Balluchi, M. Di Benedetto, C. Pinello, C. Rossi, C., et al. Hybrid control for automotive engine management: the cut-off case. In *Hybrid Systems: Computation and Control* (HSCC'98), Springer-Verlag, p. 13-32, 1998.

[13] A. Balluchi, M.D. Di Benedetto, C. Pinello, A. Sangiovanni-Vincentelli. A hybrid approach to the fast positive force transient tracking problem in automotive engine control. *Proceedings of the IEEE Conference on Decision and Control* (CDC '98), vol. 3, pp. 3226-3231, 1998.

[14] M. Bardi and I. Capuzzo-Dolcetta. *Optimal control and viscosity solutions of Hamilton-Jacobi-Bellman equations.* Birkhäuser, Boston, 1997.

[15] A. Bensoussan and J.L. Lions. *Impulse control and quasi-variational inequalities.* Trans-Inter-Scientia, 1984.

[16] L. Berardi, E. De Santis, and M.D. Di Benedetto. Invariant sets and control synthesis for switching systems with safety specifications. *Hybrid Systems: Computation and Control*, N. Lynch et. al., eds., Springer-Verlag, LNCS 1790, pp. 59-72, 2000.

[17] P. Billingsley. *Convergence of probability measures*, Wiley, New York, 1968.

[18] A.M. Bloch, M. Reyhanoglu, N.H. McClamroch. *Control and stabilization of nonholonomic dynamic systems. IEEE Transactions on Automatic Control.* vol. 37. pp. 1746-1757, 1992.

[19] V.G. Boltyanskii. Sufficient conditions for optimality and the justification of the dynamic programming method. *SIAM Journal of Control*, 4, pp. 326-361, 1966.

[20] M. Branicky, V. Borkar, S. Mitter. A unified framework for hybrid control: model and optimal control theory. *IEEE Trans. AC*, vol. 43, no. 1, pp. 31-45, January, 1998.

[21] R.W. Brockett. Asymptotic stability and feedback stabilization. In *Differential geometric control theory*, R.W. Brockett, et.al, eds. Birkhauser, pp. 181-191, 1983.

[22] M. Broucke. Regularity of solutions and homotopic equivalence for hybrid systems. *Proceedings of the 37th IEEE Conference on Decision and Control* (CDC '98), vol. 4, pp. 4283-8, 1998.

[23] M. Broucke. A geometric approach to bisimulation and verification of hybrid systems. In *Hybrid Systems: Computation and Control*, LNCS 1569, p. 61-75, Springer-Verlag, 1999.

[24] R. Bryant, S. Chern, R. Gardner, H. Goldschmidt, P. Griffiths. *Exterior Differential Systems*. Springer-Verlag, New York, 1991.

[25] J. Burch, E. Clarke, K. McMillan, D. Dill, Hwang. Symbolic Model Checking: 10^{20} states and beyond. *Information and Computation*, 98(2), p. 142-70, 1992.

[26] P. Caines and Y. Wei. On dynamically consistent hybrid systems. *Hybrid Systems II*, pp. 86-105, Springer-Verlag, 1995.

[27] I. Capuzzo Dolcetta and L.C. Evans. Optimal switching for ordinary differential equations. *SIAM J. Control and Optimization*, vol. 22, no. 1, pp. 143-161, January 1984.

[28] I. Capuzzo Dolcetta. On a discrete approximation of the Hamilton-Jacobi equation for dynamic programming. *Applied Math. Optim.*, vol. 10, pp. 367-377, 1983.

[29] A. Cellina. On the set of solutions to Lipschitzian differential inclusions. *Differential and Integral Equations*, vol. 1, no. 4, pp. 495-500, October, 1988.

[30] A. Cellina and A. Ornelas. Representation of the attainable set for Lipschitzian differential inclusions. *Rocky Mountain Journal of Mathematics*, vol. 22, no. 1, Winter 1992.

[31] L.O. Chua, M. Komuro, and T. Matsumoto. The double scroll family - part I: rigorous proof of chaos. *IEEE Transactions on Circuits and systems* vol. 33, no. 11, pp. 1072-1097, November, 1986.

[32] E.M. Clarke, E.A. Emerson, and A.P. Sistla. Automatic verification of finite-state concurrent systems using temporal logic specifications. *ACM Transactions on Programming Languages and Systems*, vol. 8, no. 2, pp. 244-263, 1986.

[33] E.M. Clarke, O. Grumberg, D.A. Peled. *Model Checking.* Princeton University Press, 1999.

[34] F.H. Clarke, et. al. *Nonsmooth analysis and control theory.* Springer Graduate Texts in Mathematics, 178, 1998.

[35] M Crandall, P. Lions. Viscosity solutions of Hamilton-Jacobi equations. *Trans. Amer. Math. Soc.*, vol. 277, no. 1, pp. 1-42, 1983.

[36] M.G. Crandall, P.L. Lions. Two approximations of solutions of Hamilton-Jacobi equations. *Mathematics of Computation*, vol. 43, no. 176, pp. 1-19, July 1984.

[37] J.M. Davoren. *Modal Logics for Continuous Dynamics.* PhD. Dissertation, Cornell University, 1998.

[38] E.W. Dijkstra. A note on two problems in connection with graphs. *Numerische Mathematik* 1, p. 269-271, 1959.

[39] S. N. Ethier and T. G. Kurtz. *Markov processes : characterization and convergence.* Wiley, New York, 1986.

[40] M. Falcone. A numerical approach to the infinite horizon problem of deterministic control theory. *Applied Mathematics and Optimization*, 15, pp. 1-13, 1987.

[41] A. F. Filippov. *Differential Equations with Discontinuous Righthand Sides.* Kluwer, Boston, 1988.

[42] A. F. Filippov. Classical solutions of differential equations with multivalued right hand side. *SIAM Journal of Control*, 5, pp. 609-621, 1967.

[43] W.H. Fleming, R.W. Rishel. *Deterministic and stochastic optimal control.* Springer-Verlag, New York, 1975.

[44] A. T. Fuller. Study of an optimum non-linear control system. *J. Electronics Control*, 15, pp.63-71, 1963.

[45] A. Gollu, P. Varaiya. Hybrid dynamical systems. *Proceedings the IEEE Conference on Decision and Control* (CDC '89), vol 3, pp. 2708-12, 1989.

[46] R. Gonzales and E. Rofman. On deterministic control problems: an approximation procedure for the optimal cost. I: the stationary problem. *SIAM J. Contr. Optim.*, vol. 23, no. 2, pp. 242-266, 1985.

[47] V. Gupta and T.A. Henzinger and R. Jagadeesan, Robust timed automata. *HART 97: Hybrid and Real-time Systems*, ed. O. Maler, Lecture Notes in Computer Science 1201, Springer-Verlag, pp. 331–345, 1997.

[48] T.A. Henzinger. Hybrid automata with finite bisimulations. In *"Proceedings 22nd ICALP: Automata, Languages and Programming*, LNCS 944, pp. 324-335, Springer-Verlag, 1995.

[49] T. Henzinger. The theory of hybrid automata. In *Proc. 11th IEEE Symposium on Logic in Computer Science*, pp. 278-292, New Brunswick, NJ, 1996.

[50] T. Henzinger, P. Kopke, A. Puri, and P. Varaiya. What's decidable about hybrid automata? In *Proc. 27th Annual Symp. Theory of Computing Science*, pp. 373-382, ACM Press, 1995.

[51] T.A. Henzinger and P.-H. Ho. HyTech: The Cornell Hybrid Technology Tool. In P. Antsaklis, et.al. eds., *Hybrid Systems II*, LNCS 999, pp. 265-293, Springer-Verlag, 1995.

[52] T. Henzinger and P.-H. Ho. Algorithmic analysis of nonlinear hybrid systems. In P. Wolper, ed., *Computer Aided Verification*, LNCS 939, pp. 225-238, Springer-Verlag, 1995.

[53] T. Henzinger and H. Wong-Toi. Linear phase-portrait approximations for nonlinear hybrid systems. *Hybrid Systems III*, LNCS 1066, pp. 377-388, Springer-Verlag, 1996.

[54] M. Hirsch, S. Smale. *Differential equations, dynamical systems, and linear algebra.* Academic Press, 1974.

[55] V. Jurdjevic. *Geometric Control Theory.* Cambridge Studies in Advanced Mathematics; 52. Cambridge University Press, 1997.

[56] Y. Kesten, A. Pnueli, J. Sifakis, S Yovine. Integration graphs: a class of decidable hybrid systems. In *Workshop on Theory of Hybrid Systems*, Springer-Verlag, LNCS 736, June 1993.

[57] D. Koditschek. An approach to autonomous robot assembly. *Robotica*, vol.12, pt.2, pp. 137-55, March-April, 1994.

[58] B. Kuipers and K. Astrom. The composition and validation of heterogeneous control laws. In *Multiple model approaches to modelling and control.* R. Murray-Smith and T. Johansen, eds. Taylor & Francis, 1997.

[59] I. Kupka. The ubiquity of the Fuller phenomenon. In *Nonlinear controllability and optimal control*, H.J. Sussmann, ed. Dekker, 1990.

[60] G. Lafferriere, G. Pappas, S. Yovine. A new class of decidable hybrid systems. *Hybrid Systems: Computation and Control*, LNCS 1569, p. 137-151, Springer-Verlag, 1999.

[61] H. B. Lawson. The Quantitative theory of foliations. *Regional Conference Series in Mathematics*, no. 27. American Mathematical Society, Providence, 1977.

[62] P.L. Lions. *Generalized solutions of Hamilton-Jacobi equations.* Pitman, Boston, 1982.

[63] J. Lygeros, D. Godbole, S. Sastry. A game-theoretic approach to hybrid system design. *Hybrid Systems III. Verification and Control*, R. Alur et. al. eds., Springer-Verlag, LNCS

[64] O. Maler, Z. Manna, and A. Pnueli. From timed to hybrid systems. *Proceedings of the REX Workshop on Real-Time: Theory in Practice*, LNCS 600, pp. 447-484, Springer-Verlag, 1992.

[65] O. Maler, A Pnueli, J. Sifakis. On the synthesis of discrete controllers for timed systems. In *Proc. STACS '95*, E.W. Mayr and C. Puech, eds. LNCS 900, Springer-Verlag, p. 229-242, 1995.

[66] Y.-K. Man. Computing closed-form solutions of first-order ODE's using the Prelle-Singer procedure. *Journal of Symbolic Computation*, no. 16, p. 423-443, 1993.

[67] Y.-K. Man. First integrals of autonomous systems of differential equations and the Prelle-Singer procedure. *Journal of Physics A: Mathematical and general*, no. 27, pp. 329-332, 1994.

[68] N.H. McClamroch and I. Kolmanovsky. Hybrid control for global stabilization of nonlinear systems. In *Control Using Logic-Based Switching*. A.S. Morse, ed., Springer-Verlag, pp. 128-141, 1997.

[69] R. Milner. *Communication and Concurrency*. Prentice Hall, 1989.

[70] A.S. Morse. *Control Using Logic-Based Switching*. Springer-Verlag, 1997.

[71] R. Murray and S. Sastry. Nonholonomic motion planning: steering using sinusoids. *IEEE Transactions on Automatic Control*, vol.38, no.5, pp. 700-16, May, 1993.

[72] X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. An approach to the description and analysis of hybrid systems. *Hybrid Systems I*, LNCS 736, pp. 149-178, Springer-Verlag, 1993.

[73] R. Paige and R.E. Tarjan. Three partition refinement algorithms. *SIAM Journal on Computing*, vol.16, no.6, pp. 973-89, December 1987.

[74] D.M.R. Park. Concurrency and automata on infinite sequences. *Fifth GI Conference on Theoretical Computer Science*, pp. 167-183, Springer, 1981.

[75] L. Polymenakos, D. Bertsekas, and J. Tsitsiklis. Implementation of efficient algorithms for globally optimal trajectories. *IEEE Trans. AC*, vol.43, no.2, pp. 278-83, Feb. 1998.

[76] A. Pnueli. The temporal logic of programs. *Proc. of the 18th Annual Symposium on Foundations of Computer Science*, pp. 46-57, IEEE COmputer Society Press, 1977.

[77] L. S. Pontryagin, et. al. *The mathematical theory of optimal processes*. Interscience Publishers, 1962.

[78] M.J. Prelle and M.F. Singer. Elementary first integrals of differential equations. *Transactions of the American Mathematical Society*, vol. 279, no. 1, September 1983, pp. 215-229.

[79] A. Puri and P. Varaiya. Decidability of hybrid systems with rectangular differential inclusions. *Computer-Aided Verification* (CAV'94), LNCS 818, 1995.

[80] A. Puri and P. Varaiya. Driving safely in smart cars. *Proceedings of the 1995 American Control Conference* (ACC '95), pp. 3597-9, vol.5, 1995.

[81] J. Queilli and J. Sifakis. Specification and verification of concurrent systems in CESAR. *Fifth International Symposium on Programming*, LNCS 137, pp. 337-351, Springer-Verlag, 1981.

[82] J. Raisch. Controllability and observability of simple hybrid control systems-FDLTI plants with symbolic measurements and quantized control inputs. *International Conference on Control '94*, IEE, vol. 1, pp. 595-600, 1994.

[83] P. Ramadge, W. Wonham. The control of discrete event systems. *Proceedings of the IEEE*, vol.77, no.1, pp. 81-98, Jan. 1989.

[84] R.T. Rockafellar. *Convex Analysis.* Princeton University Press, 1970.

[85] A. Sangiovanni-Vincentelli. Embedded system design and hybrid systems. In *Control Using Logic-Based Switching.* A.S. Morse, ed., Springer-Verlag, pp. 17-38, 1997.

[86] H. Schattler. Regularity properties of optimal trajectories: recently developed techniques. In *Nonlinear controllability and optimal control*, Dekker, pp. 351-381, 1990.

[87] S. Simic, K. Johansson, S. Sastry, and J. Lygeros. Towards a geometric theory of hybrid systems. In *Hybrid Systems: Computation and Control*, LNCS 1790, p. 421-436, Springer-Verlag, 2000.

[88] W. Sluis. *Absolute Equivalence and its Applications to Control Theory.* Ph.D. thesis, University of Waterloo, 1992.

[89] S. Smale. *Differentiable dynamical systems.* Bulletin American Mathematical Society, 73, pp. 747-817, 1967.

[90] P.E. Souganidis. Approximation schemes for viscosity solutions of Hamilton-Jacobi equations. *Journal of Differential Equations*, vol. 59, no. 1, p. 1-43, August 1985.

[91] J. Borges Sousa, F. Lobo Pereira, E. Pereira da Silva. A general control architecture for multiple AUVs. *Proceedings of the 1996 Symposium on Autonomous Underwater Vehicle Technology.* pp. 223-30, June 1996.

[92] J. Stiver, P. Antsaklis, M. Lemmon. A logical DES approach to the design of hybrid control systems. *Mathematical and computer modelling.* vol. 23, no. 11-1, pp. 55-76, June, 1996.

[93] J.C. McKinsey and A. Tarski. The algebra of topology. *Annals of Mathematics*, 45, pp. 141-191, 1944.

[94] L. Tavernini. Differential automata and their discrete simulators. *Nonlinear Analysis, Theory, Methods & Appl.*, vol. 11, no. 6, pp. 665-683, 1987.

[95] C. Tomlin, G. Pappas, J. Lygeros, D. Godbole, and S. Sastry. Hybrid control models of next generation air traffic management. *Hybrid Systems IV*, LNCS 1273, pp. 378-404, Springer-Verlag, 1997.

[96] J.N. Tsitsiklis. Efficient algorithms for globally optimal trajectories. *IEEE Transactions on Automatic Control*, vol. 40, no. 9, pp. 1528-1538, September 1995.

[97] V.I. Utkin. *Sliding modes and their application in variable structure systems.* Mir Publishers, 1978.

[98] P. Varaiya. Smart cars on smart roads: problems of control. *IEEE Transactions on Automatic Control*, vol. 38, no. 2, pp. 195-207, February 1993.

[99] M. Vardi. Verfication of concurrent programs: the automata-theoretic framework. *Annals Pure and Applied Logic*, 51, p. 79-98, 1991.

[100] M.Y. Vardi and P. Wolper. An automata-theoretic approach to automatic program verification. *Proceedings of the First Annual Symposium on Logic in Computer Science*, pp. 322-331, IEEE Computer Society Press, 1986.

[101] F. Warner. *Foundations of Differential Manifolds and Lie Groups.* Springer-Verlag, New York, 1983.

[102] H.S. Witsenhausen. A class of hybrid-state continuous-time dynamic systems. *IEEE Trans. AC*, vol. 11, no. 2, pp. 161 - 167, April, 1966.

[103] H. Wong-Toi. The synthesis of controllers for linear hybrid automata. In *Proc. 36th IEEE Conference on Decision and Control*, pp. 4607-4612, 1997.