

Verification of Stochastic Systems using Barrier Certificates

A DISSERTATION

*Submitted in partial fulfillment of the
requirements for the the award of the degree
of*

MASTER OF TECHNOLOGY

in

DEPARTMENT OF ELECTRICAL ENGINEERING

(With specialization in Systems and Control)

By

MAHATHI ANAND



DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE

ROORKEE - 247 667 (INDIA)

MAY, 2019

CANDIDATE'S DECLARATION

I hereby declare that this thesis report entitled **Verification of Stochastic Systems using Barrier Certificates**, submitted to the Department of Electrical Engineering, Indian Institute of Technology, Roorkee, India, in partial fulfillment of the requirements for the award of the Degree of Master of Technology in Electrical Engineering with specialization in Systems and Control is an authentic record of the work carried out by me during the period from July 2018 to May 2019 under the combined supervision of **Dr. G. N. PILLAI, Department of Electrical Engineering, Indian Institute of Technology, Roorkee** and **Prof. Dr. Majid Zamani, Department of Electrical and Computer Engineering, Technical University of Munich**. The matter presented in this thesis report has not been submitted by me for the award of any other degree of this institute or any other institute.

Date:

Place: Roorkee

Mahathi Anand

CERTIFICATE

This is to certify that the above statement made by the candidate is true to the best of my knowledge and belief.

Dr. G. N. PILLAI

Professor

Department of Electrical Engineering

Indian Institute of Technology, Roorkee.

ABSTRACT

Design and implementation of control systems in safety critical applications regularly involves formal verification to ensure specification satisfaction and correctness of implementation. The M.Tech dissertation work presents a methodology for temporal logic verification of stochastic systems using a discretization-free approach that combines automata-based verification and barrier certificates. The main objective is to provide a lower bound on the probability that a given temporal logic specification is satisfied over a finite time horizon. This work considers a subclass of temporal logic specifications called safe-LTL properties over finite traces. The method essentially utilizes the automaton representation of the negation of specification for decomposing the specification to a sequence of simpler reachability problems and compute upper bounds for the reachability probabilities using barrier certificates.

The work proposes novel theoretical results for barrier certificate based verification of safety properties for switched stochastic systems in continuous-time, which is then implemented using SMT solvers and Counter Example Guided Inductive Synthesis (CEGIS) framework. In addition, this work also handles the implementation of safety verification for discrete-time stochastic systems using a similar technique. The approach is examined through simple illustrative examples and results are provided.

Acknowledgements

I would like to express gratitude towards my respected supervisor **Dr. G.N. PILLAI**, Department of Electrical Engineering, Indian Institute of Technology, Roorkee, for being extremely supportive to my research goals and for providing constant motivation and inspiration. His periodic suggestions have helped me evolve as a researcher. I am extremely thankful to him for providing me an excellent opportunity to carry out my research work as an exchange student at Technical University of Munich, Germany.

I would also like to extend my sincere thanks to **Prof. Dr. MAJID ZAMANI**, Department of Electrical and Computer Engineering, Technical University of Munich, for supervising my research work and regularly reviewing my progress and providing me solutions to various problems within the scope of research. I'd like to take this opportunity to thank Pushpak Jagtap for being an excellent mentor to me, both academically and otherwise, whose active involvement in my project has been quite conducive in finishing this report.

It is with immense gratitude I say that my report would have been incomplete without the motivation from the faculty of Systems and Control specialisation of Electrical Engineering Department at IIT Roorkee.

I would also extend my thanks to fellow classmates, friends and family for their constant support.

Mahathi Anand

Contents

Candidate's Declaration	i
Abstract	ii
Acknowledgements	iii
List of Figures	vi
List of Tables	vii
Abbreviations	viii
1 Introduction	1
2 Notations and Preliminaries	5
2.1 Notations	5
2.2 Continuous-Time Switched Stochastic Systems	5
2.2.1 Generator	7
2.3 Discrete-Time Stochastic Control Systems	7
2.4 Linear Temporal Logic	8
2.5 Property Satisfaction	11
2.5.1 Continuous-Time	11
2.5.2 Discrete-Time	12
3 Verification of Continuous-Time Switched Stochastic Systems	14
3.1 Barrier Certificates	14
3.1.1 Supermartingales and c-martingales	15
3.1.2 Common Barrier Certificate	16
3.1.3 Multiple Barrier Certificates	17
3.2 Decomposition into Sequential Reachability	19
3.3 Computation of Probabilities Using Barrier Certificates	21
3.4 Computation of Barrier Certificates	23

<i>Contents</i>	v
4 Controller Synthesis of Discrete-Time Stochastic Systems	28
4.1 Control Barrier Certificates	28
4.2 Computation of Control Barrier Certificates	30
5 Examples and Conclusion	33
5.1 Two Dimensional Switched Stochastic System	33
5.2 Temperature Control System	37
5.3 Conclusion	40

Bibliography	42
---------------------	-----------



List of Figures


2.1	Illustration of LTL_F formulas	9
2.2	Example of a Solution Trajectory	13
3.1	DFA for $\neg\varphi$	20
3.2	Flowchart for CEGIS framework	27
5.1	State space and regions of interest	35
5.2	DFA for $\neg\varphi$	35
5.3	Barrier certificate as a function of state	39
5.4	Controller values as a function of state	39
5.5	10 realizations of state vs time	40

List of Tables

5.1 Values of c and γ for all $\nu \in \mathcal{P}^p(\mathbf{q})$, $\mathbf{q} \in \mathcal{R}^p$ 37



Abbreviations



BMC	Bounded Model Checking
CEGIS	Counter Example Guided Inductive Synthesis
DFA	Discrete Finite Automaton
LTL	Linear Temporal Logic
PNF	Positive Normal Form
SAS	Switched Affine Systems
SAT	SATisfiability
SDE	Stochastic Differential Equation
SOS	Sum Of Squares

Chapter 1

Introduction

Control theory involves building effective control systems for complex physical processes which match required specifications and standards. This usually involves modeling a system, measuring the system parameters in comparison to the specifications and providing corrective action with the help of controllers. These systems are checked against simple specifications such as stability. On the other hand, formal verification is the process of providing mathematical or algorithmic proof against complex specifications expressed in terms of temporal logic, for an abstract or a simple model of a software system described as finite state machines, labeled transition systems, timed automata, etc. However, with the advent of increasingly complex cyber-physical systems which have safety-critical components, it becomes unsurprisingly important to deal with the verification of complex dynamical systems against complex specifications including safety, reachability, etc. This topic has gained significant attention in the past few decades and extensive research has resulted in the development of model checking [1], first introduced by E.M Clarke [2], which require models represented as finite state automata that describe all the possible behaviors of the system unambiguously. These pieces of software or tools go through all the possible system states to examine all behaviors in a systematic manner and come up with a counterexample that violates the required specification. As expected,

this method suffers from what we call the 'State Space Explosion', meaning that the model checker cannot traverse through a vast number of states, hence inapplicable to the infinite states represented by continuous and hybrid dynamical systems. It also fails to check properties such as liveness, which requires verification of an event that must 'eventually happen'. Symbolic model checking [3] to an extent addresses the former issue of increasing complication with the number of states by representing a set of states implicitly as boolean functions. However, with further increase in states, the number of boolean functions required also can grow exponentially. Bounded model checking (BMC) [4] does not reduce the complexity of the previous methods but allows specifications to be checked in a finite time horizon and keeps increasing this horizon until it arrives at unsatisfiability or some already known upper bound. This way, liveness properties for a limited execution time could be checked. Moreover, a BMC problem can be reframed by reducing it to a propositional (or boolean) satisfiability problem which can then be solved using SAT solvers, thereby reducing significantly the computational intensity. Abstraction based verification allows to model the continuous dynamics of hybrid systems as much simpler, discretized models such as timed automata [5] or switched affine systems (SAS) [6] and use these models to perform model checking for infinite state systems. These abstract models have smaller state spaces that capture the required behavior of the original system by omitting some unnecessary details. Simulation and bisimulation relations [7], or approximate bisimulation relations [8] help establish the behavioral consistency between the dynamical system and its abstraction. Property satisfaction of abstract models implies property satisfaction of the original complex models. However, this method too subsequently has the drawback of curse of dimensionality and cannot be applied to systems with a large number of state variables.

Formal verification of stochastic dynamical systems, *i.e.*, systems riddled with noise and uncertainties is even more challenging and little progress has been made in literature. For discrete-time stochastic systems, available results include that of verification of probabilistic properties in stochastic hybrid systems using probabilistic model checkers [9] and linear time specifications using Markov

chain abstractions [10]. For continuous and hybrid systems with linear dynamics, reachable set computation [11] has been used for verification of safety properties in the worst case setting. For non-linear dynamics, examples include probabilistic guarantees in stochastic hybrid systems using discrete approximation [12] and verification of stochastic hybrid systems described as piece-wise deterministic Markov processes [13]. Each of these works is dependent on state set discretization and suffer from state space explosion. Verification with the help of barrier certificates, as introduced in [14] for non-linear model invalidation is a discretization-free approach. It has also been adopted for safety verification of continuous-time stochastic systems in [15] and attempts to resolve these previously mentioned disadvantages. In [16], probabilistic guarantees for infinite-time horizon are achieved for verifying whether a stochastic hybrid system reaches what we call an unsafe region. In order to achieve this, a supermartingale property is required to be assumed, which presupposes stochastic stability, hence decreasing the number of systems the method can be applicable to. This issue is handled in [17], where a relaxation of the supermartingale property known as c-martingale property is considered for discrete-time stochastic systems. This property is applicable to a larger group of systems as it does not require any stability assumption. However, probabilistic guarantees can only be achieved for a finite-time horizon. This work also combines the idea of automata based verification and barrier certificates for verification against a general class of linear temporal logic specifications.

The main aim of this work is to provide a systematic discretization-free approach for the probabilistic verification of continuous-time switched stochastic systems against a wide class of temporal logic properties called safe-LTL properties. The method involves computing a lower bound on the probability such that a certain specification given as temporal logic is satisfied by a system. In order to do this, we utilize the automaton representation of negation of the specification to decompose the problem into simpler reachability tasks. Barrier certificates are then used to evaluate the probability bounds for these reachability problems. These individual probability bounds are then combined to obtain a (potentially conservative) lower bound on the probability for satisfaction of the original

specification which is the ultimate objective. ates for arbitrary switching and (ii) using multiple barrier certificates for some probabilistic switching. In addition, controller synthesis and verification of discrete-time stochastic systems for safety properties is also handled. Suitable algorithms are provided and the methods are illustrated with the help of numerical examples.

The rest of the thesis is presented in the following order: Chapter 2 introduces preliminary notations and concepts relevant to the work. Chapter 3 discusses the method involving the verification of continuous-time switched stochastic systems using barrier certificates, and corresponding algorithm. Chapter 4 deals with controller synthesis of discrete-time stochastic systems for satisfaction of safety properties and finally, chapter 6 presents illustrative examples to support the theory developed, along with conclusion and future work.



Chapter 2

Notations and Preliminaries

2.1 Notations

We represent the set of real, positive real, non-negative real, positive integer and non-negative integer numbers with the notations \mathbb{R} , \mathbb{R}^+ , \mathbb{R}_0^+ , \mathbb{N} , and \mathbb{N}_0 respectively. \mathbb{R}^n denoted an n -dimensional Euclidean space and $\mathbb{R}^{n \times m}$ denotes the space of real matrices with n rows and m columns. Given a matrix $A \in \mathbb{R}^{n \times n}$, $\text{Tr}(A)$ represents trace of A which is the sum of all diagonal elements of A .

2.2 Continuous-Time Switched Stochastic Systems

Let $(\Omega, \mathcal{F}, \mathbb{P})$ denote a probability space Ω being the sample space, \mathcal{F} being filtration, and \mathbb{P} as the probability measure. The filtration $\mathbb{F} = (\mathcal{F}_s)_{s \geq 0}$ satisfies the conditions of right continuity and completeness [18]. Let $(W_s)_{s \geq 0}$ be an r -dimensional \mathbb{F} -Brownian motion.

Definition 2.1. A switched stochastic system is a tuple $S = (\mathbb{R}^n, M, \mathcal{M}, F, G)$, where

- \mathbb{R}^n is the real state space;

- $M = \{1, 2, \dots, l\}$ is a finite set of modes;
- \mathcal{M} is a subset of the set of all piece-wise constant càdlàg functions of time from \mathbb{R}_0^+ to M , characterized by a finite number of discontinuities on every bounded interval in \mathbb{R}_0^+ ;
- $F = \{f_1, f_2, \dots, f_l\}$ and $G = \{g_1, g_2, \dots, g_l\}$ are such that for any $m \in M$, $f_m : \mathbb{R}^n \rightarrow \mathbb{R}^n$ and $g_m : \mathbb{R}^n \rightarrow \mathbb{R}^{n \times r}$ satisfy following conditions:
 - (i) Locally Lipschitz continuity: for any $h \in \mathbb{R}^+$, there exists a $K_h > 0$ such that

$$\begin{aligned} \|x_1\|, \|x_2\| \leq h &\implies \\ \|f_m(x_1) - f_m(x_2)\| + \|g_m(x_1) - g_m(x_2)\| &\leq K_h \|x_1 - x_2\|. \end{aligned}$$

- (ii) Linear growth condition: There exists a $K' > 0$ such that for all $x \in \mathbb{R}^n$,

$$\|f_m(x)\| + \|g_m(x)\| \leq K'(1 + \|x\|).$$

A continuous-time stochastic process $\xi : \Omega \times \mathbb{R}_0^+ \rightarrow \mathbb{R}^n$ is a solution process of the system S if there exists $\mu \in \mathcal{M}$ that satisfies

$$d\xi = f_\mu(\xi)dt + g_\mu(\xi)dW_t \quad (2.1)$$

\mathbb{P} -almost surely (\mathbb{P} -a.s.) at each time $t \in \mathbb{R}_0^+$. For any given $m \in M$, we denote S_m as the subsystem of S defined by the stochastic differential equation

$$d\xi = f_m(\xi)dt + g_m(\xi)dW_t. \quad (2.2)$$

Solution process of S_m exists and is unique due to the assumptions on f_m and g_m [18]. $\xi^\mu(t)$ represents the value of the solution process at time $t \in \mathbb{R}_0^+$ under the switching signal μ , starting from the initial state $\xi^\mu(0) = x_0$ \mathbb{P} -a.s. Solution process of S_m is nothing but the solution process of S under the switching signal $\mu(t) = m$, for all $t \in \mathbb{R}_0^+$. $\xi^m(t)$ represents the value of the solution process of S_m at time $t \in \mathbb{R}_0^+$, starting from the initial state of $\xi^m(0) = x_0$ \mathbb{P} -a.s.

2.2.1 Generator

The infinitesimal generator \mathcal{D} of the solution process ξ on function $B : \mathbb{R}^n \rightarrow \mathbb{R}$ is defined by:

Definition 2.2. For any given $m \in M$, the generator \mathcal{D} of the process ξ of the stochastic system S_m acting on function $B : \mathbb{R}^n \rightarrow \mathbb{R}$ is given by

$$\mathcal{D}B(x_0, m) = \lim_{t \rightarrow 0} \frac{\mathbb{E}[B(\xi^m(t)) | \xi^m(0) = x_0] - B(x_0)}{t}. \quad (2.3)$$

The generator is essentially the stochastic equivalent of the partial derivative term in deterministic processes. It is the characterization the evolution of the expected value of the barrier certificate, *i.e.* $E(B(x(t)))$ by using Dynkin's formula [19], which is given by

$$\begin{aligned} \mathbb{E}[B(\xi^m(t_2)) | \xi^m(t_1)] \\ = B(\xi^m(t_1)) + \mathbb{E}\left[\int_{t_1}^{t_2} \mathcal{D}B(\xi^m(t), m) dt | \xi^m(t_1)\right], \end{aligned} \quad (2.4)$$

for $t_2 \geq t_1 \geq 0$.

2.3 Discrete-Time Stochastic Control Systems

We consider the probability space $(\Omega, \mathcal{F}_\Omega, \mathbb{P}_\Omega)$ with Ω being sample space, \mathcal{F}_Ω being the sigma algebra on Ω that consists a subset of Ω as events and \mathbb{P}_Ω is the probability assigned to these events. Random variables are assumed to be measurable functions $(X, \Omega) \rightarrow (S_X, \mathcal{F}_X)$ and $Prob\{A\} = \mathbb{P}_\Omega\{X^{-1}(A)\}$ for any $A \in \mathcal{F}_X$.

Definition 2.3. Discrete-time stochastic control system is denoted by the tuple $S = (X, V_w, U, w, f)$ where

- X and V_w are Borel spaces pertaining to state and uncertainties in the system;

- U is a set of discrete control inputs;
- w is a set of independently and identically distributed random variables on the set V_w with $w := \{w(k) : \Omega \rightarrow V_w, k \in \mathbb{N}_0\}$
- $f : X \times U \times V_w \rightarrow X$ is a measurable function that characterizes the evolution of the state trajectories.

For an initial condition $x(0) \in X$, the state evolution of the system is evaluated from:

$$x(k+1) = f(x(k), u(k), w(k)) \quad k \in \mathbb{N}_0 \quad (2.5)$$

2.4 Linear Temporal Logic

Verification almost always deals with the state behaviour of a system, and not just input-output behaviour. Linear Temporal Logic helps describe the specifications for the state trajectories with a simple yet mathematically precise notation [1]. LTL is a type of modal temporal logic that has modalities with respect to time. It allows to reason about the future of paths, for example, a condition that will never happen or that a condition will happen at the very next transition. LTL specification is primarily used because it can describe certain very important properties such as safety (This bad event will not happen globally) or liveness (Eventually a good event will happen). LTL is further classified into Metric Temporal Logic, Real Time Temporal Logic, Signal Temporal Logic, etc., but for our application, we form the basis through Propositional Temporal Logic, which is an extension of propositional logic with temporal operators. Hence, it contains the usual Boolean operators such as NOT (\neg), AND (\wedge) and OR (\vee) in addition to which temporal operators such as NEXT (\circ or X), GLOBALLY (\square or G), EVENTUALLY (\diamond or F) and UNTIL (U). Each of these operators describe the behaviour of the system in future time. For example, $X\varphi$ where φ is a certain LTL property, is true if φ holds in the next state of the system and $F\varphi$ is true if φ holds eventually, that is, in at least one of the states during system execution.

The LTL formulas over a set Π of atomic propositions are obtained as

$$\varphi ::= \top \mid p \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \bigcirc\varphi \mid \diamond\varphi \mid \square\varphi \mid \varphi_1 \mathcal{U}\varphi_2$$

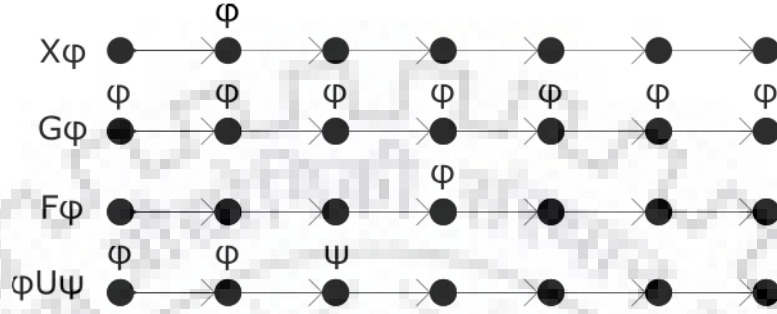


FIGURE 2.1: Illustration of LTL_F formulas.

In our work, as we are concerned with the verification of stochastic systems in finite time, we discuss LTL formulas over finite traces, represented by LTL_F . The syntax of LTL over finite traces is more or less the same as LTL formulas over infinite traces, however, the semantics of LTL_F is written through finite traces, *i.e.*, a non empty finite sequence of consecutive steps over a set of atomic propositions Π . In other words, this finite sequence is also called a finite word. $|\sigma|$ is used to represent the length of σ and σ_k represents a interpretation of a proposition at k th position in the trace, where $0 \leq k < |\sigma|$. Given a finite trace σ and an LTL_F formula φ , we can say that the LTL_F formula φ is true at the k th step ($0 \leq k < |\sigma|$), denoted by $\sigma, k \models \varphi$ by the following definitions:

- $\sigma, k \models \top$;
- $\sigma, k \models p$, for $p \in \Pi$ iff $p \in \sigma_k$;
- $\sigma, k \models \neg\varphi$ iff $\sigma, k \not\models \varphi$;
- $\sigma, k \models \varphi_1 \wedge \varphi_2$ iff $\sigma, k \models \varphi_1$ and $\sigma, k \models \varphi_2$;
- $\sigma, k \models \varphi_1 \vee \varphi_2$ iff $\sigma, k \models \varphi_1$ or $\sigma, k \models \varphi_2$;
- $\sigma, k \models \bigcirc\varphi$ iff $k < |\sigma| - 1$ and $\sigma, k + 1 \models \varphi$;

- $\sigma, k \models \diamond\varphi$ iff for some l such that $k \leq l < |\sigma|$, we have $\sigma, l \models \varphi$;
- $\sigma, k \models \square\varphi$ iff for all l such that $k \leq l < |\sigma|$, we have $\sigma, l \models \varphi$;
- $\sigma, k \models \varphi_1 \mathcal{U} \varphi_2$ iff for some l such that $k \leq l < |\sigma|$, we have $\sigma, l \models \varphi_2$, and for all m s.t. $k \leq m < l$, we have $\sigma, m \models \varphi_1$.

$\sigma \models \varphi$ is the representation for when σ satisfies the formula φ and is valid if and only if $\sigma, 0 \models \varphi$. $\mathcal{L}(\varphi)$ denotes the language associated with a given LTL_F formula φ . The regular Boolean equivalences like $\varphi_1 \vee \varphi_2 \equiv \neg(\neg\varphi_1 \wedge \neg\varphi_2)$, $\varphi_1 \implies \varphi_2 \equiv \neg\varphi_1 \vee \varphi_2$, $\diamond\varphi \equiv \top \mathcal{U} \varphi$, and $\square\varphi \equiv \neg\diamond\neg\varphi$ are also applicable. LTL_F formulas for an execution trace of length 6 is illustrated in figure 2.1.

In chapter 3, we consider only a fragment of LTL_F formulas called safe- LTL_F formulas [20]. Here, in addition, we exclude the next (\circ) operator which enable us to describe behaviour of continuous trajectories using such properties. Therefore, we use a subset of LTL_F known as safe- $LTL_{F \setminus \circ}$, which has been introduced in [21].

Definition 2.4. A safe- LTL_F is a subclass of LTL_F formula that is represented in a positive normal form (PNF) and consists of negations only adjacent to atomic propositions with temporal logic operator always (\square)

Deterministic Finite Automata (DFA) can be used to represent LTL_F specifications. It is defined as follows:

Definition 2.5. A deterministic finite automaton is given by the tuple $\mathcal{A} = (Q, Q_0, \Sigma, \delta, F)$ where

- Q represents the finite set of states,
- $Q_0 \subseteq Q$ denotes the set of initial states,
- Σ is a finite set of symbols called the alphabet,
- $\delta : Q \times \Sigma \rightarrow Q$ is a transition function that determines the transition between one state to the other,
- $F \subseteq Q$ is a set of accepting states.

The notation $q \xrightarrow{\sigma} q'$ denotes the transition relation $(q, \sigma, q') \in \delta$. A finite word $\sigma = (\sigma_0, \sigma_1, \dots, \sigma_{n-1}) \in \Sigma^n$ is said to be accepted by an automaton \mathcal{A} if there exists a finite state run $q = (q_0, q_1, \dots, q_n) \in Q^{n+1}$ such that $q_0 \in Q_0$, $q_k \xrightarrow{\sigma_k} q_{k+1}$ for all $0 \leq k < n$ and $q_n \in F$. $\mathcal{L}(\mathcal{A})$ is the language of \mathcal{A} and it is the set of all words accepted by the automaton.

According to [22], every LTL_F formula φ can be represented by a DFA \mathcal{A}_φ that accepts the the language (set of all words) of the specification φ , *i.e.*, we can say that $\mathcal{L}(\varphi) = \mathcal{L}(\mathcal{A}_\varphi)$. Such DFA can be either explicitly or symbolically constructed using tools like SPOT [23] and MONA [24].

Remark 2.6. : The DFA \mathcal{A}_φ is constructed over the alphabet of the atomic propositions, *i.e.* $\Sigma = 2^\Pi$. A Labeling function from the state space to the alphabet, $L : \mathbb{R}^n \rightarrow \Sigma$, associates the solution trajectory of the system S to the finite set of words, thereby enabling us to physically interpret the trajectories of the system with the help of state sequences. We work with the set of atomic propositions Π as the alphabet Σ instead of its power set 2^Π for ease of understanding.

2.5 Property Satisfaction

2.5.1 Continuous-Time

For a given continuous-time switched stochastic system $S = (\mathbb{R}^n, M, \mathcal{M}, F, G)$ with dynamics (2.1), the solution trajectories over finite time intervals are connected to $\text{LTL}_{F\cap O}$ formulas with the help of a measurable labeling function $L : \mathbb{R}^n \rightarrow \Pi$, for state space \mathbb{R}^n and the set of atomic propositions Π .

Definition 2.7. For a switched stochastic system $S = (\mathbb{R}^n, M, \mathcal{M}, F, G)$ and the labeling function $L : \mathbb{R}^n \rightarrow \Pi$, a finite sequence $\sigma_\xi = (\sigma_0, \sigma_1, \dots, \sigma_{n-1}) \in \Pi^n$ is a finite trace of the solution process ξ over a finite time horizon $[0, T) \subset \mathbb{R}_0^+$ if there exists an associated time sequence t_0, t_1, \dots, t_{n-1} such that $t_0 = 0$, $t_n = T$, and for all $j \in \{0, 1, \dots, n-1\}$, $t_j \in \mathbb{R}_0^+$ following conditions hold

- $t_j < t_{j+1}$;

- $\xi^\mu(t_j) \in L^{-1}(\sigma_j)$;
- If $\sigma_j \neq \sigma_{j+1}$, then for some $t'_j \in [t_j, t_{j+1}]$, $\xi^\mu(t) \in L^{-1}(\sigma_j)$ for all $t \in (t_j, t'_j)$; $\xi^\mu(t) \in L^{-1}(\sigma_{j+1})$ for all $t \in (t'_j, t_{j+1})$; and either $\xi^\mu(t'_j) \in L^{-1}(\sigma_j)$ or $\xi^\mu(t'_j) \in L^{-1}(\sigma_{j+1})$.

For illustration, consider the solution trajectory represented in 2.2 with the regions of interest given by X_0, X_1, X_2 and X_3 . The finite trace of this trajectory would be the sequence of atomic propositions that would hold true until a period of time T , measured at t_0, t_1, t_2 and t_3 .

Next we define the probability for the solution trajectory ξ of the switched stochastic system S starting from some initial state $\xi^\mu(0) = x_0 \in \mathbb{R}^n$ to satisfy safe-LTL_{F\setminus\circ} formula φ over a given finite time horizon $[0, T] \subset \mathbb{R}_0^+$.

Definition 2.8. Consider a switched stochastic system S in definition 2.1 and a safe-LTL_{F\setminus\circ} formula φ over Π . Then $\mathbb{P}_{x_0}\{\sigma_\xi \models \varphi\}$ denotes the probability that solution process ξ of the system S starting from the initial value of $x_0 \in \mathbb{R}^n$ over a finite time horizon $[0, T] \subset \mathbb{R}_0^+$ satisfies the specification φ .

Remark 2.9. The set of atomic propositions $\Pi = \{p_0, p_1, \dots, p_N\}$ and the labeling function $L : \mathbb{R}^n \rightarrow \Pi$ separate the state space into a measurable partition $\mathbb{R}^n = \bigcup_{i=1}^N X_i$ as $X_i := L^{-1}(p_i)$. We can assume that $X_i \neq \emptyset$ for any i without loss of generality.

2.5.2 Discrete-Time

For a given discrete-time stochastic control system $S = (X, V_w, U, w, f)$ with state evolution described by equation 2.5, a labeling function $L : X \rightarrow \Pi$ is again used to associate the solution processes with LTL_F formulas. For the state evolution of the solution process described by $x_N = (x(0), x(1), \dots, x(N-1)) \in X^N, N \in \mathbb{N}_0$, and labeling function L , the finite trace of the solution process is given by $L(x_N) = \{\sigma_0, \sigma_1, \dots, \sigma_N\} \in \Pi^N$, where $\sigma_k = L(x(k))$, for all $k = \{0, 1, 2, \dots, N-1\}$.

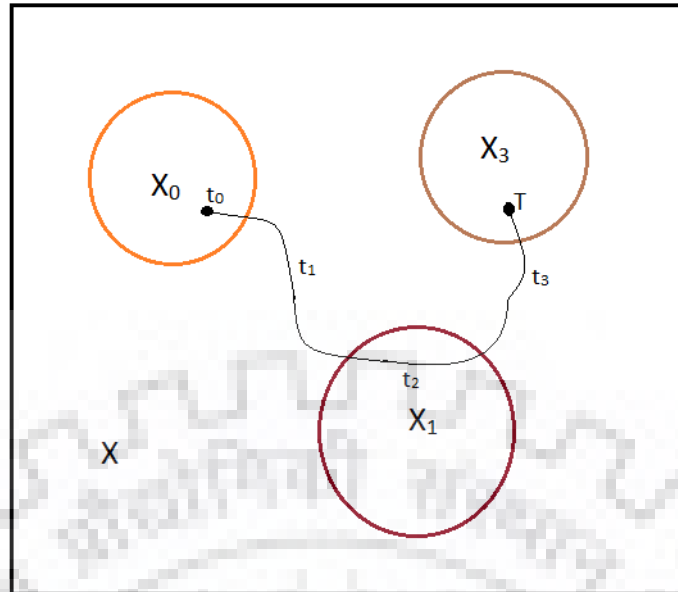


FIGURE 2.2: Example of a Solution Trajectory and its Regions of Interest.

For a given LTL_F specification φ over finite traces of length N , we define the probability of specification satisfaction by the given discrete-time stochastic control system by the following.

Definition 2.10. For a given stochastic control system S as defined in definition 2.3, the probability that the system satisfies the given LTL_F property φ is given by $\mathbb{P}_{x_0}^\rho = \{L(x_N) \models \varphi\}$ where x_0 is the initial condition of the state evolution and ρ is the control policy.

Remark 2.9 applies in the discrete-time case too.

Chapter 3

Verification of Continuous-Time Switched Stochastic Systems

3.1 Barrier Certificates

Safety specification in a system suggests that the states of a control system do not visit a particular region of the state space throughout their operation. As an example, for a line-following robot, it is required that the position of the robot never leaves a given path. Other extensive applications where safety verification is required includes rocket range launch safety systems, where the range of the rocket or missile must not exceed a specified perimeter or air traffic controllers that ensure traffic separation. Barrier certificates is a concept that is vital in ensuring safety of a system. Mathematical verification of safety using barrier certificates is quite similar to the Lyapunov's approach of proving stability. Both use functions that give us information about the properties of the system without explicitly knowing the state evolution. Barrier certificates are functions that separate the regions of state space into a safe region which the states can visit and unsafe region which the states of the system cannot and hence, certain conditions imposed on these functions, if satisfied, imply that the given system is safe.

In order to apply the concept of barrier certificates to continuous-time switched stochastic systems, the following terms must be introduced.

3.1.1 Supermartingales and c-martingales

A function $B : \mathbb{R}^n \rightarrow \mathbb{R}$ is called a supermartingale for a system S if the condition $E(B^\mu(t_2) | B^\mu(t_1)) \leq E(B^\mu(t_1))$ for all $t_2 \geq t_1$ holds. This condition implies that the expected value of the function B is non-decreasing over a period of time. A sufficient condition for a stochastic system to be a supermartingale is $\mathcal{D}B(x_0) \leq 0$ where $\mathcal{D}B(x)$ is the infinitesimal generator defined in definition 2.2.

Although the supermartingale property on stochastic systems is useful for safety verification in infinite time horizon, it assumes stochastic stability, *i.e.*, zero noise at equilibrium point which is not always applicable [25]. Finding practical systems where such a condition holds is extremely difficult, and hence we relax the supermartingale property to what we call a c-martingale property, which is applicable to a wider class of systems but can only provide safety verification in a finite-time horizon.

Definition 3.1. A function $B : \mathbb{R}^n \rightarrow \mathbb{R}$ is called a c-martingale for the system S if

$$\mathbb{E}[B(\xi^\mu(t_2) | \xi^\mu(t_1))] \leq B(\xi^\mu(t_1)) + \int_{t_1}^{t_2} c(t)dt$$

for all $t_2 \geq t_1$, where c is a function of time.

The c-martingale property of the system asks for the expectation of a barrier certificate to increase gradually over a period of time, and hence for a finite time period, the value would still be bounded.

The following lemma is a consequence of [26, Theorem 1] and is also discussed in [25, Theorem II.1]. It will be further used to prove theorems 3.3 and 3.4.

Lemma 3.2. Let $B : \mathbb{R}^n \rightarrow \mathbb{R}_0^+$ be c-martingale for the system S , $c \geq 0$. Then for any positive constant λ and an initial condition $x_0 \in \mathbb{R}^n$,

$$\mathbb{P}\{\sup_{0 \leq t < T} B(\xi^\mu(t)) \geq \lambda \mid x(0) = x_0\} \leq \frac{B(x_0) + \int_0^T c(t)dt}{\lambda}. \quad (3.1)$$

The next two subsections deal with the conditions imposed on barrier certificates to give an upper bound on reachability probability. These theorems have been inspired by the results in [15] in which supermartingale condition is used for verification of continuous-time switching diffusion systems for safety properties.

3.1.2 Common Barrier Certificate

For a switched stochastic system S given in definition 2.1 with several switching modes, we now look at how existence of a barrier certificate allows us to compute a probabilistic guarantee via an upper bound that the unsafe region of the state space is visited by the system. We later use this upper bound for probabilistic verification of satisfaction of a safe-LTL $_{F \setminus O}$ property φ .

Theorem 3.3. *Consider a switched stochastic system $S = (\mathbb{R}^n, M, \mathcal{M}, F, G)$ with dynamics (2.1) and sets $X_0, X_1 \subseteq \mathbb{R}^n$. Suppose there exists a twice differentiable function $B : \mathbb{R}^n \rightarrow \mathbb{R}_0^+$ and constants $c \geq 0$ and $\gamma \in [0, 1]$, such that*

$$B(x) \leq \gamma \quad \forall x \in X_0, \quad (3.2)$$

$$B(x) \geq 1 \quad \forall x \in X_1, \quad (3.3)$$

$$\frac{\partial B}{\partial x}(x)f_m(x) + \frac{1}{2}\text{Tr}(g_m^T(x)\frac{\partial^2 B}{\partial x^2}(x)g_m(x)) \leq c \quad \forall x \in \mathbb{R}^n, \forall m \in M. \quad (3.4)$$

Then $\gamma + cT$ is the upper bound on the probability that the solution process ξ of the system S starts from an initial state $\xi^\mu(0) = x_0 \in X_0$ and reaches X_1 , the unsafe region, within time horizon $[0, T) \subset \mathbb{R}_0^+$.

Proof. The generator associated with the system S_m is given by

$$DB(x, m) = \frac{\partial B}{\partial x}(x)f_m(x) + \frac{1}{2}\text{Tr}(g_m^T(x)\frac{\partial^2 B}{\partial x^2}(x)g_m(x)),$$

where $m \in M$. By using Dynkin's formula, for any $m \in M$ and for $0 \leq t_1 \leq t_2 < T$, we have

$$\begin{aligned} \mathbb{E}[B(\xi^m(t_2)) | \xi^m(t_1)] &= B(\xi^m(t_1)) + \mathbb{E}\left[\int_{t_1}^{t_2} \mathcal{D}B(\xi^m(t), m) dt | \xi^m(t_1)\right] \\ &\leq B(\xi^m(t_1)) + \int_{t_1}^{t_2} c dt. \end{aligned}$$

This implies that $B(x)$ is a nonnegative c -martingale for all $m \in M$ and hence (3.1) in Lemma 3.2 holds. Using (3.2) and the condition $X_1 \subseteq \{x \in \mathbb{R}^n \mid B(x) \geq 1\}$, we have $\mathbb{P}\{\xi^\mu(t) \in X_1 \text{ for some } 0 \leq t < T \mid \xi^\mu(0) = x_0\} \leq \mathbb{P}\{\sup_{0 \leq t < T} B(\xi^\mu(t)) \geq 1 \mid \xi^\mu(0) = x_0\} \leq B(x_0) + cT \leq \gamma + cT$. This concludes the proof. \square

It must be noted that in theorem 3.3, X_0 refers to the region where the solution trajectories are initialized and X_1 refers to the unsafe region the states are prohibited to enter.

If there exists a twice differentiable function $B : \mathbb{R}^n \rightarrow \mathbb{R}_0^+$ satisfying the conditions (3.2)-(3.4) of Theorem 3.3, then we call it a common barrier certificate. In most of the cases, finding common barrier certificates may not be feasible or may result in conservative probability bounds. To alleviate these issues, we provide results using multiple barrier certificates for switched stochastic systems with a restricted set of switching signals.

3.1.3 Multiple Barrier Certificates

Consider a switched stochastic system S as defined in (2.1) and $m, m' \in M = \{1, 2, \dots, k\}$. At any instant t , the transition probability between modes is given by

$$\mathbb{P}\{(m, m'), t + h\} = \begin{cases} \lambda_{mm'}(\xi^\mu(t))h, & \text{if } m \neq m', \\ 1 + \lambda_{mm}(\xi^\mu(t))h, & \text{if } m = m', \end{cases} \quad (3.5)$$

where $h > 0$, $\lambda_{mm'} : \mathbb{R}^n \rightarrow \mathbb{R}$ is a bounded and Lipschitz continuous function representing transition rates such that $\lambda_{mm'}(x) \geq 0$ for all $x \in \mathbb{R}^n$ if $m \neq m'$ and

$\sum_{m' \in M} \lambda_{mm'}(x) = 0$ for all $m \in M$. It is assumed that the transition from one mode to another is independent of the Wiener process W_t . Refer to [27] for a detailed discussion on how the transitions are generated.

The next theorem provides conditions to obtain an upper bound on the reachability probability for switched stochastic systems using multiple barrier certificates.

Theorem 3.4. *Consider a switched stochastic system $S = (\mathbb{R}^n, M, \mathcal{M}, F, G)$ with dynamics (2.1), sets $X_0, X_1 \subseteq \mathbb{R}^n$, and the transition rates between two switching modes $m, m' \in M$ as $\lambda_{mm'} : \mathbb{R}^n \rightarrow \mathbb{R}$. Suppose there exists a set of twice differentiable functions $B_m : \mathbb{R}^n \rightarrow \mathbb{R}_0^+$, and constants $c \geq 0$ and $\gamma \in [0, 1]$, such that*

$$B_m(x) \leq \gamma \quad \forall x \in X_0, \quad (3.6)$$

$$B_m(x) \geq 1 \quad \forall x \in X_1, \quad (3.7)$$

$$\begin{aligned} \frac{\partial B_m}{\partial x}(x) f_m(x) + \frac{1}{2} \text{Tr}(g_m^T(x) \frac{\partial^2 B_m}{\partial x^2} g_m(x)) \\ + \sum_{m' \in M} \lambda_{mm'}(x) B_{m'}(x) \leq c \quad \forall x \in \mathbb{R}^n. \end{aligned} \quad (3.8)$$

for all $m \in M$. Then $\gamma + cT$ is the upper bound on the probability that the solution process ξ of the system S starts from an initial state $\xi^u(0) = x_0 \in X_0$ and reaches X_1 , the unsafe region, within time horizon $[0, T) \subset \mathbb{R}_0^+$.

Proof. The generator associated with the system S is given by

$$\begin{aligned} \mathcal{D}B_m(x, m) = \frac{\partial B_m}{\partial x}(x) f_m(x) + \frac{1}{2} \text{Tr}(g_m^T(x) \frac{\partial^2 B_m}{\partial x^2} g_m(x)) \\ + \sum_{m' \in M} \lambda_{mm'}(x) B_{m'}(x), \end{aligned}$$

where $m \in M$. With the help of condition (3.8) and Dynkin's formula, one can say that $B_m(x)$ is a nonnegative c -martingale. Thus, condition (3.1) in Lemma 3.2 holds. The rest of the proof follows similar to that of Theorem 3.3. \square

3.2 Decomposition into Sequential Reachability

For a wide class of LTL properties such as a safe-LTL_{F\O} formula φ , the process of safety verification for a switched stochastic system entails the following steps:

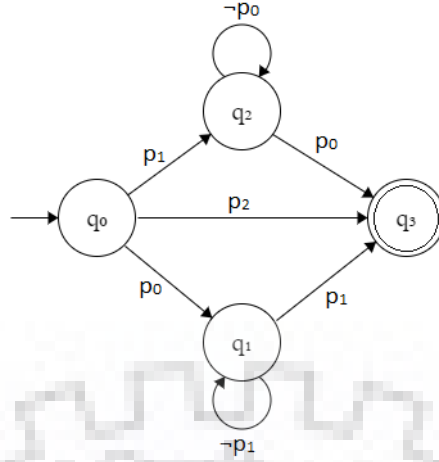
- Consider the negation of the safe-LTL_{F\O} formula *i.e.*, $\neg\varphi$ and construct its corresponding DFA.
- From the DFA, decompose $\neg\varphi$ into simpler reachability problems.
- Use barrier certificates to calculate the upper bound of the probability that the reachability problem is satisfied.
- Once the upper bound on the probabilities of each sequential reachability problem is obtained, combine them to compute the over all upper bound on the probability of violation of the safety property, which can be used to calculate the tight lower bound on the probability that safe-LTL_{F\O} specification φ is satisfied.

The procedure for decomposition into sequential reachability is illustrated parallelly with an example.

For a set of atomic propositions $\Pi = \{p_0, p_1, p_2\}$, consider the following safe-LTL_{F\O} formula φ adapted from [17]:

$$\varphi = (p_0 \wedge \Box \neg p_1) \vee (p_1 \wedge \neg \Box p_0)$$

Consider a DFA $\mathcal{A}_{\neg\varphi} = (Q, Q_0, \Pi, \delta, F)$ that accepts all finite words over the set of atomic propositions Π that satisfy $\neg\varphi$, the negation of the specification. For the given example, the corresponding DFA is given in figure 3.1. The sequence $\mathbf{q} = (q_0, q_1, \dots, q_n) \in Q^{n+1}$, $n \in \mathbb{N}$ is called an accepting state run if $q_0 \in Q_0$, $q_n \in F$, and there exists a finite word $\sigma = (\sigma_0, \sigma_1, \dots, \sigma_{n-1}) \in \Pi^n$ such that $q_k \xrightarrow{\sigma_k} q_{k+1}$ for all $k \in \{0, 1, \dots, n-1\}$. The set of such finite words are given by $\sigma(\mathbf{q}) \subseteq \Pi^n$. The length of $\mathbf{q} \in Q^{n+1}$ by $|\mathbf{q}|$ is $n + 1$. Let \mathcal{R} denote the set of all finite state runs that

FIGURE 3.1: DFA for $\neg\varphi$.

are accepted, starting from $p \in \Pi$ without considering self-loops, where

$$\mathcal{R} := \{\mathbf{q} = (q_0, q_1, \dots, q_n) \in Q^{n+1} \mid q_n \in F, q_k \neq q_{k+1}, \forall k < n\}. \quad (3.9)$$

\mathcal{R} can be computed by considering $\mathcal{A}_{\neg\varphi}$ as a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with vertices $\mathcal{V} = Q$ and edges $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ such that $(q, q') \in \mathcal{E}$ if and only if $q' \neq q$ and there exist $p \in \Pi$ such that $q \xrightarrow{p} q'$. It can be easily noticed from the graph of the automaton that an accepting state run is nothing but the finite path in the graph that starts from a vertex $q_0 \in Q_0$ and ends at $q_n \in Q_F$, i.e., a state run that starts at the initial state and ends at the accepting state without any self-loop. Hence, such a path belongs to the set of accepting state runs, \mathcal{R} . Various depth first search algorithms [28] are available to compute \mathcal{R} .

For each $p \in \Pi$, we define a set \mathcal{R}^p as

$$\mathcal{R}^p := \{\mathbf{q} = (q_0, q_1, \dots, q_n) \in \mathcal{R} \mid \sigma(q_0, q_1) = p\}. \quad (3.10)$$

For any $\mathbf{q} = (q_0, q_1, \dots, q_n) \in \mathcal{R}^p \forall p \in \Pi$, $\mathcal{P}^p(\mathbf{q})$ is a set of all sequence of state runs of length 3,

$$\mathcal{P}^p(\mathbf{q}) := \{(q_k, q_{k+1}, q_{k+2}) \mid 0 \leq k \leq n-2\}. \quad (3.11)$$

Remark 3.5. Note that $\mathcal{P}^p(\mathbf{q}) = \emptyset$ for $|\mathbf{q}| = 2$. This is because any accepting state run of length 2 that starts at the subset of the state space definitely reaches

the same subset, and hence there is trivial probability for satisfaction of the specification.

This is what we call decomposition into sequential reachability.

Consider the above stated safe-LTL_F specification φ and the corresponding DFA of $\neg\varphi$ in figure 3.1. For this example, the accepting state runs without self-loops \mathcal{R}^p for each proposition $p_i, i = \{0, 1, 2\}$ are given by

$$\mathcal{R}^{p_0} = \{(q_0, q_1, q_3)\}$$

$$\mathcal{R}^{p_1} = \{(q_0, q_2, q_3)\}$$

$$\mathcal{R}^{p_2} = \{(q_0, q_3)\}$$

For each of these accepting state runs, we consider the sequence of subpaths of lengths 3, $\mathcal{P}^p(q)$ given by

$$\mathcal{P}^{p_0} = \{(q_0, q_1, q_3)\}$$

$$\mathcal{P}^{p_1} = \{(q_0, q_2, q_3)\}$$

Note that accepting state runs of length 2 or less are not considered.

3.3 Computation of Probabilities Using Barrier Certificates

Now that we have the subpaths of lengths 3 from the DFA, we can compute lower bound on the probability of satisfaction of φ for the solution trajectories ξ for a given initial condition. Given the DFA $\mathcal{A}_{\neg\varphi}$ for the negation of specification $\neg\varphi$, we perform the computation of upper bound on probability of reachability over each element of $\mathcal{P}^p(\mathbf{q}), \mathbf{q} \in \mathcal{R}^p$ using barrier certificates. The following theorem allows us to compute the over all upper bound on the probability of satisfaction of negation of specification $\neg\varphi$ from the individually computed lower bounds of probability for reachability tasks.

Theorem 3.6. For a given safe-LTL_{F\O} specification φ , let $\mathcal{A}_{\neg\varphi}$ denote the DFA of to its negation, \mathcal{R}^p denote the set defined in (3.10), and \mathcal{P}^p be the set of runs of length 3 defined in (3.11). Then the upper bound on the probability that the solution process of system S starts from any initial state $x_0 \in L^{-1}(p)$ satisfies $\neg\varphi$ within time horizon $[0, T)$ is given by:

$$\mathbb{P}_{x_0}\{\sigma_\xi \models \neg\varphi\} \leq \sum_{\mathbf{q} \in \mathcal{R}^p} \prod \{(\gamma_v + c_v T) \mid v = (q, q', q'') \in \mathcal{P}^p(\mathbf{q})\}. \quad (3.12)$$

Here $\gamma_v + c_v T$ is the upper bound on the probability that the solution trajectory of system S starting from $X_0 := L^{-1}(\sigma(q, q'))$ and reaches $X_1 := L^{-1}(\sigma(q', q''))$ within time horizon $[0, T)$ computed as given in Theorem 3.3 (or Theorem 3.4).

Proof. For $p \in \Pi$, where Π is the set of atomic propositions, let $\mathbf{q} \in \mathcal{R}^p$ be an accepting run and set $\mathcal{P}^p(\mathbf{q})$ be the set of runs of length 3 as defined in (3.11). For a particular element $v = (q, q', q'') \in \mathcal{P}^p(\mathbf{q})$, $\gamma_v + c_v T$ is the upper bound on the probability that the solution trajectories of the system S reach $L^{-1}(\sigma(q', q''))$ after starting in $L^{-1}(\sigma(q, q'))$ within time T . This is derived in Theorem 3.3 (or Theorem 3.4). Now the upper bound on the probability that traces corresponding to solution processes reach the accepting state through the path of q is given by the product of individual probability bounds of all elements $v = (q, q', q'')$ belonging to the set $\mathcal{P}^p(\mathbf{q})$, *i.e.*, the product of the probability for reachability tasks of all sub-paths of length three corresponding to a particular accepting state run. This is given by

$$\mathbb{P}\{\sigma(\mathbf{q}) \models \neg\varphi\} \leq \prod \{(\gamma_v + c_v T) \mid v = (q, q', q'') \in \mathcal{P}^p(\mathbf{q})\}. \quad (3.13)$$

The above formula only considers one accepting state run and its subpaths of length three. The product essentially represents the events happening consequentially. Now, to calculate the overall upperbound on the probability that solution processes that start from any initial state $x_0 \in L^{-1}(p)$ violate the specification φ (or satisfy $\neg\varphi$) can be obtained from the sum of product probability bounds for all possible accepting state runs and the overall tight upperbound is given by the following formula.

$$\mathbb{P}_{x_0}\{\sigma_\xi \models \neg\varphi\} \leq \sum_{\mathbf{q} \in \mathcal{R}^p} \prod \{(\gamma_\nu + c_\nu T) \mid \nu = (q, q', q'') \in \mathcal{P}^p(q)\}.$$

□

Theorem 3.6 lets us decompose the complex specification into a set of sequential reachabilities, compute upper bounds on the reachability probabilities using Theorem 3.3 (or Theorem 3.4), and then combine the bounds in a sum-product expression.

Remark 3.7. In the case that for certain elements $\nu \in \mathcal{P}^p(\mathbf{q})$ in (3.12), barrier certificates cannot be found, we can replace the upper bound by a trivial probability of 1. We must be able to find at least one barrier certificate for each accepting state run $\mathbf{q} \in \mathcal{R}^p$ in order to get a final non-trivial probability.

Corollary 3.8. *Given the result of Theorem 3.6, the lower bound on the probability that the solution process of S starting from any $x_0 \in L^{-1}(p)$ over time horizon $[0, T) \subset \mathbb{R}_0^+$ satisfies safe-LTL $_{F \setminus O}$ specification φ is given by*

$$\mathbb{P}_{x_0}\{\sigma_\xi \models \varphi\} \geq 1 - \mathbb{P}_{x_0}\{\sigma_\xi \models \neg\varphi\}.$$

3.4 Computation of Barrier Certificates

In this section, we provide the Counter-Example Guided Inductive Synthesis (CEGIS) framework for searching barrier certificates of specific forms satisfying conditions in Theorem 3.3 (or Theorem 3.4). The approach uses feasibility solvers for finding barrier certificates of a given parametric form using Satisfiability Modulo Theories (SMT) solvers such as Z3 [29] and dReal [30]. In order to use the CEGIS framework, we raise following assumption.

Assumption 3.9. System S has compact state-space $X \subset \mathbb{R}^n$ and partition sets $X_i \in L^{-1}(p_i)$, $i \in \{1, 2, \dots, N\}$ are bounded and semi-algebraic, in the sense they can be represented by polynomial equalities and inequalities.

Remark 3.10. The assumption of compactness of state-space $X \subseteq \mathbb{R}^n$ can be supported by considering stopped process $\tilde{\xi} : \Omega \times \mathbb{R}_0^+ \rightarrow X$ as

$$\tilde{\xi}^\mu(t) := \begin{cases} \xi^\mu(t), & \text{for } t < \tau, \\ \xi^\mu(\tau), & \text{for } t \geq \tau, \end{cases}$$

where τ is the first time of exit of the solution process ξ of $S = (\mathbb{R}^n, M, \mathcal{M}, F, G)$ from the open set $\text{Int}(X)$. Note that, in most cases, the infinitesimal generator corresponding to the stopped process $\tilde{\xi}$ is identical to the one corresponding to ξ over the set $\text{Int}(X)$, and is equal to zero outside of the set [26]. Thus, the results in theorems 3.3 and 3.4 can be used for the systems with this assumption.

Next lemma provides the feasibility condition required for the existence of common barrier certificate given in theorem 3.3.

Lemma 3.11. *Consider a switched stochastic system $S = (X, M, \mathcal{M}, F, G)$ with Assumption 3.9. Suppose sets X_0 , X_1 , and X are bounded semi-algebraic sets. Suppose there exists a function $B(x)$, constants $\gamma \in [0, 1]$ and $c \geq 0$, such that the following expression is true*

$$\begin{aligned} \bigwedge_{x \in X} B(x) \geq 0 \quad \bigwedge_{x \in X_0} B(x) \leq \gamma \quad \bigwedge_{x \in X_1} B(x) \geq 1 \\ \bigwedge_{m \in M} \left(\bigwedge_{x \in X} \frac{\partial B}{\partial x}(x) f_m(x) + \frac{1}{2} \text{Tr} \left(g_m^T(x) \frac{\partial^2 B}{\partial x^2}(x) g_m(x) \right) \leq c \right). \end{aligned} \quad (3.14)$$

Then $B(x)$ satisfies conditions in Theorem 3.3.

Next we provide a similar lemma giving the feasibility condition for the existence of multiple barrier certificates required in Theorem 3.4.

Lemma 3.12. *Consider a switched stochastic system $S = (X, M, \mathcal{M}, F, G)$ with switching signal following transition probability given in (3.5) and Assumption 3.9. Suppose X_0 , X_1 , and X are bounded semi-algebraic sets. Let there exist a set of functions $B_m(x)$*

for all $m \in M$, constants $\gamma \in [0, 1]$ and $c \geq 0$, such that following expression is true

$$\begin{aligned} & \bigwedge_{m \in M} \left(\bigwedge_{x \in X} B_m(x) \geq 0 \bigwedge_{x \in X_0} B_m(x) \leq \gamma \bigwedge_{x \in X_1} B_m(x) \geq 1 \right. \\ & \quad \bigwedge_{x \in X} \frac{\partial B_m}{\partial x}(x) f_m(x) + \frac{1}{2} \text{Tr}(g_m^T(x) \frac{\partial^2 B_m}{\partial x^2} g_m(x)) \\ & \quad \left. + \sum_{m' \in M} \lambda_{mm'}(x) B_{m'}(x) \leq c \right). \end{aligned} \quad (3.15)$$

Then the conditions in Theorem 3.4 holds.

In order to utilize CEGIS framework, we consider a barrier certificate of the parametric form $B(a, x) = \sum_{i=1}^k a_i b_i(x)$ with some user-defined (nonlinear) basis functions $b_i(x)$ and unknown coefficients $a_i \in \mathbb{R}, i \in \{1, 2, \dots, k\}$. With this choice of barrier certificate the feasibility expression (3.14) can be rewritten as

$$\begin{aligned} \psi(a, x) := & \bigwedge_{x \in X} B(a, x) \geq 0 \bigwedge_{x \in X_0} B(a, x) \leq \gamma \bigwedge_{x \in X_1} B(a, x) \geq 1 \\ & \bigwedge_{m \in M} \bigwedge_{x \in X} \left(\frac{\partial B}{\partial x}(a, x) f_m(x) + \frac{1}{2} \text{Tr}(g_m^T(x) \frac{\partial^2 B}{\partial x^2}(a, x) g_m(x)) \leq c \right). \end{aligned} \quad (3.16)$$

Similarly one can obtain feasibility expression $\psi(a, x)$ for multiple barrier certificates using (3.15). The coefficients a_i can be efficiently found using SMT solvers such as Z3 for the finite set $\bar{X} \subset X$ of data samples. We denote the obtained candidate barrier certificate with fixed coefficients a_i by $B(a, x)|_a$ and the corresponding feasibility expression by $\psi(a, x)|_a$. Next we obtain counterexample $x \in X$ such that $B(a, x)|_a$ satisfies $\neg \psi(a, x)|_a$. If $\neg \psi(a, x)|_a$ has no feasible solution, then the obtained $B(a, x)|_a$ is a true barrier certificate. If $\neg \psi(a, x)|_a$ is feasible, we update data samples as $\bar{X} = \bar{X} \cup x$ and recompute coefficients a_i iteratively until $\neg \psi(a, x)|_a$ becomes infeasible. For detailed overview on CEGIS procedure we refer readers to [31]. To obtain a tight upper bound on the probability, one can utilize bisection method over c and γ iteratively. The pseudocode for CEGIS framework to compute such barrier certificates is given in Algorithm 1. In addition, one can also refer to figure 3.2 which describes the flowchart of the CEGIS framework.

Remark 3.13. In addition, under the assumption that f_m and g_m , $m \in M$ are polynomial functions of ξ , the conditions in theorems 3.3 and 3.4 can be formulated as a sum-of-square program to compute polynomial type barrier certificates. [15].

Algorithm 1 CEGIS Framework

Require: c, γ

- 1: Define $\bar{X} \subset X$ ▷ set of finite data samples in X
 - 2: Define $B(a, x) := \sum_{i=1}^k a_i b_i(x)$
 - 3: **while** True **do**
 - 4: **if** $\psi(a, x)$ is *unsat* **then**
 - 5: *infeasible*
 - 6: **break**
 - 7: **else**
 - 8: Compute candidate $B(a, x)|_a$ for given c and γ
 - 9: **if** $\neg\psi(a, x)|_a$ is *unsat* **then**
 - 10: $B(a, x)|_a$ is a barrier certificate
 - 11: **break**
 - 12: **else**
 - 13: $cex = x \in X$ s.t. $\neg\psi(a, x)|_a$ is *sat*
 - 14: $\bar{X} \leftarrow \bar{X} \cup cex$
-

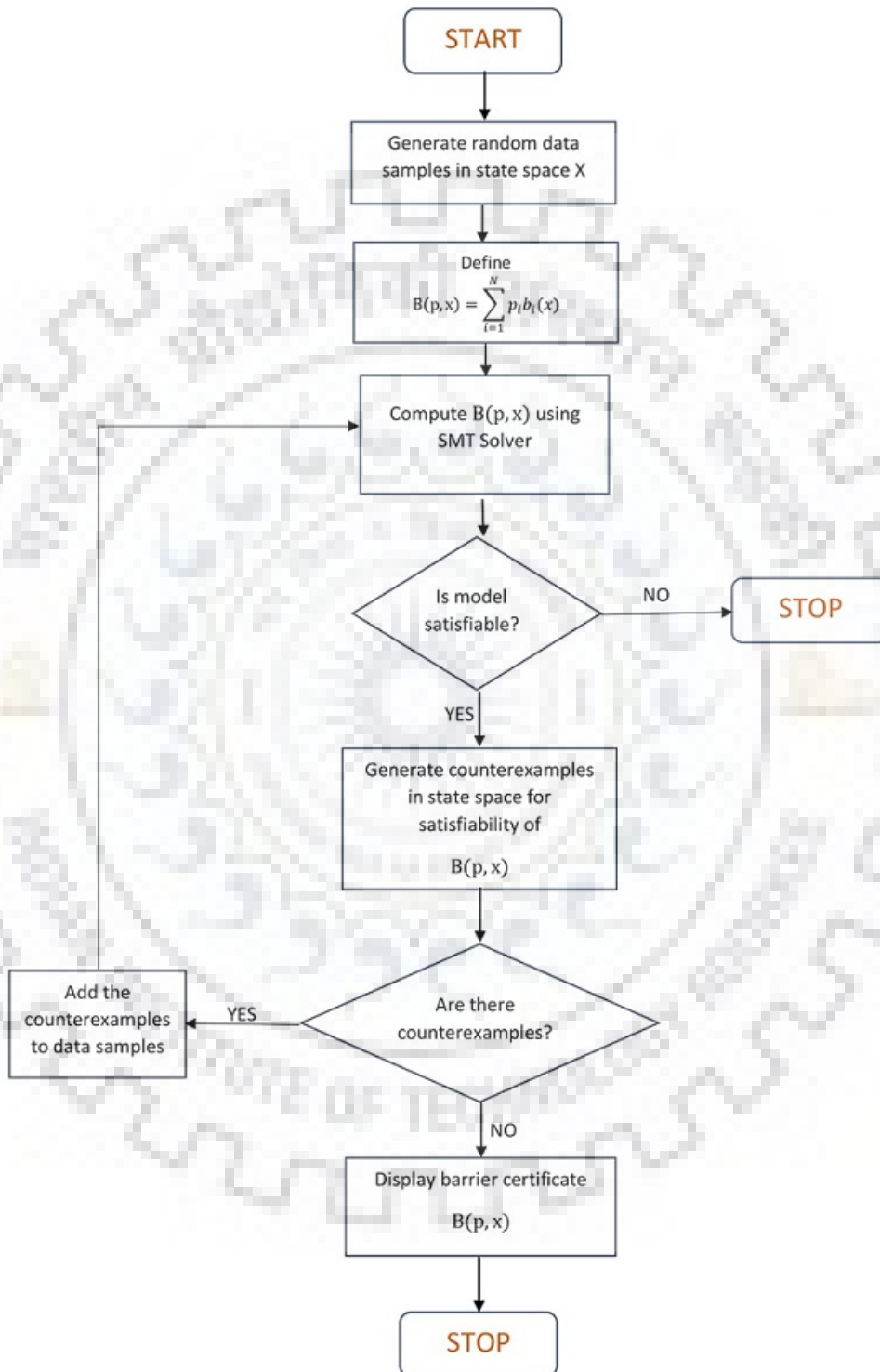


FIGURE 3.2: Flowchart for CEGIS framework

Chapter 4

Controller Synthesis of Discrete-Time Stochastic Systems

4.1 Control Barrier Certificates

As in the case of continuous-time switched stochastic systems, we apply the concept of barrier certificates in order to provide verification to safety problems. In this chapter, however, it must be noted that we only deal with one single safety verification problem, where we are given a region that represents the possible initial conditions of the discrete solution processes x_N and an unsafe region that the processes must avoid at any cost. The safety verification problem, as mentioned before, relies on finding a tight lower bound on probability for property satisfaction of the solution processes, and in case of a safety problem we handle in this chapter, the specification states that the solution processes do not enter an unsafe region. Ensuring low probability in a finite time horizon will give us guarantee regarding the safety of the system.

Here, since we are dealing with discrete time control systems, we have to compute the right control input that will drive the system to safety. For this, we introduce the notion of a control barrier certificate, which is pretty similar to the

barrier certificate in chapter 3, but here, the expectation of the barrier certificate will not only depend on the state of the system, but also on the control input at the current state.

Definition of a control barrier certificate is as follows.

Definition 4.1. A function $B : X \rightarrow \mathbb{R}_0^+$ is a control barrier certificate of a discrete-time stochastic control system $S = (X, V_w, U, w, f)$ with $U = (u_1, u_2, \dots, u_p)$, $p \in \mathbb{N}$ being a finite set of discrete inputs if

$$\bigvee_{u \in U} \mathbb{E}[B(f(x(k), u(k))) \mid x(k), u(k)] \leq B(x(k)) + c \quad (4.1)$$

for all $x \in X, k \in \mathbb{N}_0$ and for a constant $c > 0$

Now, we look at the following lemma and utilize this for our subsequent theorem for safety verification using control barrier certificates.

Lemma 4.2. For a discrete-time stochastic control system $S = (X, V_w, U, w, f)$, let us assume that a control barrier certificate $B : X \rightarrow \mathbb{R}_0^+$ exists with some non negative constant c . Then, for any constant $\lambda > 0$ and any initial condition $x(0) \in X$, the probability that the value of barrier certificate being greater than λ given the initial condition is given by

$$\mathbb{P}\left\{ \sup_{0 \leq t < T_d} B(x(k)) \geq \lambda \mid x(0) \right\} \leq \frac{B(x_0) + cT_d}{\lambda}. \quad (4.2)$$

To compute the tight upper bound on the probability of a reachability problem using barrier certificates, we state the following theorem, that has been the primary work of the author of [17].

Theorem 4.3. For a discrete time stochastic control system $S = (X, V_w, U, W, f)$, consider $X_0, X_1 \subseteq X$. Suppose there exists a control barrier certificate $B : X \rightarrow \mathbb{R}_0^+$ and a constant $c > 0$ such that the condition in definition 4.1 is satisfied and there exists a constant $\gamma \in [0, 1]$ such that

$$B(x) \leq \gamma \quad \forall x \in X_0 \quad (4.3)$$

$$B(x) \geq 1 \quad \forall x \in X_1 \quad (4.4)$$

Then the probability that the solution processes start at X_0 and reach X_1 within a finite time horizon $[0, T_d] \subseteq \mathbb{N}_0$ is upper bounded by $\gamma + cT_d$.

Proof. $B(x(k))$ is a control barrier certificate so 4.2 in 4.2 holds. Since $X_1 \subseteq \{x \in X_s.t.B(x) > 1\}$, we have $\mathbb{P}\{x(k) \in X_1 \text{ for some } 0 < k < T_d \mid x(0) = x_0\} \leq \mathbb{P}\{\sup_{0 < k < T_d} B(x(k)) \geq 1 \mid x(0) = x_0\} \leq \gamma + cT_d \quad \square$

This is a typical optimization problem and we minimize the value of c and γ , while finding the optimum discrete controller values for regions within the state space.

Remark 4.4. The corresponding controller $u(x)$ in the discrete case is given by $u(x) = \{u \in U \mid E[B(f(x, u)) \mid (x, u)] \leq B(x) + c\}$. What it means is that for different regions in state space, we arrive with different control inputs that are active while the solution process lies under those regions and definition 4.1 provides regions of state space in which a given control input is valid and can be given as $X_i : \{x \in X \mid E[B(f(x, u)) \mid (x, u)] \leq B(x) + c\}$ for all $i = \{1, 2, \dots, l\}$ where and $\bigcup_i X_i = X$.

Corollary 4.5. *Let the safety specification φ represent the specification that no solution process that begins in X_0 must reach X_1 . Given the result of Theorem 4.3, the probability that the solution process of S starting from any $x \in X_0$ over time horizon $[0, T) \subset \mathbb{R}_0^+$ satisfies the specification φ under control policy ρ is lower-bounded by*

$$\mathbb{P}_{x_0}^\rho \{\sigma_\xi \models \varphi\} \geq 1 - \mathbb{P}_{x_0}^\rho \{\sigma_\xi \models \neg\varphi\}.$$

4.2 Computation of Control Barrier Certificates

In this section, we once again provide the Counter-Example Guided Inductive Synthesis (CEGIS) framework for searching control barrier certificates of specific forms satisfying conditions in 4.3. The approach uses feasibility solvers for finding barrier certificates of a given parametric form using Satisfiability Modulo

Theories (SMT) solvers such as Z3 [29] and dReal [30]. In order to use the CEGIS framework, we raise following assumption.

Assumption 4.6. System S has compact state-space $X \subset \mathbb{R}^n$ and partition sets X_0 and X_1 are bounded, semi-algebraic sets, *i.e.*, they can be represented by polynomial equalities and inequalities.

We provide the following lemma that allows us to formulate the controller optimization as a satisfiability problem which is required for finding the existence of a control barrier certificate and a corresponding control strategy using the CEGIS approach.

Lemma 4.7. *Suppose assumption 4.6 holds and partition sets X_0, X_1 and X are bounded semi-algebraic sets. If there exists a barrier certificate $B(x)$ such that the following condition is true*

$$\bigwedge_{x \in X} B(x) \geq 0 \quad \bigwedge_{x \in X_0} B(x) \leq \gamma \quad \bigwedge_{x \in X_1} B(x) \geq 1 \quad \bigwedge_{x \in X} \left(\bigvee_{u_i \in U} E[B(f(x, u_i, w)) \mid (x, u_i)] \leq B(x) + c \right) \quad (4.5)$$

Then $B(x)$ satisfies conditions in Theorem 4.3 and

$$u(x) \in u_i \in U \mid \{E[B(f(x, u_i)) \mid x, u_i] \leq B(x) + c\}$$

is the control input that drives the discrete stochastic control system to safety.

In order to utilize CEGIS framework, we consider a barrier certificate of the parametric form $B(p, x) = \sum_{i=1}^k p_i b_i(x)$ with some user-defined (nonlinear) basis functions $b_i(x)$ and unknown coefficients $p_i \in \mathbb{R}, i \in \{1, 2, \dots, k\}$. With this choice of barrier certificate the feasibility expression (4.7) can be rewritten as

$$\begin{aligned} \psi(p, x) := & \left(\bigwedge_{x \in X} B(p, x) \geq 0 \bigwedge_{x \in X_0} B(p, x) \leq \gamma \bigwedge_{x \in X_1} B(p, x) \geq 1 \right. \\ & \left. \bigwedge_{x \in X} \left(\bigvee_{u_i \in U} E[B(p, f(x, u_i, w)) \mid (x, u_i)] \leq B(p, x) + c \right) \right) \end{aligned} \quad (4.6)$$

We denote the obtained candidate barrier certificate with fixed coefficients a_i by $B(a, x)|_a$ and the corresponding feasibility expression by $\psi(a, x)|_a$. Next we obtain counterexample $x \in X$ such that $B(a, x)|_a$ satisfies $\neg\psi(a, x)|_a$. If $\neg\psi(a, x)|_a$ has no feasible solution, then the obtained $B(a, x)|_a$ is a true barrier certificate. If $\neg\psi(a, x)|_a$ is feasible, we update data samples as $\bar{X} = \bar{X} \cup x$ and recompute coefficients a_i iteratively until $\neg\psi(a, x)|_a$ becomes infeasible. For detailed overview on CEGIS procedure we refer readers to [31]. To obtain a tight upper bound on the probability, one can utilize bisection method over c and γ iteratively. The pseudocode for CEGIS framework to compute such barrier certificates is given in Algorithm 1 in chapter 3. In addition, one can also refer to figure 3.2 which describes the flowchart of the CEGIS framework.

Remark 4.8. For the implementation of CEGIS approach and computation of barrier certificate using z3 solver, we must calculate the value of $E[B(f(x, u, w)) \mid (x, u)]$. This expectation value cannot be calculated directly and hence a simple workaround is used. This can be done by considering w as a normal variable. We start by expanding $B(f(x, u, w))$, separating terms without the variable w , terms associated with odd powers of variable w and terms multiplied with even powers of w . Terms without the stochastic variable w can be treated as constants, since x and u are non-stochastic and known. Plain central moments of odd powers of the normal variable w is 0, and hence the expectation of terms with odd powers of w are 0. The plain central moments of the normal variable is given by $\sigma_p(p-1)!!$ where σ is the standard deviation and p is the p^{th} power associated with w . $!!$ denotes double factorial, which is the product of all numbers from 1 to p with the same parity as p . Once we have the expectation of all terms separately, the expectation of $E(B(f(x, u, w)) \mid (x, u))$ is nothing but the sum of the expectations of individual terms.

Chapter 5

Examples and Conclusion

In this chapter, we apply the theorems and implementation technique mentioned in chapters 3 and 4 on examples and provide results that help us assert that our method of probabilistic verification of stochastic systems using barrier certificates is indeed effective and accurate.

5.1 Two Dimensional Switched Stochastic System

Consider a two dimensional switched stochastic system $S = (\mathbb{R}^2, M, \mathcal{M}, F, G)$ with $M = \{1, 2\}$, and dynamics

$$S_1 : \begin{cases} d\xi_1 = -0.1\xi_2^2 dt + dW_{1t}, \\ d\xi_2 = -0.1\xi_1\xi_2 dt + dW_{2t}; \end{cases} \quad (5.1)$$

$$S_2 : \begin{cases} d\xi_1 = -0.1\xi_1^2 dt + dW_{1t}, \\ d\xi_2 = -0.1\xi_1\xi_2 dt + dW_{2t}. \end{cases} \quad (5.2)$$

Let the regions of interest be given as

$$X_0 = \{(x_1, x_2) \in \mathbb{R}^2 \mid (x_1 + 5)^2 + x_2^2 \leq 2.5\},$$

$$X_1 = \{(x_1, x_2) \in \mathbb{R}^2 \mid (x_1 - 5)^2 + (x_2 - 5)^2 \leq 3\},$$

$$X_2 = \{(x_1, x_2) \in \mathbb{R}^2 \mid (x_1 - 4)^2 + (x_2 + 3)^2 \leq 2\}, \text{ and}$$

$$X_3 = \mathbb{R}^2 \setminus (X_0 \cup X_1 \cup X_2).$$

The sets $X_0, X_1, X_2,$ and X_3 are shown in Figure 5.1.

The set of atomic propositions is given by $\Pi = \{p_0, p_1, p_2, p_3\}$, with labeling function $L(x) = p_i$ for any $x \in X_i, i \in \{0, 1, 2, 3\}$. Given an initial state, we are interested in computing a tight lower bound on the probability that the solution process of S over time horizon $[0, T) \subset \mathbb{R}_0^+$ satisfies the following specification:

- If it starts in X_0 , it will always stay away from X_1 or always stay away from X_2 within time horizon $[0, T) \subset \mathbb{R}_0^+$. If it starts in X_2 , it will always stay away from X_1 within time horizon $[0, T) \subset \mathbb{R}_0^+$.

This property can be expressed by the safe-LTL_F formula

$$\varphi = (p_0 \wedge (\Box \neg p_1 \vee \Box \neg p_2)) \vee (p_2 \wedge \Box \neg p_1). \quad (5.3)$$

For this system, we first perform decomposition into sequential reachability for the negation of the given specification, *i.e.*, DFA for $\neg\varphi$ which is given in figure 5.2. This DFA shows us all the words that satisfy $\neg\varphi$, and in principle, all the words that our system must not possess. From figure 5.2, we get $Q_0 = \{q_0\}$ and $F = \{q_3\}$. We first use the DFA to compute all the accepting state runs and then decompose these state runs to simpler subpaths of length 3.

The set of accepting state runs without self-loops for the given example is

$$\mathcal{R} = \{(q_0, q_4, q_3), (q_0, q_1, q_2, q_3), (q_0, q_1, q_4, q_3), (q_0, q_3)\}.$$

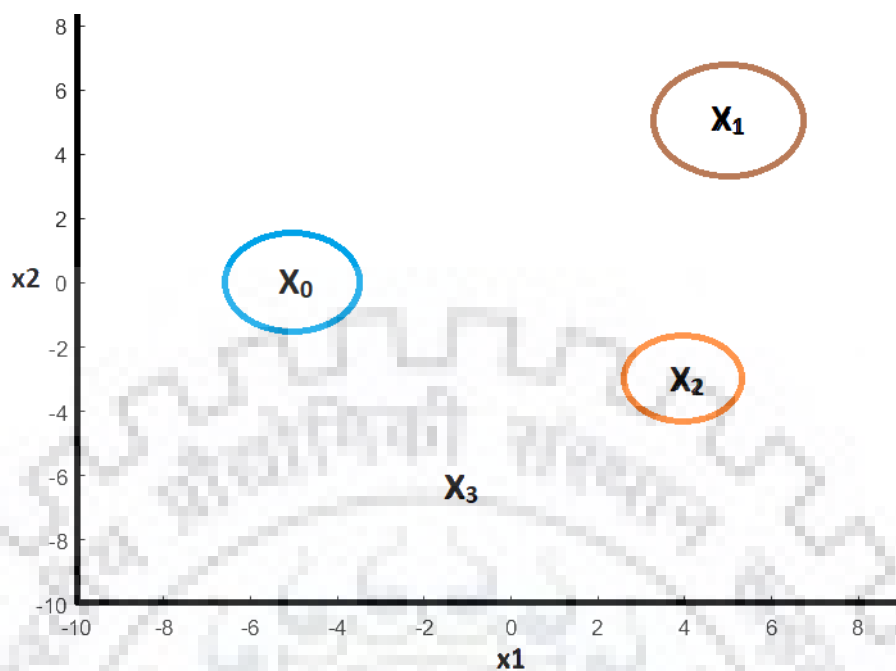


FIGURE 5.1: State space and regions of interest.

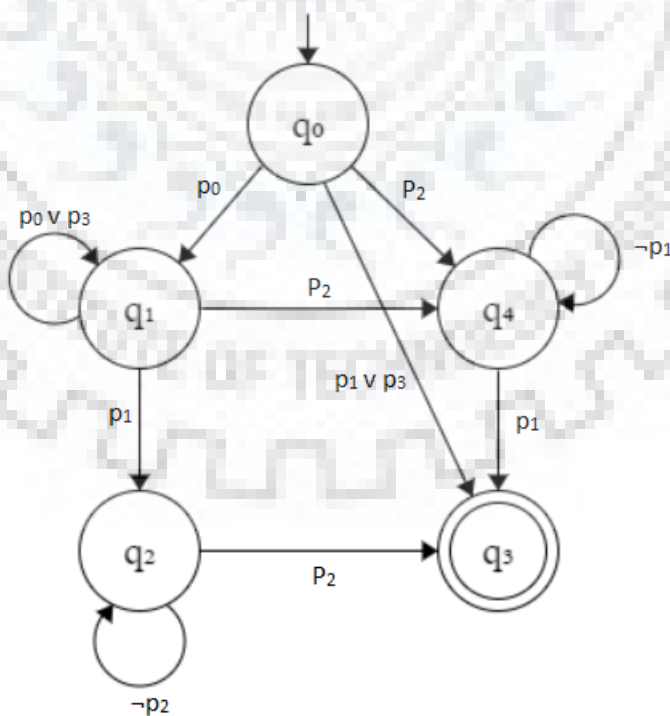


FIGURE 5.2: DFA for $\neg\varphi$.

The sets of \mathcal{R}^p for $p \in \Pi$ are

$$\begin{aligned}\mathcal{R}^{p_0} &= \{(q_0, q_1, q_2, q_3), (q_0, q_1, q_4, q_3)\}, \mathcal{R}^{p_1} = \{(q_0, q_3)\}, \\ \mathcal{R}^{p_2} &= \{(q_0, q_4, q_3)\}, \mathcal{R}^{p_3} = \{(q_0, q_3)\}.\end{aligned}$$

The sets $\mathcal{P}^p(\mathbf{q})$ for $\mathbf{q} \in \mathcal{R}^p$ are as follows:

$$\begin{aligned}\mathcal{P}^{p_0}(q_0, q_1, q_2, q_3) &= \{(q_0, q_1, q_2), (q_1, q_2, q_3)\}, \\ \mathcal{P}^{p_0}(q_0, q_1, q_4, q_3) &= \{(q_0, q_1, q_4), (q_1, q_4, q_3)\}, \\ \mathcal{P}^{p_2}(q_0, q_4, q_3) &= \{(q_0, q_4, q_3)\}, \mathcal{P}^{p_1}(q_0, q_3) = \mathcal{P}^{p_3}(q_0, q_3) = \emptyset.\end{aligned}$$

Note that each of the element of $\mathcal{P}^p(q)$ for $p \in \Pi$ is a simple reachability problem for which we use the concept of barrier certificate in accordance with theorems 3.3 or 3.4.

To compute the upper bound on reachability probabilities in each element of $\mathcal{P}^p(q)$ for all $p \in \Pi$, we use the SMT solver Z3 and CEGIS approach to compute common barrier certificates and minimize values of c and γ using bisection method. The obtained values of c and γ for each of the elements of $\mathcal{P}^p(\mathbf{q})$ and their computed upper bounds $\gamma + cT$ are listed in Table 5.1. Now, using Theorem 3.6 we get,

$$\begin{aligned}\mathbb{P}_{x_0}\{\sigma_\xi \models \neg\varphi\} &\leq (0.002038 \times 0.03437) + (0.002050 \times 1) \\ &= 0.00212 \quad \forall x_0 \in L^{-1}(p_0); \\ \mathbb{P}_{x_0}\{\sigma_\xi \models \neg\varphi\} &\leq 0.03437 \quad \forall x_0 \in L^{-1}(p_2); \text{ and} \\ \mathbb{P}_{x_0}\{\sigma_\xi \models \neg\varphi\} &= 1 \quad \forall x_0 \in L^{-1}(p_1) \text{ and } \forall x_0 \in L^{-1}(p_3).\end{aligned}$$

The lower bound on the probabilities that ξ starts at any $x_0 \in L^{-1}(p)$, $p \in \Pi$ satisfying safe-LTL $_{F \setminus \emptyset}$ property (5.3) over time horizon $T = 10$ are

$$\begin{aligned}\mathbb{P}_{x_0}\{\sigma_\xi \models \varphi\} &\geq 0.99788 \quad \forall x_0 \in L^{-1}(p_0); \\ \mathbb{P}_{x_0}\{\sigma_\xi \models \varphi\} &\geq 0.96563 \quad \forall x_0 \in L^{-1}(p_1); \text{ and} \\ \mathbb{P}_{x_0}\{\sigma_\xi \models \varphi\} &\geq 0 \quad \forall x_0 \in L^{-1}(p_1) \text{ and } \forall x_0 \in L^{-1}(p_3).\end{aligned}$$

TABLE 5.1: Values of c and γ for all $\nu \in \mathcal{P}^p(\mathbf{q})$, $\mathbf{q} \in \mathcal{R}^p$

ν	c	γ	$\gamma + cT$
(q_0, q_1, q_2)	1.953125×10^{-4}	9.765×10^{-5}	0.002050
(q_1, q_2, q_3)	0.25	0.25	1
(q_0, q_1, q_4)	1.853125×10^{-4}	1.853125×10^{-4}	0.002038
(q_1, q_4, q_3)	1.953125×10^{-4}	9.765×10^{-5}	0.002050
(q_0, q_4, q_3)	0.003125	0.003125	0.003437

For this computation, we used polynomial barrier certificates of order 5 each with 21 coefficients for all ν . Each individual computation takes on an average 3 hours.

5.2 Temperature Control System

Consider a room temperature control system governed by the following stochastic difference equation adapted from [32].

$$x(k+1) = x(k) + \tau_s(\alpha_e(T_e - x(k)) + \alpha_H(T_h - x(k))u(k)) + 0.1w(k)$$

$x(k)$ denotes the state of the system, *i.e.*, the temperature of the room. $u(k)$ is the control input that represents the heater value and $w(k)$ is a standard normal random variable that represents uncertainties in the system operation. τ_s is the sampling time of 1 minute, $\alpha_e = 0.008$ and $\alpha_h = 0.0036$ are heat exchange coefficients. $T_h = 55^\circ\text{C}$ and $T_e = 15^\circ\text{C}$ are the heater temperature and ambient temperature respectively.

The regions of interest is given by $X_0 = [21, 22]$ and $X_1 = [0, 20]$, $X_2 = [23, 45]$ and $X_3 = X \setminus (X_0 \cup X_1 \cup X_2)$ and the objective of our problem is to compute a control policy that any solution process that starts at X_0 must not reach any point in either X_1 or X_2 . The specification φ for a set of atomic propositions $\Pi = \{p_0, p_1, p_2, p_3\}$ is given as $\varphi = p_0 \wedge \neg(p_1 \vee p_2)$. The control policy must be optimized in such a way that we get the tightest upper bound of probability that this specification is satisfied.

We consider that the control input takes the values within the set $U = [0, 0.5, 1]$ and for each state that the system visits, one of these controller values is assigned such that the system is not driven to an unsafe region. We initialize the computation by assuming that there exists a polynomial control barrier certificate of the order 4. We initialize the values of c and γ with 0.002 and 0.5 respectively. We here consider the horizon to be of length 50, equivalent to 50 minutes time duration.

By using z3 solver and CEGIS approach, we obtain the barrier certificate given by:

$$B(x) = 0.197561325479868x^4 - 16.9985338044351x^3 + 548.479208526386x^2 - 7865.64018165559x + 42300.6247825696$$

The minimum values of c and γ are obtained as

$$c = 0.0005$$

$$\gamma = 0.015625 + 0.0005 \times 50 = 0.040625$$

Hence, the upper bound on the probability of reachability is given by:

$$\mathbb{P}_{x_0}^p \{L(x_N) \mid \varphi\} = 0.959375$$

for all $x_0 \in L^{-1}(p_0)$

Plot of this barrier certificate as a function of state is shown in figure 5.3. As one can see, for the initial region of $X_0 = [21, 22]$, the value of $B(x)$ is less than $\gamma = 0.040625$ and $B(x) > 1$ for regions $X_1 = [0, 20]$ and $X_2 = [23, 50]$.

The corresponding controller obtained is:

$$u(x) = \min\{u_i \in U \mid E[B(f(x, u_i)) \mid (x, u_i)] \leq B(x) + c\}$$

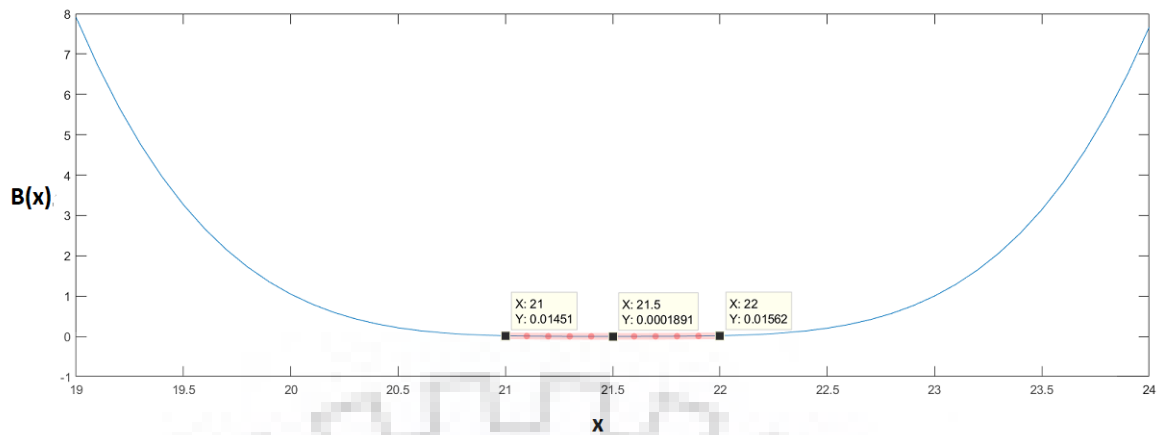


FIGURE 5.3: Barrier certificate as a function of state.

The plot of the controller $u(x)$ obtain in accordance with state x is shown in figure 5.4 and multiple realizations of state evolution with different initial conditions over the given time horizon is represented in figure 5.5. One can see that in no realization is the state reaching the unsafe set. This proves that our method is extremely effective for safety verification of stochastic systems over a finite horizon of time.

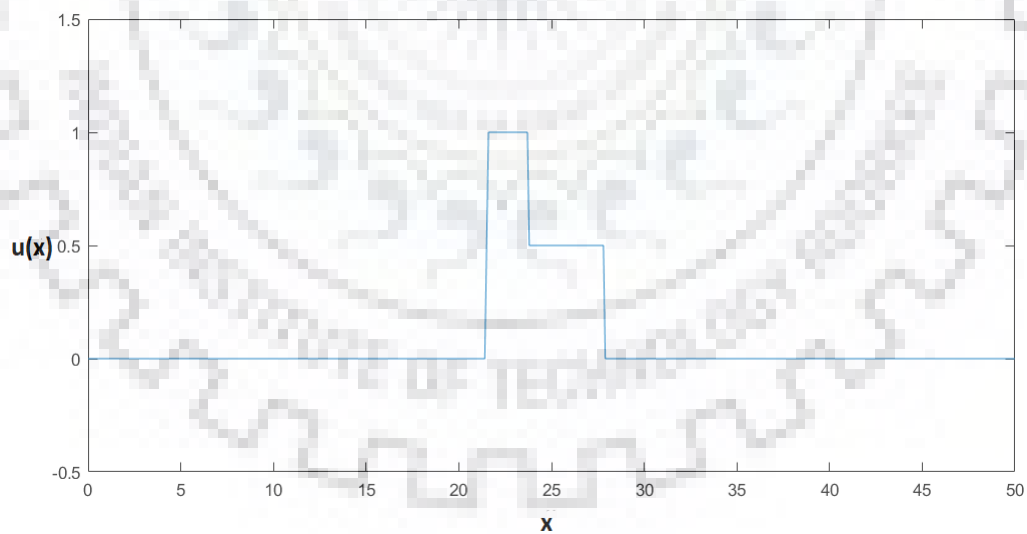


FIGURE 5.4: Controller values as a function of state

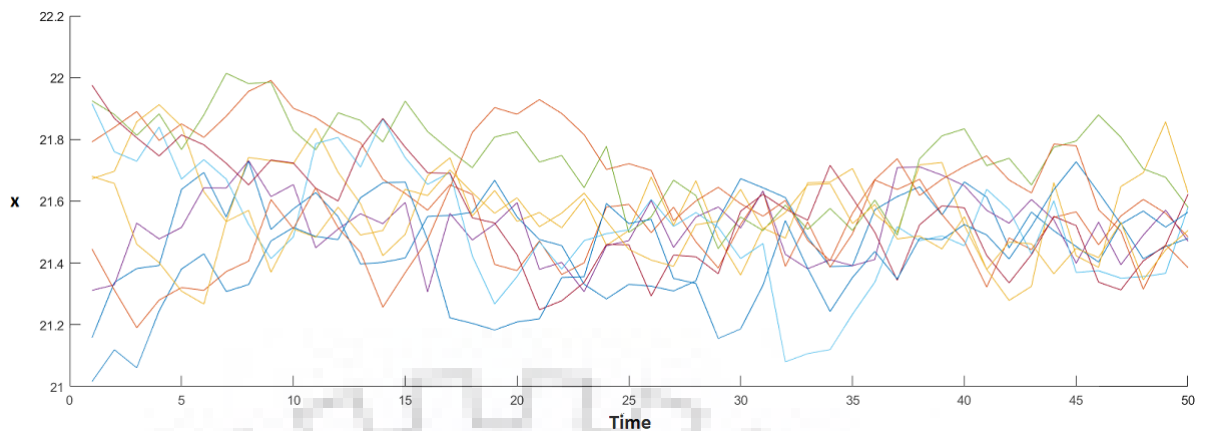


FIGURE 5.5: 10 realisations of state vs time.

5.3 Conclusion

In this thesis, a discretization-free approach for safety verification of stochastic system has been proposed as an alternate to existing state-space discretization methods. The approach uses a combination of barrier certificates and automata based verification in order to provide effective results with the lower bound of the probability that a given stochastic system satisfies a wide class of Linear Temporal Logic Properties. In order to do this, the specification was first decomposed into simpler reachability problems using automata based approach and then probability for each reachability problem was handled using barrier certificate approach. These individual results were combined to obtain the lower bound on the probability of property satisfaction. Both continuous time and discrete time stochastic systems were handled. Novel theory for barrier certificate approach in continuous-time switched stochastic system was developed and results were obtained through SMT based solvers and CEGIS approach, for two particular examples in continuous-time and discrete-time. While handling discrete systems, only a fraction of the LTL properties called safety properties were dealt with. A generalized code was built for implementation for application to higher order systems with a wide class of dynamics.

In the future, the generalized code can be converted into a full-fledged tool box to be made available to public. In addition, the barrier certificate approach can be utilized for a wider class of systems such as interconnected stochastic

systems, where the existence barrier certificates could be found for verification of individual subsystems and a compositionality result can be obtained for verification for the whole interconnected system.



Bibliography

- [1] Christel Baier and Joost-Pieter Katoen. *Principles of model checking*. The MIT Press, Cambridge, Mass., 2008. ISBN 026202649X.
- [2] E. M. Clarke, Orna Grumberg, and Doron Peled. *Model checking*. MIT Press, Cambridge, MA and London, 1999. ISBN 0262032708.
- [3] J. R. Burch, E. M. Clarke, K. L. McMillan, D. L. Dill, and L. J. Hwang. Symbolic model checking: 1020 states and beyond. *Information and Computation*, 98(2):142–170, 1992. ISSN 08905401. doi: 10.1016/0890-5401(92)90017-A.
- [4] Armin Biere, Alessandro Cimatti, Edmund M. Clarke, and Yunshan Zhu. Symbolic model checking without bdds. In *Proceedings of the 5th International Conference on Tools and Algorithms for Construction and Analysis of Systems, TACAS '99*, pages 193–207, Berlin, Heidelberg, 1999. Springer-Verlag. ISBN 3-540-65703-7. URL <http://dl.acm.org/citation.cfm?id=646483.691738>.
- [5] Arnaud Hélias, François Guerrin, and Jean-philippe Steyer. Abstraction of continuous system trajectories into timed automata. *IFAC Proceedings Volumes*, 37(18):309–314, 2004. ISSN 14746670. doi: 10.1016/S1474-6670(17)30764-4.
- [6] N. Giorgetti, G. J. Pappas, and A. Bemporad. Bounded model checking of hybrid dynamical systems. In *2005 44th IEEE conference on decision and control & European control conference*, pages 672–677, New York, 2005. IEEE Control Systems Society. ISBN 0-7803-9567-0. doi: 10.1109/CDC.2005.1582233.

- [7] R. Alur, T. A. Henzinger, G. Lafferriere, and G. J. Pappas. Discrete abstractions of hybrid systems. *Proceedings of the IEEE*, 88(7):971–984, 2000. ISSN 0018-9219.
- [8] Antoine Girard and George J. Pappas. Approximation metrics for discrete and continuous systems. *IEEE Transactions on Automatic Control*, 52(5):782–798, 2007. ISSN 0018-9286.
- [9] Sadegh Esmail Zadeh Soudjani and Alessandro Abate. Adaptive and sequential gridding procedures for the abstraction and verification of stochastic processes. *SIAM Journal on Applied Dynamical Systems*, 12(2):921–956, 2013.
- [10] Alessandro Abate, Joost-Pieter Katoen, and Alexandru Mereacre. Quantitative automata model checking of autonomous stochastic hybrid systems. In Emilio Frazzoli and Radu Grosu, editors, *Hybrid systems*, page 83, Berlin and New York, 2011. Springer. ISBN 9781450306294.
- [11] Gerardo Lafferriere, George J. Pappas, and Sergio Yovine. Symbolic reachability computation for families of linear vector fields. *Journal of Symbolic Computation*, 32(3):231–253, 2001. ISSN 07477171.
- [12] X. D. Koutsoukos and D. Riley. Computational methods for verification of stochastic hybrid systems. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 38(2):385–396, 2008. ISSN 1083-4427.
- [13] Manuela L. Bujorianu and John Lygeros. Reachability questions in piecewise deterministic markov processes. In O. Maler and Amir Pnueli, editors, *Hybrid systems*, volume 2623 of *Lecture notes in computer science*, 0302-9743, pages 126–140. Springer, Berlin and London, 2003. ISBN 978-3-540-00913-9.
- [14] S. Prajna. Barrier certificates for nonlinear model validation. *Automatica*, 42(1):117–126, 2006. ISSN 00051098. doi: 10.1016/j.automatica.2005.08.007.
- [15] S. Prajna, A. Jadbabaie, and G. J. Pappas. A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control*, 52(8):1415–1428, 2007.

- [16] C. Huang, Xi Chen, Wang Lin, Zhengfeng Yang, and Xuandong Li. Probabilistic safety verification of stochastic hybrid systems using barrier certificates. *ACM Transactions on Embedded Computing Systems*, 16(5s):1–19, 2017. ISSN 15399087. doi: 10.1145/3126508.
- [17] Pushpak Jagtap, Sadegh Soudjani, and Majid Zamani. Temporal logic verification of stochastic systems using barrier certificates. In *International Symposium on Automated Technology for Verification and Analysis*, pages 177–193. Springer, 2018.
- [18] B. Øksendal. *Stochastic Differential Equations: An Introduction with Applications*. Springer-Verlag, Berlin, 2000.
- [19] L Chris G Rogers and David Williams. *Diffusions, Markov processes and martingales: Volume 2, Itô calculus*, volume 2. Cambridge university press, 2000.
- [20] Orna Kupferman and MosheY Vardi. Model checking of safety properties. In *International Conference on Computer Aided Verification*, pages 172–183. Springer, 1999.
- [21] I. Saha, R. Ramaithitima, V. Kumar, G. J. Pappas, and S. A. Seshia. Automated composition of motion primitives for multi-robot systems from safe LTL specifications. In *2014 IEEE/RSJ International Conference on Intelligent Robots and Systems*, pages 1525–1532, 2014.
- [22] Giuseppe De Giacomo and Moshe Y Vardi. Synthesis for LTL and LDL on finite traces. In *International Joint Conference on Artificial Intelligence*, volume 15, pages 1558–1564, 2015.
- [23] Alexandre Duret-Lutz, Alexandre Lewkowicz, Amaury Fauchille, Thibaud Michaud, Etienne Renault, and Laurent Xu. Spot 2.0: A framework for LTL and ω -automata manipulation. In *International Symposium on Automated Technology for Verification and Analysis*, pages 122–129. Springer, 2016.
- [24] Jesper G Henriksen, Jakob Jensen, Michael Jørgensen, Nils Klarlund, Robert Paige, Theis Rauhe, and Anders Sandholm. Mona: Monadic second-order

- logic in practice. In *International Workshop on Tools and Algorithms for the Construction and Analysis of Systems*, pages 89–110. Springer, 1995.
- [25] Jacob Steinhardt and Russ Tedrake. Finite-time regional verification of stochastic non-linear systems. *The International Journal of Robotics Research*, 31(7):901–923, 2012. ISSN 0278-3649.
- [26] Harold J Kushner. On the stability of stochastic dynamical systems. *Proceedings of the National Academy of Sciences*, 53(1):8–12, 1965.
- [27] Mrinal K Ghosh, Aristotle Arapostathis, and Steven I Marcus. Optimal control of switching diffusions with application to flexible manufacturing systems. *SIAM Journal on Control and Optimization*, 31(5):1183–1204, 1993.
- [28] Stuart J. Russell and Peter Norvig. *Artificial Intelligence: A Modern Approach*. Pearson Education, 2 edition, 2003. ISBN 0137903952.
- [29] L. de Moura and N. Bjørner. Z3: An efficient SMT solver. In C. R. Ramakrishnan and Jakob Rehof, editors, *Tools and algorithms for the construction and analysis of systems*, volume 4963 of *Lecture Notes in Computer Science*, pages 337–340. Springer, Berlin, 2008. ISBN 978-3-540-78799-0. doi: 10.1007/978-3-540-78800-3{\textunderscore}24.
- [30] Sicun Gao, Soonho Kong, and Edmund M. Clarke. dReal: An SMT solver for nonlinear theories over the reals. In Maria Paola Bonacina, editor, *Automated deduction - CADE-24*, volume 7898 of *LNCS sublibrary: SL 7 - artificial intelligence*, pages 208–214. Springer, Heidelberg, 2013. ISBN 978-3-642-38573-5. doi: 10.1007/978-3-642-38574-2{\textunderscore}14.
- [31] H. Ravanbakhsh and S. Sankaranarayanan. A class of control certificates to ensure reach-while-stay for switched systems. In *SYNT@CAV*, 2017.
- [32] Pushpak Jagtap and Majid Zamani. Quest: A tool for state-space quantization-free synthesis of symbolic controllers. In Nathalie Bertrand and Luca Bortolussi, editors, *Quantitative evaluation of systems*, volume 10503 of *LNCS sublibrary. SL 1, Theoretical computer science and general issues*, pages 309–313. Springer, Cham, Switzerland, 2017. ISBN 978-3-319-66334-0.