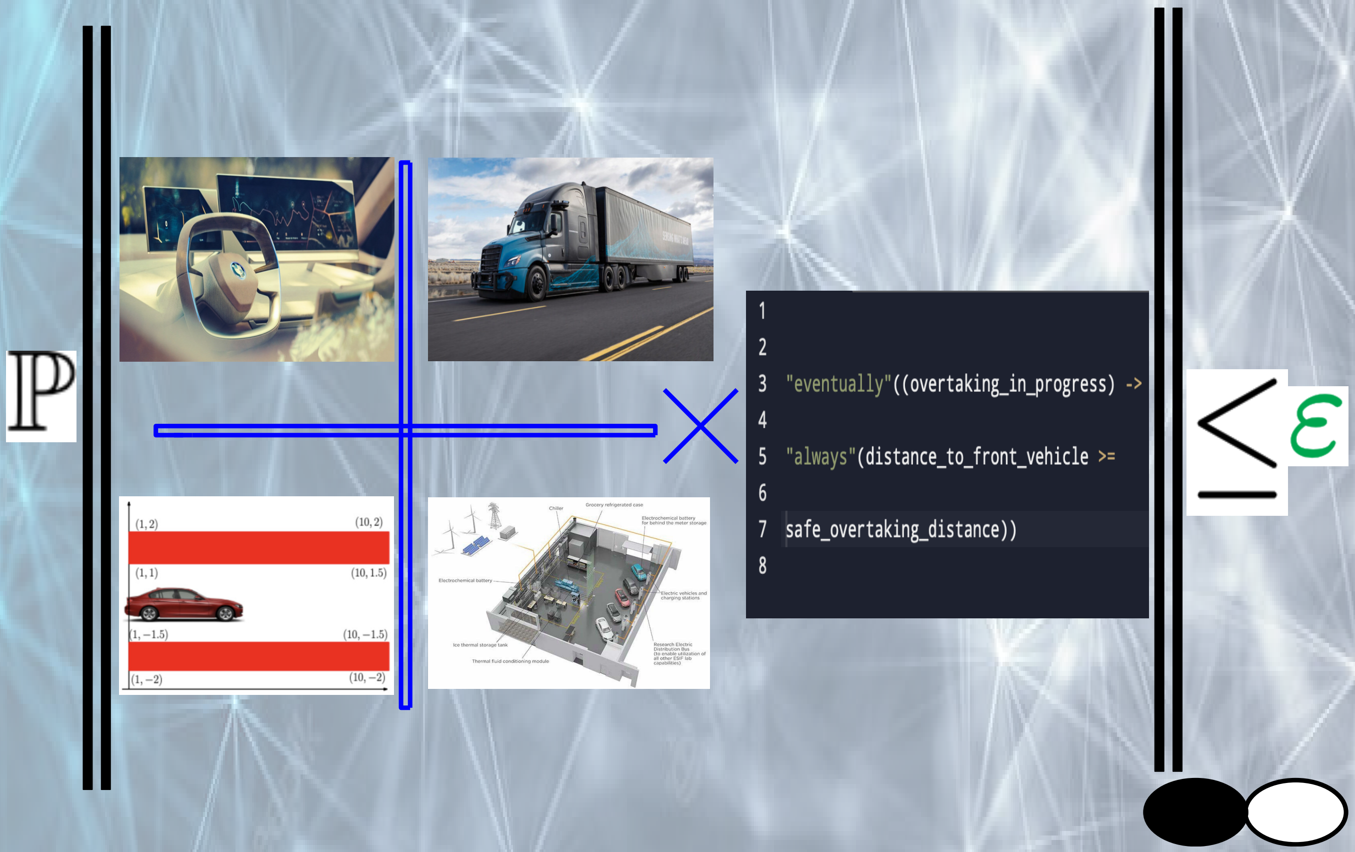
Machine Learning and Data-Driven Techniques for Verification and Synthesis of Cyber-Physical Systems

BY

Ali Salamati


ℙ
(1, 2)
(10, 2)
(1, 1)
(10, 1.5)
(1, −1.5)
(10, −1.5)
(1, −2)
(10, −2)
Chiller
Grocery refrigerated case
Electrochemical battery for behind the meter storage
Electrochemical battery
Electric vehicles and charging stations
Ice thermal storage tank
Thermal fluid conditioning module
Research Electric Distribution Bus (to enable utilization of all other ESIF lab capabilities)
≤
ε

```


"eventually"((overtaking_in_progress) ->

"always"(distance_to_front_vehicle >=

safe_overtaking_distance))

```

Machine Learning and Data-driven Techniques for Verification and Synthesis of Cyber-Physical Systems

Ali Salamati

Dissertation
an der Fakultät für Mathematik, Informatik und Statistik
der Ludwig–Maximilians–Universität
München

vorgelegt von
Ali Salamati
aus dem Iran

München, 2023
Tag der Einreichung: 25/07/2023

Erstgutachter: Prof. Majid Zamani

Zweitgutachter: Prof. Sadegh Soudjani

Drittgutachter: Prof. Raphael Jungers

Tag der mündlichen Prüfung: 04/10/2023

To
My beautiful wife for her unconditional love and patience,
My lovely parents and brother for their unconditional support, and
My wonderful people in Iran

Eidesstattliche Versicherung

Hiermit erkläre ich, Ali Salamati, an Eides statt, dass die vorliegende Dissertation ohne unerlaubte Hilfe gemäß Promotionsordnung vom 12.07.2011, § 8, Abs. 2 Pkt. 5, angefertigt worden ist.

München, 25.07.2023
Ali Salamati

Contents

List of Figures

List of Tables

Zusammenfassung

Sicherheit und Leistung sind die wichtigsten Anforderungen bei der Konzeption und Realisierung komplexer Systeme. Nehmen wir ein selbstfahrendes Auto, das nicht mit bestimmten Sicherheitsfunktionen ausgestattet ist: Es kann tödliche Unfälle, schwere Verletzungen oder gravierende Schäden an Mensch und Umwelt verursachen. Daher ist eine strenge Sicherheitsanalyse erforderlich, um die korrekte Ausführung von Funktionalitäten in vielen sicherheitskritischen Anwendungen sicherzustellen. Modellbasierte Ansätze zur Erfüllung solchen Anforderungen wurden in der Literatur ausführlich untersucht. Allerdings ist ein genaues Modell des Systems in vielen praktischen Szenarien nicht immer verfügbar. Daher fokusiert sich diese Dissertation auf datengesteuerte Methoden und Techniken des maschinellen Lernens, um diese Herausforderung zu lösen.

Zunächst gehen wir davon aus, dass nur ein unvollständiges parametrisiertes Modell des Systems verfügbar ist. Das Hauptziel ist die Untersuchung der formalen Verifikation linearer zeitinvarianter Systeme in Bezug auf ein Fragment zeitlogischer Spezifikationen, für den Fall, in dem nur eine partielle Kenntnis des Modells verfügbar ist. Das bedeutet, ein parametrisiertes Modell des Systems ist bekannt, doch die genauen Werte der Parameter sind unbekannt. Wir liefern ein probabilistisches Maß für die Erfüllung der Spezifikation durch Trajektorien des Systems unter dem Einfluss von bestimmten Unsicherheiten. Wir gehen davon aus, dass diese Spezifikationen in Form von Formeln der zeitlichen Logik ausgedrückt werden, und bieten einen Ansatz, der sich auf die Erfassung von Input-Output-Daten des Systems stützt und die Bayes'sche Inferenz auf die erfassten Daten anwendet, um mehr Vertrauen in die Erfüllung der Spezifikation zu legen.

Zweitens gehen wir davon aus, dass wir keine Kenntnis über das Modell des Systems haben und nur Zugang zu den Input-Output-Daten. Wir untersuchen Verifikations- und Syntheseprobleme für Sicherheitsspezifikationen über unbekannte zeitdiskrete stochastische Systeme. Wenn ein Modell des Systems verfügbar ist, wurde die Idee der Grenzzertifikate erfolgreich angewendet, um die Erfüllung von Sicherheitsspezifikationen zu gewährleisten. Hier formulieren wir die Berechnung von Barrierezertifikaten als ein robustes konvexes Programm (RCP). Die Lösung des erfassten RCP ist im Allgemeinen komplex, da das Modell des Systems unbekannt ist, welches in einer der Nebenbedingungen des RCP erscheint. Wir schlagen einen datengetriebenen Ansatz vor, der die unendlich Anzahl von Nebenbedingungen im RCP durch eine endliche Anzahl von Nebenbedingungen ersetzt, indem endlich viele Zufallsproben aus den Trajektorien des Systems genommen werden. Auf diese Weise ersetzen wir das ursprüngliche RCP durch ein konvexes Szenarioprogramm (SCP) und zeigen, wie man ihre Optimierung in Beziehung setzt. Wir garantieren, dass die Lösung des SCP eine Lösung des RCP mit a priori garantiertem Vertrauen ist, wenn die Anzahl der Stichproben größer als ein bestimmter Wert ist. Dies liefert eine untere Grenze für die Sicherheitswahrscheinlichkeit des ursprünglichen unbekannten Systems zusammen mit einem Regler im Falle der Synthese.

Abschließend schlagen wir drei Lösungen vor, um die hohe Notwendigkeit an Daten in unserem Ansatz zu bewältigen. Der erste Ansatz - der Wait-and-Judge-Ansatz - kontrolliert eine Bedingung über den optimalen Wert des konvexen Szenarioprogramms (SCP) unter Verwendung einer festen Anzahl von Stichproben, einer unteren Grenzwahrscheinlichkeit und der gewünschten Sicherheit für die Erfüllung der Spezifikationen. Der zweite Ansatz, der auf Wiederholung basierende Szenarien-Ansatz löst mit Hilfe iterativem Vorgehen das SCP mit Stichproben. Außerdem überprüft dieser die Durchführbarkeit und das gewünschte Fehlermaß. Eine Sicherheitsbedingung wird verifiziert, was die Berechnung einer unteren Grenze für die Erfüllung der Sicherheitskriterien ermöglicht. Der dritte Ansatz ist, der "Warten, Beurteilen und Wiederholen"- Ansatz. Auch diese Struktur löst das SCP iterativ und basierend auf computer berechneten Bedingungen bis eine Machbarkeitsbedingung erfüllt ist. Wenn die Sicherheitsbedingung erfüllt ist, gilt das System als sicher mit einer unteren Wahrscheinlichkeitsgrenze, die mit Hilfe des Optimierer der erfolgreichen Iteration berechnet wird.

Abstract

Safety and performance are the most important requirements for designing and manufacturing complex life-critical systems. Consider a self-driving car which is not equipped with certain safety functionalities. It can cause fatal accidents, severe injuries, or serious damages to the environment. Hence, rigorous analysis required to ensure the correctness of functionalities in many safety-critical applications. Model-based approaches for satisfying such requirements have been studied extensively in the literature. Unfortunately, a precise model of the system is not always available in many practical scenarios. Hence, in this thesis we focus on data-driven methods and machine learning techniques to tackle this challenge.

First, we assume that only an incomplete parameterized model of the system is available. The main goal is to study formal verification of linear time-invariant systems with respect to a fragment of temporal logic specifications when only a partial knowledge of the model is available, i.e., a parameterized model of the system is known but the exact values of the parameters are unknown. We provide a probabilistic measure for the satisfaction of the specification by trajectories of the system under the influence of uncertainty. We assume that these specifications are expressed as signal temporal logic formulae and provide an approach that relies on gathering input-output data from the system. We employ Bayesian inference on the collected data to associate a notion of confidence with the satisfaction of the specification.

Second, we assume that we do not have any knowledge about the model of the system and just have access to input-output data from the system. We study verification and synthesis problems for safety specifications over unknown discrete-time stochastic systems. When a model of the system is available, notion of barrier certificates have been successfully applied for ensuring the satisfaction of safety specifications. Here, we formulate the computation of barrier certificates as a robust convex program (RCP). Solving the acquired RCP is difficult in general because the model of the system that appears in one of the constraints of the RCP is unknown. We propose a data-driven approach that replaces the uncountable number of constraints in the RCP with a finite number of constraints by taking finitely many random samples from the trajectories of the system. We thus replace the original RCP with a scenario convex program (SCP) and show how to relate their optimizers. We guarantee that the solution of the SCP is a solution of the RCP with a priori guaranteed confidence when the number of samples is larger than a specific value. This provides a lower bound on the safety probability of the original unknown system together with a controller in the case of synthesis.

Lastly, to address the high demand for data in our data-driven barrier-based approach, we propose three remedies. First, the wait-and-judge approach that checks a condition over the optimal value of the SCP using a fixed number of samples, ensuring a lower bound probability and the desired confidence for satisfying safety specifications. Second, the repetition-based scenario framework that iteratively solves the SCP with samples, checking feasibility and achieving the desired violation error. A safety condition is verified, enabling the computation of a lower bound for safety satisfaction. Third, the wait, judge, and repeat framework that solves the SCP iteratively until a feasibility condition, based on computed support constraints, is met. If the safety condition is satisfied, the system is considered safe with a lower bound probability determined using the optimizer of the successful iteration.

Acknowledgments

This thesis summarizes four years of research studies conducted at Ludwig Maximilian University of Munich, Germany. I would like to express my sincere gratitude to all the individuals who provided invaluable assistance and support, without whom the completion of this thesis would not have been possible.

First and foremost, I would like to express my deepest gratitude to my supervisor, Prof. Majid Zamani. Throughout my journey during my PhD, he has been a true hero, offering huge support with his wisdom, enthusiasm, and patience. His generous guidance and support made the completion of this thesis possible. Not only did he provide scientific support, but he also acted as a kind teacher, offering guidance and support in various aspects of my personal life.

Second and also foremost, I would like to express my deepest thanks to my advisor, Prof. Sadegh Soudjani, who has been like a true brother and friend to me during these four years. He has always supported me unconditionally through the ups and downs of my research. He never left me alone in this way, as he promised from the first day. I sincerely hope to have the great honor of having him by my side, supporting me throughout my future endeavors in both my professional and personal life.

Besides, I must thank members of my research group, HyConSys Lab. Our weekly group meetings were essential in moving the research forward. Especially when I first joined the group, I received a tremendous amount of support in finding my own path in research. My special thanks go to Mahendra, my quiet and nice roommate, for the beautiful times we spent together, and also to Navid for the fruitful discussions we had on every aspect of life, even during the COVID-19 pandemic. I also need to thank all members of SOSY research group that I had the privilege to meet them during lunch times and many other activities. Special thanks here go to Thomas for all the wonderful moments we spent together, including hiking, cycling, running, swimming, bouldering, going to Biergartens and restaurants, and also for the very pleasant conversations. I hope he enjoys his time in South America this summer. I also would like to thank all my friends and colleagues at NRI and UT.

I wish to sincerely extend my profound gratitude to Prof. Taghirad, my master's supervisor that I still have his full support from behind of thousands of kilometers and many years. Special thanks again go to Prof. Ghazizadeh, former president of NRI, who courageously invented new rules instead of just sticking to the old-fashioned regulations and provided researchers like me with the opportunity to extend our abilities. I hope that

I have the privilege to serve my country at some point to have a little more contribution in making a better world for everyone.

I would also like to express my heartfelt gratitude to Swantje, Barbara, Lieke, Janet, Siyuan, Teymour, Vishnu, Mehrad, Navid, Bernhard, Thomas, Stephan, Felix, Sebastian, Oliver, Mahendra, and Mahmoud for their valuable and constructive comments on various parts of this thesis, which have greatly enhanced its quality.

I could not find words that bear the weight of my immense gratitude towards my family. A special thanks goes to my awesome and pretty wife, Fatemeh, for her tender love, unflappable patience, and unconditional support. Additionally, I extend unique thanks to my brother, Mahmoud, for simply being much beyond a brother. Last but not least, exceptional thanks to my lovely parents for their limitless support.

Chapter 1

Introduction

1.1 Motivation

Ensuring safety and temporal requirements on cyber-physical systems is becoming more important in many applications including self-driving cars, power grids, traffic networks, and integrated medical devices. In recent years, autonomous driving has emerged as a prominent application within the realm of cyber-physical systems, capturing substantial attention. For example, in 2023, Mercedes-Benz made history by becoming the world's pioneering automaker to attain certification for highly automated driving at Level 3, specifically for use on US roads in Nevada. It had also obtained this certification for driving on Germany's autobahns before. This milestone marks a significant advancement for automotive technology as DRIVE PILOT sets new benchmarks, standing out as the premier and sole production-ready Level 3 system authorized for deployment on public freeways in the USA. BMW also presented concept of BMW Vision iNEXT, which is a groundbreaking vehicle that showcases advanced autonomous driving capabilities. As a key part of BMW's electric and autonomous vehicle strategy, the iNEXT combines cutting-edge technologies to offer a seamless and intelligent driving experience. Equipped with level 3 autonomous driving capabilities, the BMW iNEXT allows for hands-off driving in specific conditions (Fig. 1.1). Alphabet's Waymo has recently launched an impressive Level 4 self-driving taxi service in Arizona. This momentous step comes after conducting rigorous testing of driverless cars for over a year and covering an astounding distance of more than 10 million miles, all without the need for a safety driver in the seat. In autonomous driving an array of sensors, including cameras, radar, and LiDAR, along with advanced software algorithms to perceive and interpret the surrounding environment accurately. This enables the vehicle to make real-time decisions, maintain lane control, and adjust its speed based on traffic conditions.

Another application of cyber-physical systems is the integration of electric vehicles (EVs) and their charging infrastructure with smart grids, forming a complex and interconnected framework that enables efficient and optimized charging, demand response, vehicle-to-grid integration, and real-time monitoring and control of the charging infrastructure

Figure 1.1: BMW Vision iNEXT is a groundbreaking vehicle that exemplifies advanced autonomous driving capabilities. Source: bmw.co.uk.

(Fig. 1.2). The integration of electric vehicle (EV) charging with smart grids involves the seamless coordination of physical components such as EVs, charging stations, and power grids, complemented by intelligent software and communication systems. By harnessing the capabilities of cyber-physical systems (CPS), smart grids enable efficient and optimized charging through dynamic management of electricity supply and demand, taking into account factors like grid load, renewable energy generation, and user preferences. This integration unlocks advanced functionalities including demand response, vehicle-to-grid (V2G) integration, and real-time monitoring and control of the charging infrastructure. By harmonizing EVs and charging infrastructure with smart grids, this CPS-driven approach revolutionizes sustainable transportation and energy systems, promoting effective energy management, reducing peak loads, integrating renewable energy sources, and enhancing grid stability and reliability.

Safety-critical cyber-physical systems operate in domains with high-stakes implications, such as transportation, healthcare, energy, aerospace, and industrial control. Failure in these systems can lead to significant consequences.

In 2019, a tragic accident occurred involving a fatal collision between a Tesla Model 3 car and a semi-tractor trailer (Fig. 1.3). Sadly, the driver of the car, a 50-year-old individual, lost their life in the incident. The collision took place when the truck attempted to cross the southbound lanes of U.S. 441, intending to make a left turn into the northbound lanes. Although the truck decelerated as it approached the stop sign at the intersection, it failed to come to a complete halt before proceeding to cross the southbound lanes. The car was traveling southbound at a recorded speed of 69 mph and did not engage the brakes or take any evasive measures to avoid the truck crossing its path. Consequently, the Tesla collided with the left side of the trailer just behind its midpoint, resulting in the roof of the car being sheared off. Subsequently, the car continued its trajectory under the trailer before coming to a stop in the median, approximately 1.680 feet from the point of impact. Analysis of the Tesla's system performance data revealed that the driver had activated

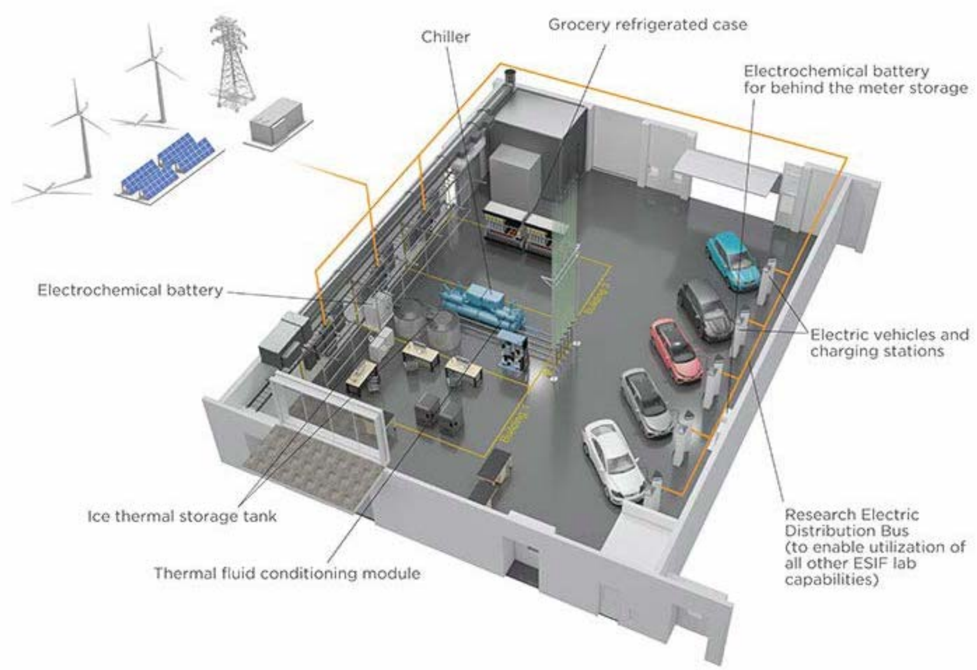

Chiller
Grocery refrigerated case
Electrochemical battery for behind the meter storage
Electrochemical battery
Electric vehicles and charging stations
Ice thermal storage tank
Thermal fluid conditioning module
Research Electric Distribution Bus (to enable utilization of all other ESIF lab capabilities)

Figure 1.2: EVs and their charging infrastructure integrated with smart grids exemplify cyber-physical systems. Source: nrel.org.

Autopilot at the time of the collision.

Complex requirements for cyber-physical systems, including safety, can be expressed as linear temporal logic formulae as well [58]. Model-based approaches for satisfying such requirements have been studied extensively in the literature [103, 8]. The challenge is that a precise model of dynamical systems is either not available in many application scenarios or too complex to be of any use. Therefore, there is a need to develop approaches which are capable of verifying or synthesizing controllers against safety specifications only based on the collected data from the system.

1.2 Literature Review

Here, we aim to contextualize our research within the current activities in the field of verification and synthesis for cyber-physical systems.

Nowadays, data-driven methods and machine learning techniques are being used extensively in many engineering applications. However, they suffer from several limitations in terms of accuracy and confidence. Due to the complexity of safety-critical cyber-physical systems (CPS), e.g., self-driving cars and traffic networks, there is a huge demand towards formal guarantees for the correctness of existing data-driven methods [6, 28]. On the other hand, formal methods can provide such guarantees when a model of the system is available. However, the main challenge which most model-based techniques face is the lack of a

Figure 1.3: The scene of Tesla Model 3 car accident in daylight. Source: roadsafetyusa.org.

precise model of the system. This motivates the need for combining data-driven methods with formal techniques that will lead to more efficient formal method algorithms [1].

Formal methods have been vastly used in the realm of computer science to provide correctness guarantees on the expected behavior of a program. Most of these formal techniques have been developed for finite-state models [10, 11]. In order to fully utilize the advantages of formal techniques in real physical applications, one needs to first construct a sufficiently precise model of the system. In general, it is hard to model a system accurately. Besides, the dynamics of a system may vary in the course of time. In such cases, statistical model checking can be beneficial if all states of the system can be measured [91, 24, 92]. However, statistical model checking generally needs a large number of experiments and is not able to handle synthesis problems directly [92].

In the first part of this thesis, we aim at putting together Bayesian inference and formal verification technique and subsequently provide a probabilistic confidence on satisfying a desired specification by trajectories of a stochastic system. We study formal verification of linear time-invariant (LTI) systems with respect to a fragment of temporal logic specifications when only a partial knowledge of the model is available, i.e., a parameterized model of the system is known but the exact values of the parameters are unknown. We provide a probabilistic measure for the satisfaction of the temporal logic specification by trajectories of the system under the influence of uncertainty. We assume these specifications are expressed by signal temporal logic (STL) formulae [68] and provide an approach that relies on collecting input-output data from the system. The following four paragraphs discuss a review of some related work:

A comparison between statistical model checking and probabilistic numerical model checking methods is provided in [112]. A multi-level statistical model checking approach is proposed in [100] for hybrid systems. A novel method is introduced in [78] for learning control Lyapunov-like functions in order to synthesize controllers for nonlinear dynamical systems for stability, safety, and reachability specifications. A data-driven approach was developed in [82] for control of piecewise affine systems with additive disturbances against STL specifications. In [7], concepts from formal modeling and machine learning are exploited to develop methodologies that can identify temporal logic formulae that discriminate different stochastic processes based on observations. In [22], authors propose an approach to approximate the posterior distributions of unknown parameters for nonlinear deterministic systems.

Properties expressed as STL formuale are introduced and used in the literature including the works in [76] and [30]. A new definition for probabilistic STL formulae is introduced in [81] that assigns probabilities to the atomic propositions and then combines them through Boolean operators. A robust treatment of uncertainties under STL constraints is performed in [32] in the framework of model predictive control. An under-approximation of constraints described as probabilistic STL formulae is proposed in [31] and applied to design control strategies for the Barcelona wastewater system [33].

In recent years, researchers also have investigated data-driven techniques for formal policy synthesis of dynamical systems due to their applicability to high dimensional spaces. A data-driven approach is proposed in [93] for synthesis of safe digital controllers for sampled-data stochastic nonlinear systems. The learning approach proposed in [21] finds Lyapunov functions for dynamical systems ensuring their stability. The work in [44] applies model-free reinforcement learning for policy synthesis of *finite-state* models. This method is extended in [63, 62] for continuous-space dynamical systems and finite-horizon specifications under continuity assumptions on the dynamics of the system. The authors in [46] propose a reinforcement learning for the synthesis of continuous-state dynamical systems but the convergence is only demonstrated empirically. The recent approach in [56] applies reinforcement learning for satisfying linear temporal logic (LTL) specifications with convergence guarantees and without requiring any continuity assumption on the system dynamics. Translating LTL specifications to average objectives for reinforcement learning is studied in [55].

A data-driven and model-based formal verification approach for partially unknown LTI systems is recently developed in [41], [43]. In these works, authors propose a new method based on Bayesian inference and reachability analysis to provide a confidence based on which a physical system affected by noisy measurements verifies a given bounded-time LTL specification. In [42], a method based on Bayesian inference and model checking is developed for Markov decision processes. The recent results in [85] extend those of [41] and [43] to verification of stochastic LTI systems under specifications expressed as STL formulae. Utilizing data to construct abstractions and checking properties of dynamical systems has been studied recently in [54, 67]. A Bayesian approach to construct models and perform robust verification and synthesis of stochastic systems is proposed recently in [90].

Safety is considered a crucial aspect among the specifications of cyber-physical systems. Model-based approaches for satisfying safety requirements have been studied extensively in the literature [35**?** , 103, 8]. In the setting of formal approaches for stochastic systems, a number of abstraction-based methods have been developed for the verification and synthesis of dynamical systems in order to either verify the desired specifications or synthesize controllers enforcing these systems to satisfy such specifications [60, 66, 101, 114]. In order to improve scalability of abstraction-based methods, some other techniques such as sequential gridding [97, 95], discretization-free abstraction [115], and compositional abstraction-based techniques [98] have been introduced in the literature in order to efficiently deal with the verification and synthesis problems.

An approach for formal verification and synthesis with respect to safety specifications in dynamical systems is to use a notion of barrier certificates [74]. Barrier certificates have been the focus of the recent literature as an abstraction-free technique that is scalable with the dimension of the system, i.e., they do not require construction of an abstraction of the system and can provide directly the controller together with the guarantee on the satisfaction of the safety specification [116], [110], [14]. A barrier-based methodology is introduced in [74] in order to verify safety in deterministic hybrid systems. In [75], a framework is proposed for safety verification of stochastic systems using barrier certificates which is extended to stochastic hybrid systems. The authors in [106] present barrier certificates that ensure collision-free behaviors in multi-robot systems by minimizing the difference between the actual and the nominal controllers subject to safety constraints. In [94], a compositional analysis is proposed for verifying the safety of an interconnection of subsystems using barrier certificates. The results in [51] use barrier certificates for the synthesis of controllers against complex requirements expressed as co-safe linear temporal logic formulas.

The common requirement of the approaches mentioned above is the fact that they need a mathematical model of the system. However, a precise model of dynamical systems is either not available in many application scenarios or too complex to be of any use. Therefore, there is a need to develop approaches which are capable of verifying or synthesizing controllers against safety specifications only based on collected data from the system.

In the second part of the thesis, we develop a data-driven approach in order to tackle the safety problem for stochastic systems. Data-driven methods have gained significant attentions recently for formally verifying some desired specifications. A data-enabled predictive control is introduced in [25] that utilizes noisy data of the system and produces optimal control inputs ensuring the satisfaction of desired chance constraints with high probability. A data-driven model predictive control scheme is proposed in [9] which only requires initially measured input-output trajectories together with an upper bound on the dimension of the unknown system. In [104], a methodology is developed in order to make a single-input single-output system stable only based on data. The stability problem of black-box linear switching systems with desired confidences is investigated in [57] based on collected data. This approach is extended in [107] by providing a methodology for computing the invariant sets of discrete-time black-box systems. A novel Bayes-adaptive planning algorithm for data-efficient verification of uncertain Markov decision processes is introduced in [108]. A framework is proposed in [82] to provide a formal guarantee on data-driven model identification and controller synthesis. In [86], a methodology is developed for providing a probabilistic confidence over the verification of signal temporal logic properties for partially unknown stochastic systems based on collected data. The authors in [73] propose a framework to learn a decision tree as a model for a black box continuous system.

The work in [26] develops a method to synthesize robust feedback controllers with safety and stability guarantees. In [80], a data-driven approach is proposed in order to synthesize controllers for deterministic hybrid systems using barrier certificates while providing a correctness guarantee on the obtained barrier certificate. A data-driven, model-based approach is developed in [2] to provide stability guarantees using Satisfiability Modulo Theories (SMT). The authors in [70] develop a data-driven technique to synthesize controllers for unknown deterministic systems. The framework developed in [23] computes barrier certificates for complete- and incomplete-information systems affected by Gaussian process and measurement noises under unbounded inputs.

An optimization-based approach is proposed in [79] to learn a control barrier certificate through safe trajectories under suitable Lipschitz smoothness assumption on the dynamical system. A sub-linear algorithm is developed in [45] for the barrier-based data-driven model validation of dynamical systems which computes the barrier function using a large dataset of trajectories. In [49], a two-step procedure is proposed to synthesize a controller for an unknown nonlinear system, where the first step is to learn a Gaussian process as a replacement of the unknown dynamics, and the second step is to construct the control barrier function for the learned dynamics.

A data-driven optimization called *scenario convex program* (SCP) is introduced in [17] to solve robust convex optimizations. This approach replaces the infinite number of constraints in the robust optimization with a finite number of constrained by sampling the uncertain variables from their distributions. The approach relates the feasibility of the SCP to that of the robust optimization while providing bounds on the probability of violating the constraints. The results in [53] studies the same approach and relates worst-case violation of the constraints to the probability of their violation. While [17, 53] focus on feasibility, the authors in [29] establish a quantitative relation between the optimal value of the robust optimization and its associated SCP. In Chapter 3, we deploy the results in [29] in order to connect the solution of an SCP to an RCP that is equivalent to a safety problem for stochastic systems.

Since the developed approach requires a large number of samples to provide the desired concrete guarantee on the safety of the stochastic systems, we develop approaches in Chapter 4 to tackle this problem. The authors propose an approach in [19] that utilizes the number of constraints whose elimination affects an optimization problem instead of considering all constraints in order to connect the solutions of a scenario convex program and a chance constraint program (CCP). A repetitive scenario design is developed in [16] in to potentially reduce the number of required samples in order to connect the optimizers of an SCP and an CCP. We leverage the ideas in these papers together with the results in [29] to develop three techniques in order to improve the results in Chapter 3 in terms of required number of samples.

1.3 Contributions

We have developed two approaches in this thesis to address the issue of lack of access to a precise model for a system with a partially unknown parameterized model, as well as a system with a completely unknown model.

- First, we investigate the formal verification of linear time-invariant (LTI) systems in relation to a fragment of temporal logic specifications when only partial knowledge of the model is available. In other words, we have a parameterized model of the system, but the exact parameter values are unknown. Our overall goal is to integrate Bayesian inference and formal verification techniques to offer a probabilistic measure of confidence in satisfying a desired specification through stochastic system trajectories. We establish a probabilistic measure for assessing the satisfaction of the temporal logic specification by system trajectories, considering the presence of uncertainty. We assume these specifications are expressed by signal temporal logic (STL) formulae [68] and provide an approach that relies on collecting input-output data from the system. We employ Bayesian inference to associate a notion of confidence to the satisfaction of the specification. Our main objective is to combine both data-driven and model-based techniques for stochastic LTI systems in order to verify the system against STL specifications. Our approach considers probability thresholds as the lower bounds for the satisfaction of STL specifications by the stochastic trajectories of the system. We under-approximate the feasible parameter sets of the probabilistic constraints by transforming them into algebraic inequalities. Then, confidence values are computed using the obtained feasible sets and distributions of parameters which are updated based on collected data from the systems. We also propose relaxation of the algebraic inequalities in order to reduce the conservativeness of under-approximations.

- Second, we propose formal verification and synthesis procedures for unknown stochastic systems with respect to safety specifications based on collected data. We first cast a barrier-based safety problem as a robust convex program (RCP). Solving the obtained RCP is hard in general because the unknown model of the system appears in the constraints. To tackle this issue, we resort to a scenario-driven approach by collecting samples from the system. Using the results in [29], we connect the optimal solution of the acquired scenario convex program (SCP) with that of the original RCP. We provide a lower bound on the safety probability of the unknown stochastic system using a certain number of data which is related to the desired confidence. We extend this result to provide a new confidence bound for a class of non-convex barrier-based safety problems.

- Continuing with this thesis, we introduce three theoretical approaches that are designed to address and reduce the sample complexity inherent in our second proposed approach. This complexity arises due to the concrete formal guarantee we provide regarding the safety of the system.

First, inspired by the findings in [19], we propose a wait-and-judge approach. This approach offers a data-driven scheme for safety verification of stochastic systems with unknown models. It provides an out-of-sample performance guarantee while also addressing the issue of sample complexity. To begin, we employ the concept of barrier certificates, which allows us to formulate the safety problem as a robust convex program (RCP). However, solving this optimization program becomes intractable due to the presence of the unknown model in one of the constraints. Instead, we propose a scenario convex program (SCP) that corresponds to the original RCP. We achieve this by utilizing an arbitrary number of samples obtained from the system's trajectories. Next, we establish a condition on the optimal value of the obtained SCP. This condition indicates that the original unknown stochastic system is safe with a lower bound on the probability and a guaranteed confidence. This condition is closely related to the number of support constraints. Support constraints are those whose elimination significantly affects the optimal value. By establishing a posteriori relations between the desired confidence, the probability of constraint violation, and the number of samples, we drastically reduce the required amount of data compared to other approaches that require these relations to be known a priori. Refer to the results in [83] for more details.

Second, inspired by the results in [16], we propose here a so-called repetitive scenario approach that provides a data-driven framework to formally verify safety of stochastic systems with unknown models, while providing out-of-sample performance guarantees over the verification results. Similar to the results in [83] and [84], we leverage a notion of barrier certificates in order to cast the safety problem as an RCP. Since solving this optimization program is not tractable, and also the unknown model appears in one of the constraints, instead we propose an SCP corresponding to the original RCP by using N samples collected from trajectories of the system. To tackle the underlying sample complexity in the results in [83] and [84], here we construct a *repetitive scenario program* (RSP) with a specific number of iterations based on the original SCP. At each iteration, we feed the optimal solution of the SCP with N samples to a feasibility checker, called the feasibility oracle, with N_0 new test samples. The feasibility condition is defined in a way that the empirical error of the violations should be less than a desired threshold. There is a theoretical upper bound on the required number of iterations in order to satisfy the feasibility condition. Finally, a safety condition, which is derived based on Lipschitz constants of the constraints of RCP, is checked on top of the feasibility condition. If both conditions are satisfied, then the optimal solution of the RSP is formally related to the original safety verification problem. As a result, for a fixed a-priori confidence, the unknown stochastic system is safe with a quantified probability lower bound computed using feasible solutions of the successful iteration.

Third, we present a novel approach that enhances the benefits of two existing approaches in [88] and [89] by computing both the number of support constraints and confidence bounds a posteriori. Moreover, we introduce a new method that significantly reduces the number of required samples for the same level of confidence. First, similar to [83], we cast the safety problem as an RCP. We select a specific number of samples and construct an SCP. This SCP is solved iteratively until a feasibility condition on its optimizer is satisfied. This feasibility condition is constructed based on the exact number of support constraints at each iteration. The lower number of samples leads to a higher number of iterations and vice versa. It is also shown that there is an upper bound on the number of required iterations. In the end, a safety condition is checked over the optimal value of the successful iteration. If this condition is satisfied, then one can conclude that the system is safe with a probability lower bounded by a value computed using the optimizer of the successful iteration. A confidence can be computed a posteriori based on the exact number of support constraints at the successful iteration, resulting in a less conservative confidence.

1.4 Thesis Organization

This dissertation provides theoretical foundations based on machine learning and data-driven techniques to enable the reliable verification and synthesis of cyber-physical systems (CPS). In **Chapter 2**, we introduce a probabilistic measure to assess the satisfaction of a specification expressed in signal temporal logic by system trajectories affected by uncertainty. Our approach involves collecting input-output data from the system and utilizing Bayesian inference on the gathered data to assign a measure of confidence to the satisfaction of the specification. In **Chapter 3**, we study verification and synthesis problems for safety specifications over unknown discrete-time stochastic systems. We cast the safety problem of stochastic systems as a convex optimization problem for a finite number of collected samples from the state set. Then, we connect the solution of this optimization problem to the safety of the original stochastic system, providing a formal guarantee of safety. In **Chapter 4**, we develop three theoretical techniques in order to reduce the sample complexity arises in the proposed method in Chapter 3. **Chapter 5** concludes the results of the thesis and outlines potential future directions on related topics.

Chapter 2

A Data-Driven Method for Stochastic Systems under STL Constraints

2.1 Introduction

In this chapter, we investigate the verification and synthesis problems for stochastic systems under signal temporal logic (STL) properties which are characterized as parameterized models.

2.1.1 Motivation

Cyber-physical systems usually have complex dynamics and are required to fulfill complex tasks. In recent years, formal methods from Computer Science have been used by control theorists for both describing the required tasks and ensuring that they are fulfilled by the systems. The crucial drawback of formal methods is that a complete model of the system often needs to be available. The goal of this chapter is to study satisfaction of a fragment of temporal logic properties, over linear time invariant systems (LTI), when only a partial knowledge of the model is available, i.e., a parameterized model of the system is known but the exact values of the parameters are unknown. We provide a probabilistic measure for the satisfaction of the temporal logic property by trajectories of the system under the influence of uncertainty. We assume these properties are expressed as signal temporal logic formulae and provide an approach that relies on gathering input-output data from the system, employing Bayesian inference on the collected data to associate a notion of confidence with the satisfaction of the property.

2.1.2 Contributions

The main novelty of our approach is to combine both data-driven and model-based techniques in order to have a two-layer probabilistic reasoning over the behavior of the system. The inner layer is with respect to the uncertainties in dynamics and observed data while the outer layer is with respect to the distribution over the parameter space. The latter is updated using Bayesian inference on the collected data. We study both verification and synthesis problems with the goal of either verifying the satisfaction of property independently of the choice of input trajectory or finding one that gives the largest confidence in satisfying the property.

I need to mention that the results presented in this chapter appear in the publications [86, 87]. The first result has been presented at the 21st IFAC world congress. The latter has been published in Automatica journal. The author of the thesis has established the results and written the drafts. Sadegh Soudjani and Majid Zamani supervised the work.

2.2 Preliminaries and Problem Formulation

In this section, we provide the system definition and the problem statement.

2.2.1 Parametric LTI Systems

Consider the set of parameterized stochastic linear time-invariant (LTI) models $\Omega := \{\mathrm{M}(\theta) \mid \theta \in \Theta\}$ such that

$$\mathrm{M}(\theta) := \begin{cases} x(t+1) = A(\theta)x(t) + B(\theta)u(t) + Gw(t), \\ \quad\;\; \hat{y}(t) = C(\theta)x(t) + D(\theta)u(t), \end{cases} \tag{2.1}$$

where $x(t) \in \mathbb{R}^n$ is the state, $\hat{y}(t) \in \mathbb{R}^m$ is the output, $u(t) \in \mathcal{U} \subset \mathbb{R}^r$ is the input, and $\theta \in \Theta \subset \mathbb{R}^p$ is the parameter of the model $\mathrm{M}(\theta)$. Here, $\mathcal{U}$ is the set of valid inputs and is assumed to be bounded. The process noise $w\colon \mathbb{R}_{\geq 0} \to \mathbb{R}^n$ is selected to be a zero-mean Gaussian distribution with a covariance matrix Σ_w.

Assumption 1. *We assume that our target model S is picked from the class of stochastic dynamical systems and its behavior can be characterized by the model $\mathrm{M}(\theta_{\texttt{true}})$ for some true parameter $\theta_{\texttt{true}} \in \Theta$. This true parameter is unknown in general. Furthermore, we assume having access to the output of system S, that is,*

$$y(t) = \hat{y}(t) + e(t), \tag{2.2}$$

in which $e\colon \mathbb{R}_{\geq 0} \to \mathbb{R}^m$ represents the measurement noise with a zero-mean Gaussian distribution and a covariance matrix Σ_e. Both process and measurement noises are assumed to be uncorrelated to the input.

Consider a specification ψ defined over trajectories of the system $\mathbf{S}$. We assume ψ belongs to the class of STL specifications which will be defined formally in Subsection 2.4.1. We denote the satisfaction relation by $\mathbf{S} \models \psi$ which is true when the trajectories of the system $\mathbf{S}$ satisfy ψ.

We plan to provide a confidence value for the satisfaction of ψ by trajectories of $\mathbf{S}$. Our approach relies on collecting data from the system and using Bayesian inference to provide the confidence value.

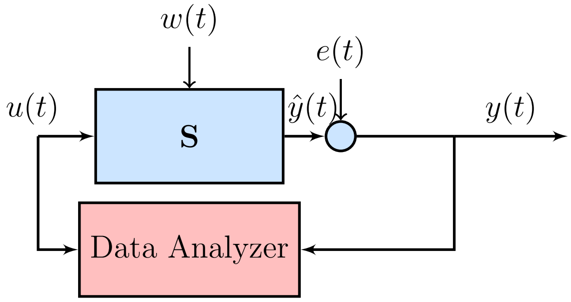


Figure 2.1: Data collection from the system **S**.

2.2.2 Data Collection

The process of data collection is depicted in Fig. 2.1. Let us denote the set of data collected from the system by $\mathcal{D} = \{\tilde{u}_{\mathtt{exp}}(t), \tilde{y}_{\mathtt{exp}}(t)\}_{t=0}^{\mathrm{N}_{\mathrm{exp}}}$, in which $\tilde{u}_{\mathtt{exp}}(t)$ and $\tilde{y}_{\mathtt{exp}}(t)$ are input-output pairs within the time horizon $\{0, \ldots, \mathrm{N}_{\mathtt{exp}}\}$. In general, it is assumed that we can excite the system with any desirable input signal but within the acceptable range of inputs.

Assumption 2. *Process noise $\{w(t),\, t = 0, 1, 2, \ldots\}$ and measurement noise $\{e(t),\, t = 0, 1, 2, \ldots\}$ are independent and identically distributed over time, and are independent from each other. In addition, the initial state $x(0)$ is known, and the input $u(t)$ is deterministic.*

The assumption on the initial state $x(0)$ can be generalized by allowing it to have a Gaussian distribution independent of $w(\cdot)$ and $e(\cdot)$. Our approach is still applicable to this more general case.

2.2.3 Stochastic Bayesian Confidence

When the model $\mathrm{M}(\theta)$ is deterministic, the satisfaction relation $\mathrm{M}(\theta) \models \psi$ is a binary relation over the parameter space Θ. This is due to having a unique state trajectory for a given input trajectory. If Ω is the set of parameterized *deterministic* models, we can define the satisfaction function for the deterministic system as $g_\psi : \Theta \to \{0, 1\}$ in which $g_\psi(\theta) \equiv (\mathrm{M}(\theta) \models \psi)$. This function can only take values that are zero or one. If the system is affected by the process noise, satisfaction relation becomes a random variable over {0,1}. We are interested in computing the probability with which the satisfaction relation holds. In this case, we define a threshold on the satisfaction probability of ψ as

$$\mathbb{P}(\mathrm{M}(\theta) \models \psi) \geq 1 - \delta, \tag{2.3}$$

where $\delta \in (0, 1)$. Now we can assign a satisfaction function f_ψ^δ to the above chance constraint which is again a binary function on the parameter space Θ.

Definition 1. *Consider $\Omega = \{\mathrm{M}(\theta) \mid \theta \in \Theta\}$ with $\mathrm{M}(\theta)$ defined as in (2.1), and the specification ψ. The satisfaction function $f_\psi^\delta : \Theta \to \{0, 1\}$ is defined as*

$$f_\psi^\delta(\theta) = \begin{cases} 1 & \textit{if } \mathbb{P}\left(\mathrm{M}(\theta) \models \psi\right) \geq 1 - \delta, \\ 0 & \textit{otherwise}, \end{cases} \tag{2.4}$$

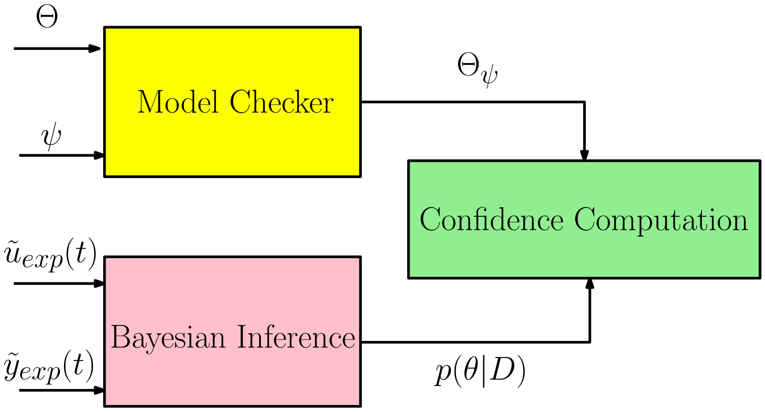


Figure 2.2: An overview of our proposed approach.

for any $\delta \in (0,1)$.

The set of parameters for which $f_\psi^\delta(\theta) = 1$ is called the feasible set of parameters which can be represented as

$$\Theta_\psi := \{\theta \in \Theta | \; f_\psi^\delta(\theta) = 1\}. \tag{2.5}$$

Let us denote by $\mathbb{P}(.)$ and $p(.)$ the probability of an event and the probability density function of a random variable, respectively. We define a probabilistic confidence on satisfaction of the specification using Bayesian inference as follows.

Definition 2. *Given a specification* ψ *and a set of data* $\mathcal{D}$, *the* confidence *on satisfaction of* ψ *by trajectories of the system is*

$$\mathbb{P}(\mathbf{S} \models \psi \mid \mathcal{D}) := \int_\Theta f_\psi^\delta(\theta) \; p(\theta \mid \mathcal{D}) \; d\theta, \tag{2.6}$$

where $p(\cdot \mid \mathcal{D})$ *is the posteriori distribution on the parameter space conditioned on the input-output data set, and* $f_\psi^\delta(\theta)$ *is the satisfaction function defined in* (2.4).

Assume that we have a prior knowledge of parameterized models for $\mathbf{S}$ in the form of some distribution over Θ. This prior knowledge can be used to improve the posterior distribution function over Θ after collecting data from the system.

2.2.4 Problem Statement

Note that the satisfaction function in (2.4), the feasible set in (2.5), and the confidence in (2.6) all depend on the input trajectory of the system. If we require the inequality in (2.4) to hold for all possible input trajectories, these quantities become independent of the input trajectory. This is indeed a verification problem stated next.

Problem 1 (Verification)**.** *Given a parameterized LTI system in* (2.1) *together with the noisy output in* (2.2), *data set* $\mathcal{D}$, *and specification* ψ, *we aim at computing the confidence* (2.6) *when* $f_\psi^\delta(\theta) = 1$ *or equivalently when*

$$\mathbb{P}\left(\mathrm{M}(\theta) \models \psi\right) \geq 1 - \delta \quad \forall u(t) \in \mathcal{U}, \forall t \geq 0. \tag{2.7}$$

A schematic of our proposed approach, which allows us to incorporate any prior information regarding appropriate parameters θ in order to achieve a more precise confidence, is depicted in Fig. 2.2.

2.3 Bayesian Inference

Bayesian inference is used extensively in machine learning to update probability distributions after collecting observations [12]. Here, we use Bayesian inference in order to provide confidences of satisfaction for the given specifications for parametric LTI systems. Given a prior density function over the set of parameters, denoted by $p(\theta)$ and an input-output data set $\mathcal{D}$, a posterior distribution $p(\theta \mid \mathcal{D})$ can be inferred for θ by

$$p(\theta \mid \mathcal{D}) = \frac{p(\mathcal{D} \mid \theta)\ p(\theta)}{\int_{\Theta} p(\mathcal{D} \mid \theta)\ p(\theta) d\theta}, \tag{2.8}$$

where $p(\mathcal{D} \mid \theta)$ is the *likelihood distribution function.*

For the dataset $\mathcal{D} = \{\tilde{u}_{\mathtt{exp}}(t), \tilde{y}_{\mathtt{exp}}(t)\}_{t=0}^{\mathrm{N}_{\mathtt{exp}}}$, the likelihood distribution is the joint distribution of all measured outputs in the form of

$$p(\tilde{y}_{\mathtt{exp}}(0), \tilde{y}_{\mathtt{exp}}(1), \ldots, \tilde{y}_{\mathtt{exp}}(\mathrm{N}_{\mathtt{exp}}) \mid \theta). \tag{2.9}$$

Proposition 1. *Consider the LTI model* (2.1)-(2.2). *The joint distribution* $p(\mathcal{D} \mid \theta)$ *is multi-variate Gaussian with mean*

$$\bar{\mathbf{y}}(\theta) = [\bar{y}(0); \cdots ; \bar{y}(\mathrm{N}_{\mathtt{exp}})], \tag{2.10}$$

and covariance matrix $\Sigma_{\tilde{\mathbf{y}}}(\theta)$*, where*

$$\begin{aligned} \bar{y}(t) &:= C(\theta)A(\theta)^t x(0) + D(\theta)u(t) \\ &\qquad\qquad + \sum_{i=0}^{t-1} C(\theta)A(\theta)^i B(\theta)u(t-i-1), \\ \Sigma_{\tilde{\mathbf{y}}}(\theta) &:= \mathcal{M}(\theta)\ \Sigma_W\ \mathcal{M}(\theta)^T + \Sigma_E, \end{aligned}$$

where $\Sigma_W := \mathrm{diag}(\Sigma_w, \ldots, \Sigma_w)$ *and* $\Sigma_E := \mathrm{diag}(\Sigma_e, \ldots, \Sigma_e)$ *are block diagonal with respectively* $\mathrm{N}_{\mathtt{exp}}$ *and* $(\mathrm{N}_{\mathtt{exp}} + 1)$ *blocks. Matrix* $\mathcal{M}(\theta) \in \mathbb{R}^{(m\mathrm{N}_{\mathtt{exp}}+m)\times(n\mathrm{N}_{\mathtt{exp}})}$ *is represented as:*

$$\mathcal{M}(\theta)=\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ C(\theta)G & 0 & 0 & \cdots & 0 \\ C(\theta)A(\theta)G & C(\theta)G & 0 & \cdots & 0 \\ C(\theta)A(\theta)^2G & C(\theta)A(\theta)G & C(\theta)G & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ C(\theta)A(\theta)^{\mathrm{N}_{\mathtt{exp}}-1}G & C(\theta)A(\theta)^{\mathrm{N}_{\mathtt{exp}}-2}G & \cdots & \cdots & C(\theta)G \end{bmatrix}.$$

Based on the above Proposition, the joint Gaussian distribution for measured outputs can be characterized as

$$p(\tilde{y}_{\texttt{exp}}(0), \tilde{y}_{\texttt{exp}}(1), \ldots, \tilde{y}_{\texttt{exp}}(\mathrm{N}_{\texttt{exp}}) \mid \theta) = \\ \frac{1}{|\Sigma_{\tilde{\mathbf{y}}}(\theta)|^{\frac{1}{2}}(2\pi)^{\frac{m\mathrm{N}_{\texttt{exp}}}{2}}} \exp\left\{-\frac{1}{2}(\tilde{\mathbf{y}} - \bar{\mathbf{y}}(\theta))^T \ \Sigma_{\tilde{\mathbf{y}}}(\theta)^{-1}(\tilde{\mathbf{y}} - \bar{\mathbf{y}}(\theta))\right\}, \tag{2.11}$$

where, $\tilde{\mathbf{y}} = [\tilde{y}_{\texttt{exp}}(0); \tilde{y}_{\texttt{exp}}(1); \cdots; \tilde{y}_{\texttt{exp}}(\mathrm{N}_{\texttt{exp}})]$ is the vector of noisy measured outputs and $\bar{\mathbf{y}}(\theta)$ is defined in (2.10). The $|\Sigma_{\tilde{\mathbf{y}}}(\theta)|$ is determinant of the covariance matrix. The density function (2.11) can be used to update the posterior distribution using (2.8).

2.4 STL and Under-Approximation

2.4.1 Signal Temporal Logic (STL)

One of the main advantages of STL specifications is their capability in quantifying temporal specifications for trajectories of physical systems. We denote an infinite state trajectory of the system in (2.1) by $\xi = x(0), x(1), x(2), \ldots$ where $x(t)$ is the state of the system at time $t \in \mathbb{N}_0 := \{0, 1, 2, \ldots\}$. Below, we define syntax and semantics of STL specifications using the standard notation employed in [68, 6].

Syntax: Signal temporal logic (STL) formulae are defined recursively using the following syntax:

$$\psi ::= \mathsf{T} \mid \mu \mid \neg\psi_1 \mid \psi_1 \wedge \psi_2 \mid \psi_1 \ \mathsf{U}_{[a,b]} \ \psi_2, \tag{2.12}$$

where the separator sign | indicates that any specification ψ in this logic can take one of the given five forms, separated by | in (2.12), and is constructed by combining specifications ψ_1, ψ_2 from this logic. T is the true predicate, and $\mu : \mathbb{R}^n \to \{\mathsf{T}, \mathsf{F}\}$ is a predicate such that its truth value is determined by the sign of a function of the state x, i.e., $\mu(x) = \mathsf{T}$ if and only if $\alpha(x) \geq 0$ with $\alpha : \mathbb{R}^n \to \mathbb{R}$ being an affine function of the state and is associated with μ. Notations $\neg$ and $\wedge$ denote negation and conjunction of formulas. Notation $\mathsf{U}_{[a,b]}$ denotes the until operator where $a, b \in \mathbb{R}_{\geq 0}$ and $a \leq b$.

Semantics: The satisfaction of an STL formula ψ by a trajectory ξ at time t is denoted by $(\xi, t) \models \psi$ which is defined recursively as follows:

$$\begin{aligned}
&(\xi, t) \models \mu \Leftrightarrow \mu(\xi, t) = \mathsf{T} \\
&(\xi, t) \models \neg\mu \Leftrightarrow \neg((\xi, t) \models \mu) \\
&(\xi, t) \models \psi \wedge \phi \Leftrightarrow (\xi, t) \models \psi \wedge (\xi, t) \models \phi \\
&(\xi, t) \models \psi \ \mathsf{U}_{[a,b]} \ \phi \Leftrightarrow \exists t' \in [t + a, t + b] \text{ s.t. } (\xi, t') \models \phi \\
&\wedge \forall t'' \in [t, t'], \ (\xi, t'') \models \psi.
\end{aligned}$$

A trajectory ξ satisfies a specification ψ, denoted by $\xi \models \psi$, if $(\xi, 0) \models \psi$. We also write $\mathbf{S} \models \psi$ to indicate that $\xi \models \psi$ with ξ being the trajectory of the system $\mathbf{S}$ started from the initial condition $x(0)$.

Furthermore, other standard operators can be expressed using the above defined ones. For *disjunction*, we can write $\psi \vee \phi := \neg(\neg\psi \wedge \neg\phi)$ and the *eventually* operator can be defined as $\Diamond_{[a,b]}\psi := \top \, \mathsf{U}_{[a,b]} \, \psi$. Finally, the *always* operator is defined as $\Box_{[a,b]}\psi := \neg\Diamond_{[a,b]}\neg\psi$. The *horizon* of an STL formula, denoted by $len(\psi)$, is the maximum over all upper bounds of intervals on the temporal operators. Intuitively, $len(\psi)$, is the horizon in which satisfaction of $(\xi, t) \models \psi$ should be studied. Let us now denote a finite trajectory by $\xi(t:N) := x(t), x(t+1), ..., x(t+N)$. For checking $(\xi, t) \models \psi$, it is sufficient to consider a finite trajectory $\xi(t:N)$ with $N = len(\psi)$.

2.4.2 Under-approximation of STL Constraints

The stochastic satisfaction function defined in (2.4) requires the exact feasible set of the chance constraint in (2.3). This feasible set does not have a closed form in general. Previous works tried to find under-approximations of the feasible set. We leverage the proposed procedure in [31] to get an under-approximation of the feasible set. This procedure transforms the chance constraints on the STL specification into similar constraints on the predicates of the specification using the structure of the STL formula. We discuss this procedure in this subsection and show how this under-approximation can be improved in Subsection 2.4.3.

The next lemma, borrowed from [31], shows how one can transform the chance constraints on the satisfaction of STL formulae into similar constraints on the predicates of formulae. Since STL formulae are defined on trajectories of the system, we write $\xi(t:N) \models \psi$ instead of $\mathrm{M}(\theta) \models \psi$ to indicate satisfaction of ψ by trajectories starting at time t.

Lemma 1. *For any STL formula ψ and a value $\delta \in (0,1)$, probability constraints of the forms $\mathbb{P}(\xi(t:N) \models \psi) \geq 1-\delta$ and $\mathbb{P}(\xi(t:N) \models \psi) \leq 1-\delta$ can be transformed into similar constraints on the predicates of ψ based on the structure of ψ.*

In the following, we discuss how this transformation is performed.

Case I Negation $\psi = \neg\psi_1$

$$\begin{aligned} \mathbb{P}(\xi(t:N) \models \psi) \geq \delta \Leftrightarrow \\ \mathbb{P}(\xi(t:N) \models \psi_1) \leq 1-\delta. \end{aligned} \tag{2.13}$$

Case II Conjunction $\psi = \psi_1 \wedge \psi_2$

$$\mathbb{P}(\xi(t:N) \not\models \psi_i) \leq \frac{1-\delta}{2}, \; i = 1, 2. \tag{2.14}$$

Case III Until $\psi = \psi_1 \, \mathsf{U}_{[a,b]} \, \psi_2$

$$\begin{aligned} \mathbb{P}(\xi(t:N) \models \psi) \geq \delta \Leftarrow \\ \mathbb{P}(\Lambda_j) \geq \frac{\delta}{(b-a+1)}, \; j = 1, \ldots, N, \end{aligned} \tag{2.15}$$

in which the event Λ_j is defined as

$$\Lambda_j := \bigwedge_{k=t}^{t+a-1} (\xi(k:N) \models \psi_1)$$
$$\bigwedge_{k=a+t}^{j-1} (\xi(k:N) \models (\psi_1 \wedge \neg\psi_2)) \wedge (\xi(j:N) \models \psi_2). \tag{2.16}$$

These transformations are based on multiple application of Boole's inequality [28]. Required transformations for the complements of Cases II and III can be derived similarly.

Lemma 1 enables us to write down probabilistic inequalities on the satisfaction of atomic predicates and use them as under-approximations of the original probabilistic STL constraints. These probabilistic inequalities can be equivalently written as algebraic inequalities given that we know the statistical properties of the state trajectories.

In the case of LTI systems under Assumption 2, $x(t)$ is also Gaussian with known mean and covariance. Let us consider predicate $\mu(x) = \{\alpha(x) \geq 0\}$ with $\alpha(x) := \tilde{\theta}_0 + \tilde{\theta}^T x$, for some $\tilde{\theta} \in \mathbb{R}^n$ and $\tilde{\theta}_0 \in \mathbb{R}$. One can write $\mathbb{E}[\alpha(x)] = \tilde{\theta}_0 + \tilde{\theta}^T\ \mathbb{E}[x]$ and $\mathrm{Var}[\alpha(x)] = \tilde{\theta}^T \mathrm{Cov}(x)\tilde{\theta}$. Therefore,

$$\begin{aligned} &\mathbb{P}(\alpha(x) \geq 0) \geq 1-\delta \ \Leftrightarrow\ \mathbb{P}(\alpha(x) < 0) \leq \delta \\ &\Leftrightarrow \mathbb{E}[\alpha(x)] + \mathrm{Var}[\alpha(x)]\mathbf{erf}^{-1}(\delta) \geq 0, \end{aligned} \tag{2.17}$$

where $\mathbf{erf}^{-1}(\cdot)$ is the error inverse function defined with $\mathbf{erf}(x) = \frac{1}{\sqrt{\pi}} \int_{-x}^{x} \exp(-t^2)dt$ where $\exp(\cdot)$ denotes the natural exponential function. In the following proposition, we show that the algebraic inequalities of the form (2.17) are linear with respect to the input.

Proposition 2. *Chance constraint $\mathbb{P}(\alpha(x(t)) \geq 0) \geq 1-\delta$, where $\alpha(x) = \tilde{\theta}_0 + \tilde{\theta}^T x$ and $x(t)$ being the state of the stochastic system (2.1) at time t, can be written as the following constraint that is affine with respect to the input:*

$$\begin{aligned} &\sum_{i=0}^{t-1} \tilde{\theta}^T A(\theta)^i B(\theta)\ u(t-i-1) \\ &\qquad + \tilde{\theta}_0 + \tilde{\theta}^T A(\theta)^t x(0) + \tilde{\theta}^T \Gamma(\theta,\delta)\tilde{\theta} \geq 0, \end{aligned} \tag{2.18}$$

where

$$\Gamma(\theta,\delta) := \mathbf{erf}^{-1}(\delta) \sum_{i=0}^{t-1} A(\theta)^i G\ \Sigma_w\ G^T (A(\theta)^T)^i. \tag{2.19}$$

Note that in general $\Gamma(\theta,\delta)$ and the left-hand side of (2.18) are nonlinear functions of θ. They become polynomial functions of θ if $A(\theta)$ and $B(\theta)$ depend on θ linearly.

2.4.3 A Less Conservative Approximation

The proposed procedure in Lemma 1 for transforming the chance constraints into similar inequalities on atomic predicates can be very conservative. This is due to the fact that constraints of type $\mathbb{P}(A_1 \cup A_2) \leq \delta$ are conservatively replaced by inequalities $\mathbb{P}(A_i) \leq \delta/2$, $i = 1, 2$. This replacement puts a uniform upper bound on the probability of events A_i and does not create any room for the intersection of these events. In this subsection, we increase the flexibility in the under-approximation and enlarge the feasible set of the probabilistic STL constraint through *intermediate weights*.

This new under-approximation procedure results in new constraints with a higher number of variables. It is based on the structure of the STL formula similar to the discussion in the previous subsection and has the following three cases:

Case I: Disjunction

$$\begin{aligned} &\mathbb{P}(\xi(t:N) \models (\psi_1 \vee \cdots \vee \psi_\iota \vee \cdots \vee \psi_N)) \geq \delta \\ \Longleftarrow\;\; &\mathbb{P}(\xi(t:N) \models \psi_\iota) \geq \alpha_\iota\, \delta,\ \iota \in \{1, \ldots, N\}, \\ &0 \leq \alpha_\iota \leq 1,\ \alpha_1 + \cdots + \alpha_N = 1. \end{aligned} \tag{2.20}$$

Case II: Conjunction

$$\begin{aligned} &\mathbb{P}(\xi(t:N) \models (\psi_1 \wedge \cdots \wedge \psi_\iota \wedge \cdots \wedge \psi_N)) \geq \delta \\ \Longleftarrow\;\; &\mathbb{P}(\xi(t:N) \not\models \psi_\iota) \leq \beta_\iota(1-\delta),\ \iota \in \{1, \ldots, N\}, \\ &0 \leq \beta_\iota \leq 1,\ \beta_1 + \cdots + \beta_N = 1. \end{aligned} \tag{2.21}$$

Case III: Until

$$\begin{aligned} &\mathbb{P}(\xi(t:N) \models \psi_1 \,\mathsf{U}_{[a,b]}\, \psi_2) \geq \delta \\ \Longleftarrow\;\; &\mathbb{P}(\Lambda_j) \geq \gamma_\iota \frac{\delta}{(b-a+1)}, \iota \in \mathbb{N}, \\ &0 \leq \gamma_\iota \leq 1,\ \gamma_1 + \cdots + \gamma_N = 1, \end{aligned} \tag{2.22}$$

in which, Λ_j is defined as in (2.16).

In relations (2.20)-(2.22), α_ι, β_ι, and γ_ι are intermediate weights that regulate the effect of each probabilistic predicate and contributes to a bigger feasible set. If any knowledge about the likelihood of the satisfaction of sub-formulas in the main formula is available, it can be exploited to select proper values for these parameters to get a less conservative result.

2.5 Verification of Probabilistic STL Constraints with unbounded support

2.5.1 Feasible Set Computation

After transforming the probabilistic STL constraints into the algebraic inequalities, as described in Section 2.4, these inequalities are in the form of (2.18) which are linear with respect to the input trajectory and must hold for the whole input range. We use *robust linear programming* to solve those inequalities. Here, the primary robust linear programming problem is converted to another dual linear programming without a universal quantifier over the input based on Farkas' lemma [34]. Assume the set of valid inputs $\mathcal{U}$ is a bounded polytope characterized by the linear inequalities $Du \leq d$ for some matrix D and vector d with appropriate dimensions. Define the set of valid input trajectories within horizon $\{0, \ldots, (t-1)\}$ with $\boldsymbol{\mathcal{U}} := \{\mathbf{Du} \leq \mathbf{d}\}$, where $\mathbf{u} = [u(0); u(1); \ldots; u(t-1)]$, $\mathbf{d} = [d; d; \ldots; d]$, and $\mathbf{D} = \text{diag}(D, \ldots, D)$.

In the next theorem, we show that the feasible set of the probabilistic predicates at each time step can be characterized by a set of constraints at that time step. The proof of this theorem leverages the dual linear programming in its symmetric form, which requires all variables to be non-negative. Therefore, we extract a lower bound $\mathbf{u}_l$ for the input trajectories and shift the input variables to make them non-negative. This lower bound $\mathbf{u}_l$ is readily computable knowing the bounded polytope containing all the input values.

Theorem 1. *Assume that the set of valid input trajectories $\boldsymbol{\mathcal{U}}$ is a bounded polytope of the form $\mathbf{Du} \leq \mathbf{d}$ such that $\mathbf{u} \geq \mathbf{u}_l$. The inequality* (2.18) *holds for all $\mathbf{u} \in \boldsymbol{\mathcal{U}}$ if the following set of inequalities is feasible over $\mathbf{z}$,*

$$\begin{cases} (\mathbf{d} - \mathbf{Du}_l)^T \mathbf{z} \leq b(\theta, \delta) + \mathbf{f}(\theta)\mathbf{u}_l, \\ -\mathbf{D}^T \mathbf{z} \leq \mathbf{f}(\theta)^T, \quad \mathbf{z} \geq 0, \end{cases} \tag{2.23}$$

where

$$\begin{aligned} & b(\theta, \delta) = \tilde{\theta}_0 + \tilde{\theta}^T A(\theta)^t x(0) + \tilde{\theta}^T \Gamma(\theta, \delta)\tilde{\theta}, \\ & \mathbf{f}(\theta) = \tilde{\theta}^T [B(\theta), A(\theta)B(\theta), A(\theta)^2 B(\theta), \ldots, A(\theta)^{t-1} B(\theta)], \end{aligned} \tag{2.24}$$

with $\Gamma(\theta, \delta)$ defined in (2.19).

Solving constraints (2.23) simultaneously for all predicates of the STL specification gives the feasible set of parameters θ for the stochastic system $\mathbf{S}$ in (2.1). However, the main challenge of using inequalities of the form (2.23) as under-approximation of the feasible set is that these inequalities are still nonlinear with respect to θ. In the following subsection we propose two numerical techniques to address this challenge.

2.5.2 Confidence Computation Techniques

Monte Carlo Method. Considering that the constraints (2.23) are in general nonlinear with respect to θ, computation of integral in (2.6) can be done efficiently using *Monte Carlo integration.* The idea is to choose $\mathbf{N}$ random points θ_i uniformly from the bounded region of the parameters and use those values that satisfy all the constraints in (2.23) associated with the predicates of the STL specification in order to compute the integral in (2.6). The confidence value $Q_{\mathbf{N}}$ computed using Monte Carlo integration is a random variable defined as

$$Q_{\mathbf{N}} := \frac{V}{\mathbf{N}} \sum_{i=1}^{\mathbf{N}} K(\theta_i) \text{ with } K(\theta_i) := f_{\psi}^{\delta}(\theta_i)\, p(\theta_i \mid \mathcal{D}),$$

where V is the volume of the parameter space. Here, $Q_{\mathbf{N}}$ is an unbiased estimator of the integral. Due to the law of large numbers, $Q_{\mathbf{N}}$ converges to the true integral when $\mathbf{N}$ goes to infinity. An unbiased estimation of the variance of $Q_{\mathbf{N}}$ can be computed as $\mathrm{Var}[Q_{\mathbf{N}}] = \frac{V^2\sigma_{\mathbf{N}}^2}{\mathbf{N}}$ with

$$\sigma_{\mathbf{N}}^2 := \frac{1}{\mathbf{N}-1} \sum_{i=1}^{\mathbf{N}} (K(\theta_i) - \bar{K})^2 \text{ and } \bar{K} := \frac{1}{\mathbf{N}} \sum_{i=1}^{\mathbf{N}} K(\theta_i).$$

Note that the $\mathrm{Var}[Q_{\mathbf{N}}]$ decreases to zero asymptotically with rate $1/\mathbf{N}$ when $\mathbf{N}$ goes to infinity and as long as the sequence $\{\sigma_1^2, \sigma_2^2, \sigma_3^2, \ldots\}$ is bounded. This result does not depend on the number of dimensions of the integral in (2.6), which is the advantage of Monte Carlo integration.

According to Chebyshev's inequality, one has

$$\mathbb{P}(\mathbb{E}[Q_{\mathbf{N}}] \in [Q_{\mathbf{N}} - \varepsilon, Q_{\mathbf{N}} + \varepsilon]) \geq 1 - \frac{\mathrm{Var}[Q_{\mathbf{N}}]}{\varepsilon^2}, \tag{2.25}$$

for any given $\varepsilon > 0$. By choosing an appropriate number of samples $\mathbf{N}$ and computing $Q_{\mathbf{N}}$, the exact value of the integral lies within the interval $[Q_{\mathbf{N}} - \varepsilon, Q_{\mathbf{N}} + \varepsilon]$ with confidence $1 - V^2\sigma_{\mathbf{N}}^2/\mathbf{N}\varepsilon^2$.

Computing the under-approximation of the confidence in (2.6) using the Monte Carlo integration requires sampling from the domain Θ and rejecting those that render (2.23) infeasible. It is also possible to find a sampling domain Θ' tighter than Θ by finding the extreme values of θ for which the inequalities (2.23) are feasible. This will improve the efficiency of the Monte Carlo integration by requiring a smaller number of samples for a given accuracy.

Piecewise Affine Approximation of the Nonlinear Constraints. Another approach for computing the confidence value in (2.6) is approximating the nonlinear terms $b(\theta, \delta)$ and $\mathbf{f}(\theta)$ in (2.24) using *piecewise affine* (PWA) functions. Then, linear programming can be used in order to approximate the feasible set. PWA approximations have been used recently in formal approaches in order to deal with the nonlinearity in dynamical systems [13, 82].

Assuming that $A(\theta)$ and $B(\theta)$ are twice differentiable with respect to θ, $b(\theta, \delta)$ and $\mathbf{f}(\theta)$ in (2.24) are also twice differentiable. We can partition their domain into polytopic regions, select a nominal value (θ_0, δ_0) in each region, and rewrite $b(\theta, \delta)$ in each region as

$$b(\theta, \delta) \in (\theta - \theta_0)^T \mathscr{M} + (\delta - \delta_0)\mathscr{N} + \epsilon\mathscr{B}, \tag{2.26}$$

where

$$\mathscr{M} := \frac{\partial b(\theta, \delta)}{\partial \theta}\Big|_{(\theta_0, \delta_0)} \text{ and } \mathscr{N} := \frac{\partial b(\theta, \delta)}{\partial \delta}\Big|_{(\theta_0, \delta_0)},$$

and ϵ is a bound where

$$\epsilon \geq \frac{1}{2}[(\theta-\theta_0)^T,(\delta-\delta_0)]\;\mathbf{H}\;[(\theta-\theta_0);(\delta-\delta_0)],$$

where $\mathbf{H}$ is the Hessian matrix of $b(\theta,\delta)$. Here, $\mathscr{B}$ denotes the unit interval $[-1,1]$. A similar approximation holds for $\mathbf{f}(\theta)$. The region of parameters is divided into sufficiently large numbers of regions and then inequalities and equations regarding the satisfaction of STL specifications in (2.23) will be checked in these regions. In the next lemma, we show that the real feasible set can be constructed in the limit when the number of piecewise regions increases.

Lemma 2. *The actual feasible set* (2.23) *for the STL specification in* (2.6) *can be recovered in the limit by increasing the numbers of regions in PWA approximation of the nonlinear terms in* (2.23)*.*

2.6 Verification of Probabilistic STL Constraints with bounded support

In this section, we show that if the given matrices A and B in (2.1) are independent of the parameters θ and are known, the probabilistic inequalities can be under-approximated by inequalities that are linear in terms of inputs. These inequalities can be solved using linear programming efficiently to compute the feasible region of parameters. The essential idea in this approach is to replace the Gaussian distributions with truncated ones while quantifying the induced error. Having a bounded support for the noise enables us to use Chernoff-Hoeffding inequality [31, 52] for the under-approximation. The Chernoff-Hoeffding inequality provides a bound on the tail probability of sum of bounded random variables that depends only on the support of these random variables regardless of the shape of their distributions. First, we formally define the support of a random variable.

Definition 3. *For a given random variable ω with values in $\mathbb{R}^{\mathsf{n}}$ and probability distribution $\mathbb{P}$, consider the set of subsets of $\mathbb{R}^{\mathsf{n}}$ as*

$$\mathcal{A} := \{C \subset \mathbb{R}^{\mathsf{n}} \mid C \textit{ is closed and } \mathbb{P}(\omega \in C) = 1\}.$$

The smallest element of $\mathcal{A}$ with respect to the inclusion property is called the support of ω and is denoted by S_ω.

The next proposition provides an upper bound on the error of the probability of satisfying the specification when the noise distributions are replaced by truncated Gaussian distributions.

Proposition 3. *Suppose we consider two distributions for the process noise $w(\cdot)$: one which is Gaussian distribution t_w and the other one which is truncated normal $\bar{t}_w$ with* *support S_w. We denote the probability measures induced on the trajectories ξ of the system $M(\theta)$ by $\mathbb{P}$ and $\mathbb{P}_t$, respectively. Then we have*

$$\mathbb{P}(\xi \models \psi) - \mathbb{P}_t(\xi \models \psi) \leq \frac{N\alpha}{1-\alpha}, \tag{2.27}$$

for any specification ψ with horizon N. Here, α is the truncated probability $\alpha := 1 - \int_{S_w} t_w(v)dv$.

Using inequality (2.27), we under-approximate the chance constraint $\mathbb{P}(\xi \models \psi) \geq 1 - \delta$ with

$$\mathbb{P}_{\mathsf{t}}(\xi \models \psi) \geq 1 - \bar{\delta}, \quad \bar{\delta} := \delta + \frac{N\alpha}{1-\alpha}. \tag{2.28}$$

Assumption 3. *For the rest of this section, we focus on under-approximating* (2.28) *when the truncated support of $w(t)$ is S_w and is contained in a hyper-rectangle* $[a, b]$ *(which is the Cartesian product of intervals with vectors a, b indicating the end points of the intervals). We also assume matrices A and B in* (2.1) *are non-parametric.*

Next lemma, borrowed from [31], shows the relation between supports of $\alpha(x(t))$ and $w(t)$ given the predicate $\mu(x) = \{\alpha(x) \geq 0\}$ with $\alpha(x) := \tilde{\theta}_0 + \tilde{\theta}^T x$.

Lemma 3. *The support of $\alpha(x(t))$ is $S_{\alpha(x(t))} := [\tilde{\theta}_0 + \tilde{a}_t + \tilde{\theta}^T \tilde{C}_t, \tilde{\theta}_0 + \tilde{b}_t + \tilde{\theta}^T \tilde{C}_t]$ where $\tilde{a}_t$ and $\tilde{b}_t$ are weighted sum of a and b obtained using interval arithmetics and $\tilde{C}_t := A^t x(0) + \sum_{i=0}^{t-1} A^i Bu(t-i-1)$.*

We use Chernoff-Hoeffding inequality to replace (2.28) with a condition on the expected value of the predicate. The following proposition, used also in [31], describes this approximation. Note that Chernoff-Hoeffding inequality requires a particular constant from the *dependency graph* of the random variables [52]. In such a graph, the nodes represent random variables and two nodes are connected if and only if their related random variables are dependent.

Proposition 4. *The probabilistic inequality $\mathbb{P}_{\mathsf{t}}(\alpha(x(t)) > 0) \geq 1 - \bar{\delta}$ can be under-approximated by the inequality*

$$\mathbb{E}_{\mathsf{t}}(\alpha(x(t))) \geq \sqrt{-\nu \log(\bar{\delta}) \sum_{t=1}^{N} \left(\tilde{b}_t - \tilde{a}_t\right)^2}, \tag{2.29}$$

where $\nu = \mathcal{X}(w)/2$, and $\mathcal{X}(w)$ is the chromatic number *of the dependency graph of the noises $w(0), \ldots, w(N-1)$.*

Note that the chromatic number of a graph $\hat{G}$ is the minimum number of colors needed to color vertices of $\hat{G}$ with no two adjacent vertices sharing the same color. This number is equal to 1 for a graph with no edges (e.g., when disturbances $w(i)$ are independent). The interested authors are referred to [72] and [15] for more information about chromatic number of a graph.

Proposition 5. *Let Assumption 3 hold. We use Lemma 3 and under-approximate constraint* (2.28) *with*

$$\sum_{i=0}^{t-1} \tilde{\theta}^T A^i B \; u(t-i-1) \\ + \tilde{\theta}_0 + \tilde{\theta}^T A^t x(0) \geq \Gamma(\delta, \tilde{a}, \tilde{b}), \tag{2.30}$$

where

$$\Gamma(\delta, \tilde{a}, \tilde{b}) := \sqrt{-\nu \log(\bar{\delta}) \sum_{t=1}^{N} (\tilde{b}_t - \tilde{a}_t)^2}. \tag{2.31}$$

Note that since $\bar{\delta} \in (0, 1)$ and, hence, $\log(\delta) < 0$, the right hand side of the inequality (2.30) becomes a real value and one has a linear inequality in terms of input. Finally, the next theorem shows that the feasible set of the chance-constraints on the predicates can be approximated by a set of *linear* constraints.

Theorem 2. *Assume that the set of input trajectories* $\boldsymbol{\mathcal{U}}$ *is a bounded polytope of the form* $\mathbf{D}\mathbf{u} \leq \mathbf{d}$, $\forall \mathbf{u} \in \boldsymbol{\mathcal{U}}$. *The inequality* (2.30) *holds for all* $\mathbf{u} \in \boldsymbol{\mathcal{U}}$ *if the set of linear inequalities* (2.23) *is feasible over* $\mathbf{z}$, *where*

$$\begin{aligned} b(\theta, \delta) &= \tilde{\theta}_0 + \tilde{\theta}^T A^t x(0) - \Gamma(\delta, \tilde{a}, \tilde{b}), \\ \mathbf{f}(\theta) &= \tilde{\theta}^T [B, AB, A^2B, \ldots, A^{t-1}B], \end{aligned} \tag{2.32}$$

with $\Gamma(\delta, \tilde{a}, \tilde{b})$ *defined in* (2.31).

Remark 1. *In presenting our approach in this section, we assumed that parameters* $\tilde{\theta}_0$ *and* $\tilde{\theta}$ *of the predicate* $\alpha(x(t))$ *are known. We emphasize that our approach is still valid if* $\tilde{\theta}_0$ *and* $\tilde{\theta}$ *depend on the unknown parameters* θ *of the model. This case can happen when the predicate is defined on the output* $\hat{y}(t)$ *instead of the state* $x(t)$ *of the system. The experimental results in the next section demonstrate this case as well.*

2.7 Synthesis Under STL Constraints

The synthesis problem under STL constraints is defined as follows:

Problem 2 (Synthesis). *Given a parameterized LTI system in* (2.1) *together with the noisy output in* (2.2), *data set* $\mathcal{D}$, *and property* ψ, *synthesize an open-loop input trajectory* $u(\cdot)$ *that maximizes the confidence in* (2.6):

$$u(\cdot) = argmax \int_{\Theta} f_{\psi}^{\delta}(\theta) \; p(\theta \mid \mathcal{D}). \tag{2.33}$$

The goal of this section is to synthesize input trajectories such that the confidence of satisfying the property of interest in (2.6) is maximized (see (2.33)). The posterior distribution $p(\theta \mid \mathcal{D})$ comes from the experiment by applying Bayesian inference on the collected data. Moreover, the feasible set Θ_ψ is the set of all parameters θ in the parameter space Θ such that desired STL property is satisfied, and is dependent on the input trajectory. The integration in (2.33) is computed over this feasible set.

In general, the synthesis problem defined in Problem 2 is nonlinear and nonconvex. One can leverage numerical methods to solve this problem. In Algorithm 1, a two-phase procedure is proposed in order to solve the optimization problem combined with collected data from the system. In the first phase, a fixed posterior distribution function is computed using collected data and prior knowledge over the parameter space Θ by the Bayesian inference technique, which is fully described in Section 2.3. In the second phase, this fixed distribution function is used to compute the confidence value over the feasible set, which is restricted by the satisfaction of the STL constraints. Here, Θ_ψ is dependent to the input trajectory, and $f_\psi^\delta(\theta)$ can be computed using (2.4). We leverage genetic algorithm (GA) to find the optimal input trajectory over the desired region of the input values. The highest value of the confidence in the second phase is considered as the maximum confidence, and its related input sequence is chosen as the desired input trajectory.

Algorithm 1 Synthesizing input sequence in order to maximize the confidence

```
 1: Bayesian Data Analysis (Phase I)
 2: input: $M(\theta)$,$\Theta$, $\mathcal{D}$, $p(\theta)$
 3: output: $p(\theta \mid \mathcal{D})$
 4: Posterior distribution computation:
    Compute $p(\theta \mid \mathcal{D})$ using (2.8)
 5: Controller Synthesis (Phase II)
 6: input: bounded input region $\mathcal{U}$, $p(\theta \mid \mathcal{D})$, and desired STL property
 7: output: maximum confidence, and optimized input sequence $u^*$.
 8: Computation of satisfaction function:
    Compute $f_\psi^\delta(\theta)$ using (2.4)
 9: Optimization:
    $\max_u \quad \int_\Theta f_\psi^\delta(\theta) p(\theta \mid \mathcal{D})$ using genetic algorithm
10: Selection:
11: Maximum confidence $\leftarrow$optimal solution of 9
12: $u^* \leftarrow$ related input trajectory
```

2.8 Experimental Results

In this section, we demonstrate the effectiveness of our proposed approaches through three case studies, including two verification problems and one synthesis problem.

2.8.1 Verification Case Study: Unbounded Support Noise

Consider a parameterized class of models $\mathrm{M}(\theta)$ with the state-space representation

$$\begin{aligned} x(t+1) &= \begin{bmatrix} a & 0 \\ 1-a^2 & a \end{bmatrix} x(t) + \begin{bmatrix} \sqrt{1-a^2} \\ -a\sqrt{1-a^2} \end{bmatrix} u(t) + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} w(t), \\ \hat{y}(t,\theta) &= \theta^T x(t). \end{aligned}$$

Each model in $\mathrm{M}(\theta)$ has a single input and a single output. The coefficient a is 0.4 and the parameter set is selected as $\theta \in \Theta = [-10, 10] \times [-10, 10]$. The system $\mathbf{S} \in \mathrm{M}(\theta)$ has the true parameter $\theta_{\texttt{true}} = [-0.5, 1]^T$. System $\mathbf{S}$ is a member of models demonstrated by the Laguerre-basis functions [41]. This is a special case of the orthonormal basis functions and can be translated to the aforementioned parameterized state space format. The system is affected by a process noise which is a Gaussian process with covariance matrix $0.5\mathbb{I}_2$, where $\mathbb{I}_2$ is a 2×2 identity matrix. There is also an additive measurement noise with zero-mean and variance 0.5. The input range is considered to be $[-0.2, 0.2]$.

We want to verify with high probability if the output of the system $\mathbf{S}$ remains in $\mathfrak{l}_1 = [-0.5, 0.5]$ until it reaches $\mathfrak{l}_2 = [-0.1, 0.1]$ at some time in the interval $[2, 4]$. We denote the atomic propositions $\mu_1 = \{y \geq -0.5\}$, $\mu_2 = \{-y \geq -0.5\}$, $\mu_3 = \{y \geq -0.1\}$, $\mu_4 = \{-y \geq -0.1\}$. Our desired property can be written as

$$\mathbb{P}(\mathbf{S} \models (\mu_1 \wedge \mu_2)\ \mathsf{U}_{[2,4]}\ (\mu_3 \wedge \mu_4)) \geq 1 - \delta.$$

We select $\delta = 0.01$. The system starts at the initial condition $x(0) = 0$.

We used the procedure in Section 2.4 to decompose this STL specification to algebraic constraints on the atomic propositions. Equation (2.21) is used to improve the conservativeness of the approximation. The feasible set is approximated either using the Monte Carlo method or the piecewise affine approximation described in Section 2.5. The initial set of parameters can be restricted by finding the extreme values of θ over all constraints as described in Subsection 2.5.2 which is considered $[-3.5, 3.5]$ for this case study. We select random points which are uniformly distributed in this restricted region in order to compute the confidence value using the Monte Carlo method with the precision 0.000001 in (2.25). Computed feasible set using the Monte Carlo technique is demonstrated in Fig. 2.3 with red-face squares. The feasible set which is recovered with the piecewise affine technique is illustrated in Fig. 2.3 with blue-edge diamonds. We used linear programming in order to find the feasible set of parameters $(\theta, \mathbf{z})$ for the linearized form of (2.23) for all time steps. Then, this feasible set is projected into θ space using MPT3 toolbox [47]. We choose the total number of regions in the piecewise affine approximation to be 25.

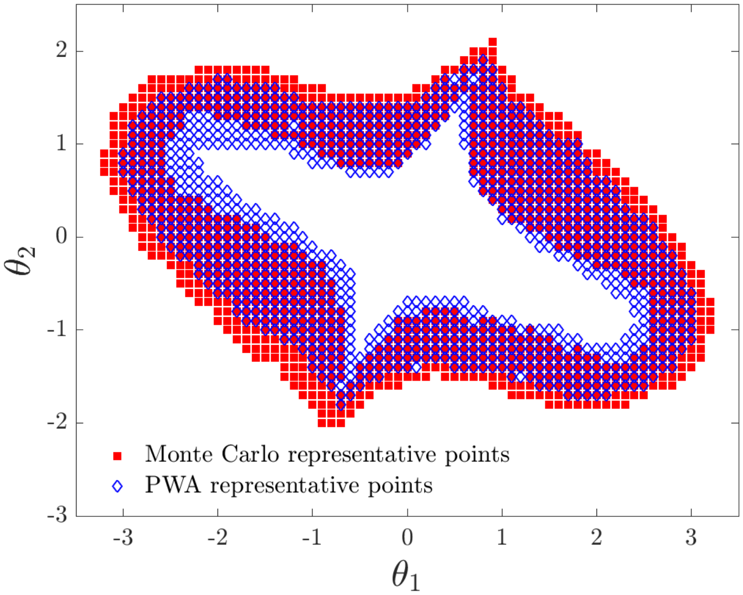


Figure 2.3: Contours of $p(\theta \mid \mathcal{D})$ for $\theta_{\texttt{true}} = [-0.5, 1]^T$ after 50 measurements over the feasible set computed by the Monte Carlo and PWA techniques which are represented by red and blue points, respectively.

As we do not have any prior knowledge about the parameters, we choose a uniform distribution $p(\theta)$ on the possible models. Based on the uniform prior, the confidence is computed using (2.6) as 0.0279 and 0.0258 with Monte Carlo and PWA approximations, respectively. Afterward, we designed an experiment on the system with the true parameter and an input sequence with a uniform distribution over $[-2, 2]$ and measured output for 50 consecutive time instances. Using updated $p(\theta \mid \mathcal{D})$ coming from the measurement data, confidence improved significantly into 0.9099 and 0.8962 for Monte Carlo and PWA, respectively. Contours of the posterior distribution are illustrated in Fig. 2.3.

We repeated the same experiment 100 times for several other true parameters $\theta_{\texttt{true}}$. For all of these instances, updated posteriori probability in (2.11), after 50 measurements, is used in order to compute the confidence value according to (2.6). Results of computing the confidence with Monte Carlo and PWA approximation are shown in Table 1. As it can be seen, for parameters that lie deep inside the feasible set, the confidence value is high with a low variance for both techniques. Meanwhile, for the points near the edges, the variance is higher and confidence value is lower. For points far enough from the feasible set, confidence tends to be very close to zero.

Table 2.1: Means and variances of computed confidence for 5 different true parameters.

	Monte Carlo		PWA	
$\theta_{\mathtt{true}}$	Mean	Variance	Mean	Variance
$[-0.5, 1]^T$	0.9587	0.0023	0.9514	0.0042
$[3, -1]^T$	0.4902	0.0061	0.5032	0.0062
$[1, 0.5]^T$	0.7932	0.0025	0.7584	0.0053
$[-2, 1.5]^T$	0.9018	0.0009	0.9156	0.0005
$[2, -1]^T$	0.0278	0.0005	0.0480	0.0006

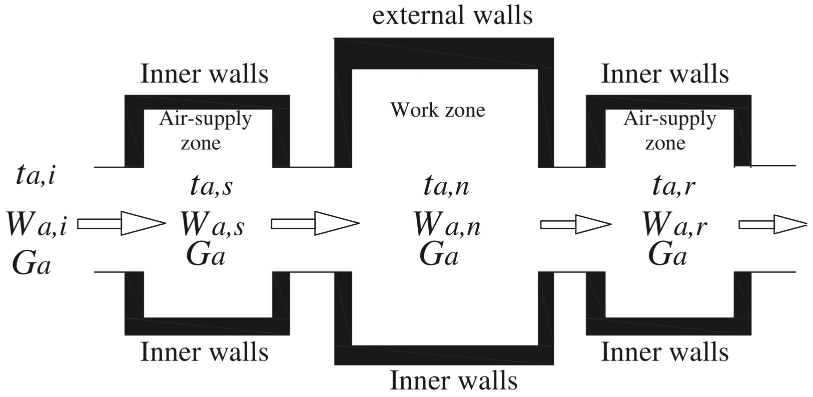


Figure 2.4: Schematic of the air-conditioned building [111].

2.8.2 Verification Case Study: Bounded Support Noise

In this section, we consider the multi-zone model of a building developed in [111]. The model gives the dynamic response of indoor temperatures and humidity for a building depicted in Fig. 2.4. The state vector is $X_{room} = [\Delta t_{a,s}, \Delta W_{a,s}, \Delta t_{riw,s}, \Delta t_{a,n}, \Delta W_{a,n}, \Delta t_{riw,n}, \Delta t_{rew,n}, \Delta t_{a,r}, \Delta W_{a,r}, \Delta t_{riw,r}]^T$, where its elements are variations in air-supply temperature, air-supply humidity, internal wall temperature (air-supply zone), work zone temperature, work zone humidity, internal wall temperature (work zone), external wall temperature (work zone), air-return temperature, air-return humidity, and internal wall temperature (air-return zone), respectively. The input vector is $[\Delta t_{a,i}, \Delta W_{a,i}, \Delta G_{a,i}, \Delta t_{a,out}, \Delta I_{sol}]$ which its elements correspond to air-supply temperature set-point, air-supply humidity set-point, air flow set-point, return temperature set-point, and solar radiant intensity, respectively.

All states are affected by a Gaussian process noise with variance of 0.001. We assume the input can change every 100 seconds. Then we discretize the dynamic by $\tau = 100s$. The comfort criterion is defined as a weighted combination of work zone temperature and humidity variations: $\theta_1 \Delta t_{a,n} + \theta_2 \Delta W_{a,n}$ with weights θ_1 and θ_2. This comfort criterion is the output of the system. The measurements of this output is available but affected by a Gaussian noise with variance 0.01. We consider the following STL specification:

$$\mathbb{P}\left(\bigwedge_{t=1}^{5} |\theta_1 \Delta t_{a,n}(t) + \theta_2 \Delta W_{a,n}(t)| \leq \beta\right) \geq 0.99, \tag{2.34}$$

with $\beta = 1$ in our numerical implementation. We assume that θ_1 and θ_2 are not known but have the true values 1 and 0.5, respectively ($\theta_{\mathtt{true}} = [1, 0.5]^T$). The initial parameter space is considered to be $(\theta_1, \theta_2) \in [-2.5, 2.5]^2$. Our goal is to verify whether the above property is satisfied for all inputs $\Delta t_{a,i}$,$\Delta W_{a,i} \in [-1, 1]$. Other inputs are considered to be zero in this case study.

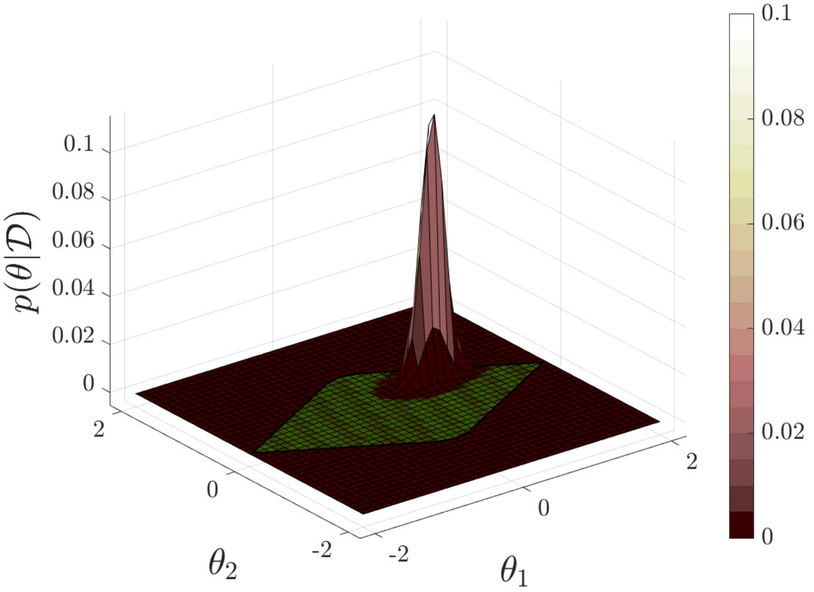


Figure 2.5: Updated posterior function after 10 measurements over the feasible polyhedron region computed using MPT3 toolbox.

We utilize the approach of Section 2.6 and limit the supports of process noise to the bounded interval $[-0.1, 0.1]$. This amounts to having $\alpha = 0.0155$ in Proposition 3 and replacing the above chance constraint with

$$\mathbb{P}_{\mathtt{t}}\left(\bigwedge_{t=1}^{5} |\theta_1 \Delta t_{a,n}(t) + \theta_2 \Delta W_{a,n}(t)| \leq \beta\right) \geq 0.9787.$$

The computed feasible region for this STL specification which is a polyhedron and computed by MPT3 toolbox [47] is demonstrated in Fig. 2.5 (green region). Since it is assumed that we do not have any prior knowledge about the parameters, a uniform distribution is chosen over the parameter space. The posterior distribution is illustrated in Fig. 2.5 after collecting 10 measurements and updating the distribution. This approach computes the feasible region and the confidence value in only 55 seconds. We have repeated this experiment 100 times and computed the confidence values using (2.6). The mean and variance of the confidence values are respectively 0.8607 and 0.0012.

If we directly apply the approach of Section 2.5 to the constraint (2.34) and the unbounded support noise, we have to use the methods in Subsection 2.5.2 in order to approximately compute the confidence value, which is computationally more expensive. We computed the confidence value using Monte Carlo integration with 6.25×10^6 samples from the parameter space, which gives the interval $[0.8505, 0.8705]$ for the confidence with probability 0.99 over the sampled parameters. This interval is close to the confidence value obtained using truncation but the computation time is 19 minutes on an iMac (3.5 GHz Intel Core i7 processor) which is much larger than 55 seconds taken based on truncation.

2.8.3 Synthesis Case Study

In this section, we apply our approach to control a helicopter in the hover mode, which is a difficult task since the helicopter model is unstable. Stochasticities such as wind, harsh weather, and structural uncertainties exacerbate this situation as well.

We consider an eight-dimensional helicopter model taken from [71]. States vector is $[u, w, q, \theta_p, v, p, \phi, r]$ that contains helicopter velocities u, v, w, Euler angles θ_p, ϕ, and the angular velocities p, q, r. This model has a three-dimensional input vector $[u_1, u_2, u_3]$, where u_1, u_2, and u_3 are desired values for pitch angle, roll angle, and yaw rate, respectively. They are used to produce commands for the longitudinal cyclic, lateral cyclic, and tail rotor collective. Pitch angle rate q is an important parameter in hover mode which its variations depends highly on itself and roll angle rate p. We show this dependency in the system states model with two unknown parameters ϑ_1 and ϑ_2. We stabilized the continuous-time system with a primary state feedback controller and discretize that with a sampling time $\tau = 0.01s$. Resulted matrices are demonstrated in the appendix. All states of the system are affected by an additive process noise with the variance $\delta_p^2 = 0.1$. We consider the pitch angle rate as the measured output of the system, affected by an additive noise with variance $\delta_m^2 = 0.1$. Parameter set is chosen as $\theta = (\vartheta_1, \vartheta_2) \in [-10, 10]^2$. We choose the true parameter as $\theta_{true} = [-1.85\ 0.5]^T$.

We aim to synthesize a controller for the helicopter that maximizes the confidence of remaining in a specific position by an admissible range of inputs, as this is desired in the hover mode maneuvering. Here, we want to keep the location (i.e. (x, y, z)) of the helicopter in the range of $[-1, 1] \times [-1, 1] \times [-0.5, 0.5]$ for 5 time steps, which can be represented as

$$\mathbb{P}\big(\Box_{[i=1:5]}(x_i \in [-1,1] \wedge y_i \in [-1,1] \wedge z_i \in [-0.5, .05]\big) \geq 0.95.$$

Here, we consider the admissible range of inputs to be $[-0.25, 0.25]^3$.

We use the first phase of Algorithm 1 in order to update a uniform distribution over the parameter set for 400 measurements of the system. Then, this updated distribution is used to find the optimal input trajectories and maximum confidence value, as described in the second phase of Algorithm 1. The feasible set regarding the obtained optimal input sequence is illustrated in Fig. 2.6 with blue squares as representative points. Contours of the updated posterior distribution after gathering 400 measurements from the system are demonstrated in this figure as well. Synthesized input trajectories are shown in Fig. 2.7. Three-dimensional location of the helicopter is depicted in Fig. 2.8 for five seconds and for 12 different executions. Helicopter's projected position in $x - y$ plane, and altitude are depicted in Fig. 2.9 and Fig. 2.10, respectively. The final locations of the helicopter after five seconds are indicated by red-face squares. As it can be seen, the location of the helicopter remains inside the desired region during the whole time horizon.

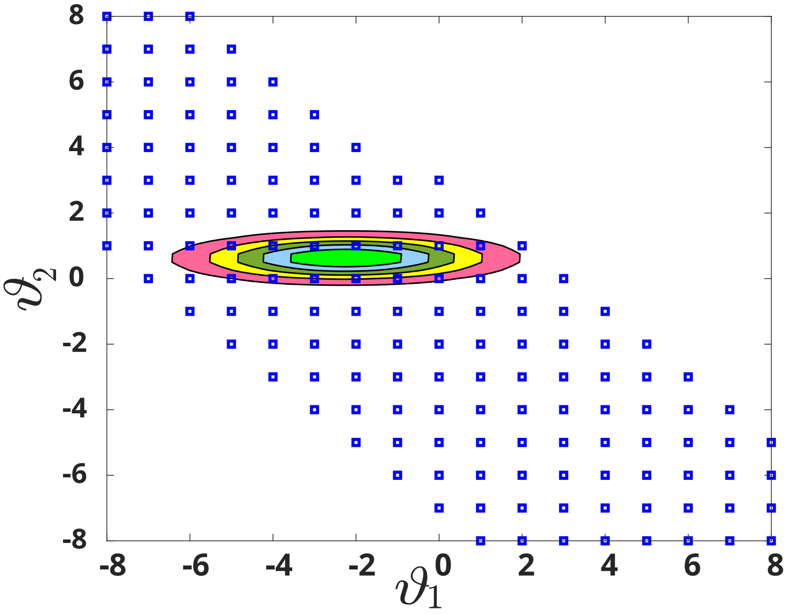


Figure 2.6: Contours of the updated posterior distribution function for $\theta_{true} = [-1.85\ 0.5]^T$ after 400 measurements over the obtained feasible set representatives.

2.9 Discussion

In this chapter, we considered parametric linear time-invariant (LTI) systems. We developed a scheme for providing a confidence value for the satisfaction of STL specifications for such systems by incorporating both model-based and Bayesian inference techniques. Using our approach, one can transform the probabilistic STL specification over the states of the system into a set of algebraic inequalities. Solving these inequalities for the whole range of inputs results in the feasible set of parameters. By leveraging the collected data from the system, the probability density of the unknown parameters is updated and the confidence value is computed over the feasible domain of the parameters.

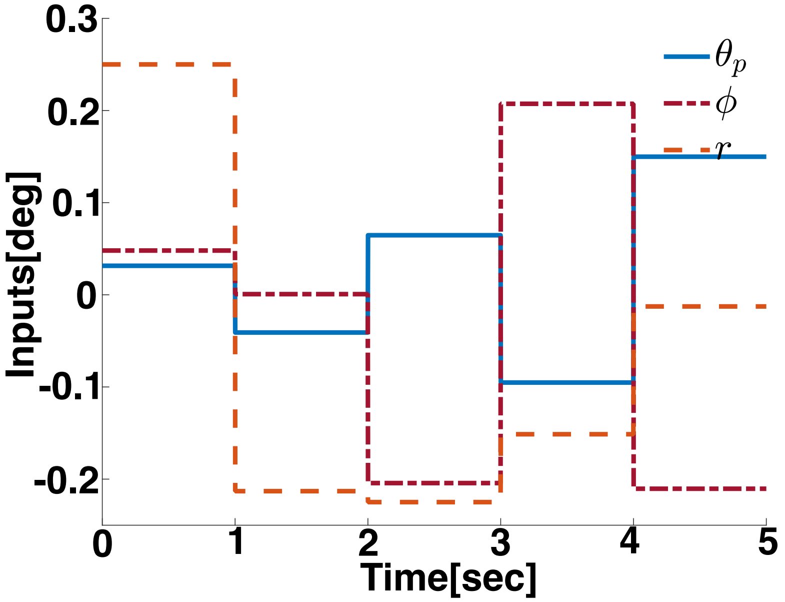


Figure 2.7: Synthesized input trajectories according to Algorithm 1.

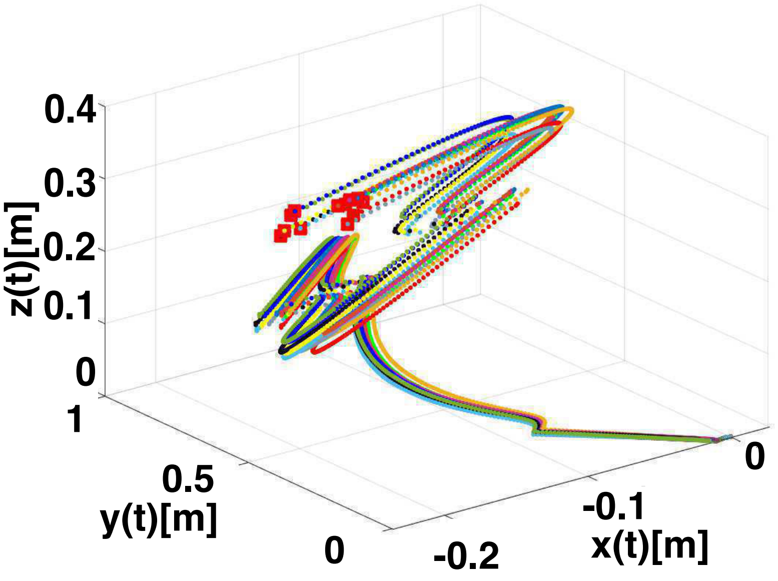


Figure 2.8: 3-dimensional location of the helicopter.

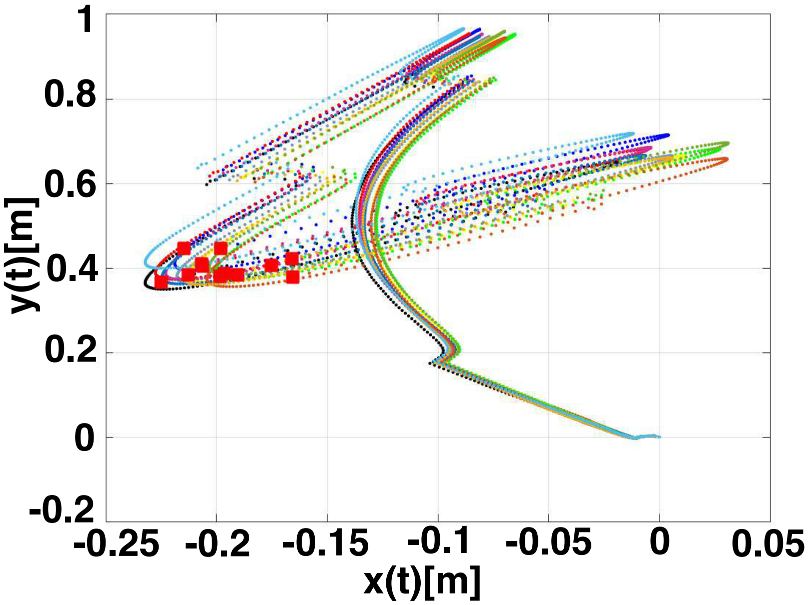


Figure 2.9: x-y plane location of the helicopter.

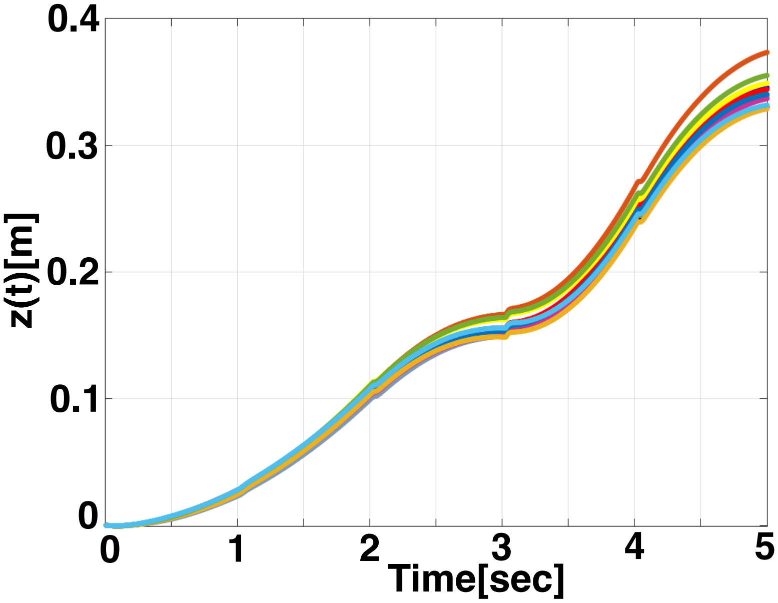


Figure 2.10: Helicopter altitude changes.

Chapter 3

Data-Driven Verification and Synthesis of Stochastic Systems Through Barrier Certificates

3.1 Introduction

In this chapter, we study verification and synthesis problems for safety specifications over unknown discrete-time stochastic systems using finite number of samples.

3.1.1 Motivation

The importance of ensuring safety and meeting temporal requirements in various applications, such as self-driving cars, power grids, traffic networks, and integrated medical devices, has increased significantly. To address the complex requirements of these practical systems, researchers have extensively studied model-based approaches, which involve expressing the requirements as linear temporal logic formulae [35, 6, 103, 8]. Additionally, in the domain of formal approaches for stochastic systems, several abstraction-based methods have been developed to verify and synthesize dynamical systems, ensuring compliance with desired specifications [60, 66, 101, 114]. These techniques are also capable of handling infinite-horizon specifications [39]. To enhance the scalability of abstraction-based methods, various other techniques have been introduced, including sequential gridding [97, 95], higher-order approximations [96], discretization-free abstraction [115], and compositional abstraction-based techniques [98]. Furthermore, model-order reductions and coupled stochastic simulation relations have been devised to assess properties of stochastic systems [39, 38, 40, 105].

Barrier certificates have been the focus of the recent literature as an abstraction-free technique that is scalable with the dimension of the system, i.e., they do not require construction of an abstraction of the system and can provide directly the controller together with the guarantee on the satisfaction of the safety specification [116], [110], and [14]. A barrier-based methodology is introduced in [74] in order to verify safety in deterministic hybrid systems. In [75], a framework is proposed for safety verification of stochastic systems using barrier certificates which is extended to stochastic hybrid systems. The authors in [106] present barrier certificates that ensure collision-free behaviors in multi-robot systems by minimizing the difference between the actual and the nominal controllers subject to safety constraints. In [94], a compositional analysis is proposed for verifying the safety of an interconnection of subsystems using barrier certificates. The results in [50, 51] use barrier certificates for the verification and synthesis of controllers against complex requirements expressed as co-safe linear temporal logic formulas.

The common requirement of the approaches mentioned above is the fact that they need a mathematical model of the system. However, a precise model of dynamical systems is either not available in many application scenarios or too complex to be of any use. Therefore, there is a need to develop approaches which are capable of verifying or synthesizing controllers against safety specifications only based on collected data from the system.

3.1.2 Contributions

Here, we propose formal verification and synthesis procedures for unknown stochastic systems with respect to safety specifications based on collected data. We first cast a barrier-based safety problem as a robust convex program (RCP). Solving the obtained RCP is hard in general because the unknown model of the system appears in the constraints. To tackle this issue, we resort to a scenario-driven approach by collecting samples from the system. Using the results in [29], we connect the optimal solution of the acquired scenario convex program (SCP) with that of the original RCP. We provide a lower bound on the safety probability of the unknown stochastic system using a certain number of data which is related to the desired confidence. We extend this result to provide a new confidence bound for a class of non-convex barrier-based safety problems. We conclude the chapter by three case studies to illustrate the applicability of our approach.

I need to mention that the results presented in this chapter appear in the publications [83, 84]. The first result has been presented at the 7th IFAC conference on analysis and design of hybrid systems. The second result has been published in the Automatica journal. The author of the thesis has established the results and written the drafts. Abolfazl Lavaei contributed to initial discussions. Sadegh Soudjani and Majid Zamani supervised the work.

3.2 Preliminaries and Problem Statement

3.2.1 Notations and Preliminaries

The set of positive integers, non-negative integers, real numbers, non-negative real numbers, and positive real numbers are denoted by $\mathbb{N} := \{1, 2, 3, \ldots\}$, $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$, $\mathbb{R}$, $\mathbb{R}_0^+$, and $\mathbb{R}^+$, respectively. We denote the indicator function of a set $\mathscr{A} \subseteq X$ by $\mathbb{1}_{\mathscr{A}} : X \to \{0, 1\}$, where $\mathbb{1}_{\mathscr{A}}(x)$ is 1 if $x \in \mathscr{A}$, and 0 otherwise. Notation $\mathbf{1}_m$ is used to indicate a column vector of ones in $\mathbb{R}^{m\times 1}$. We denote by $\|x\|$ the Euclidean norm of any $x \in \mathbb{R}^n$. We also denote the induced norm of any matrix $A \in \mathbb{R}^{m\times n}$ by $\|A\| = \sup_{x\neq 0}\|Ax\|/\|x\|$. Given N vectors $x_i \in \mathbb{R}^{n_i}$, $n_i \in \mathbb{N}$, and $i \in \{1,\ldots,N\}$, we use $[x_1;\ldots;x_N]$ and $[x_1,\ldots,x_N]$ to denote the corresponding column and row vectors, respectively, with dimension $\sum_i n_i$. The absolute value of a real number x is denoted by $|x|$. For a function $f : X \to Y$, we denote its inverse by $f^{-1} : Y \to X$, whenever exists. A regularized incomplete beta function for parameters $(z;a,b)$ is defined as $\mathrm{I}(z;a,b) = \frac{\int_0^z u^{a-1}(1-u)^{b-1}du}{\int_0^1 u^{a-1}(1-u)^{b-1}du}$. If a system, denoted by $\mathcal{S}$, satisfies a property Ψ during a time horizon $\mathcal{H}$, it is denoted by $\mathcal{S} \models_{\mathcal{H}} \Psi$. We also use $\models$ in this chapter to show the feasibility of a solution for an optimization problem.

The sample space of random variables is denoted by Ω. The Borel σ-algebras on a set X is denoted by $\mathfrak{B}(X)$. The measurable space on X is denoted by $(X,\mathfrak{B}(X))$. We have two probability spaces in this chapter. The first one is represented by $(X,\mathfrak{B}(X),\mathbb{P})$ which is the probability space defined over the state set X with $\mathbb{P}$ as a probability measure. The second one, $(V_w,\mathfrak{B}(V_w),\mathbb{P}_w)$, defines the probability space over V_w for the random variable w affecting the stochastic system with $\mathbb{P}_w$ as its probability measure. With a slight abuse of the notation, we use the same $\mathbb{P}$ and $\mathbb{P}_w$ when the product measures are needed in the formulations. Considering a random variable z, $\mathrm{Var}(z) := \mathbb{E}(z^2) - (\mathbb{E}(z))^2$ denotes its variance with $\mathbb{E}$ being the expectation operator.

3.2.2 System Definition

In this chapter, we first deal with (potentially) unknown discrete-time continuous-space stochastic dynamical systems as formalized next.

Definition 4. *A discrete-time stochastic system (dt-SS) is a tuple $\mathcal{S} = (X, V_w, w, f)$, where the Borel set $X \subset \mathbb{R}^n$ is the state set of the system, the Borel set V_w is the uncertainty space, $w := \{w(t) : \Omega \to V_w, t \in \mathbb{N}_0\}$ is a sequence of independent and identically distributed (i.i.d.) random variables on the Borel space V_w with some distribution $\mathbb{P}_w$, and the map $f : X \times V_w \to X$ is a measurable function that characterizes the state evolution of the system. The state trajectory of the system is constructed according to*

$$\mathcal{S} : x(t+1) = f(x(t), w(t)), \quad t \in \mathbb{N}_0. \tag{3.1}$$

We denote a finite trajectory of the system by $\xi(t) := x(0)x(1)\ldots x(t)$, $t \in \mathbb{N}_0$.

In this chapter, we assume that the map f and the distribution of the uncertainty $\mathbb{P}_w$ are unknown. Instead, we assume we can collect N *independent* and *identically distributed* state pairs (x_i, x_i^+) by initializing the system at x_i and observing its next state as $x_i^+ = f(x_i, w_i)$ for some random sample w_i. The collected dataset is denoted by

$$\mathcal{D} := \Big\{(x_i, x_i^+)\Big\} \subset X^2, \quad i \in \{1, \cdots, N\}. \tag{3.2}$$

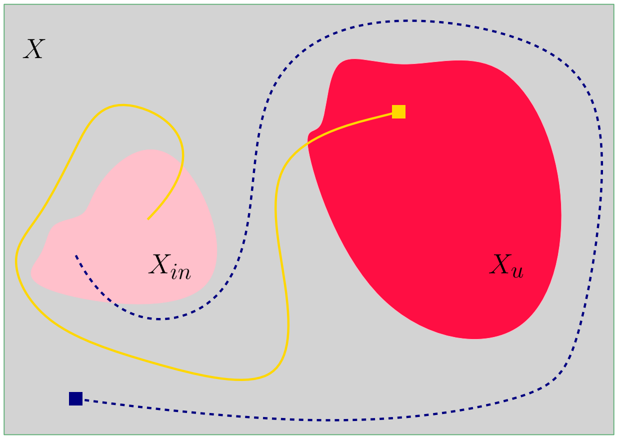


Figure 3.1: A set X containing initial and unsafe sets X_{in} and X_u. The (blue) dashed line illustrates a safe trajectory of the system, whereas the yellow one demonstrates an unsafe trajectory.

3.2.3 Problem Statement

Next definition introduces the safety specification for the unknown stochastic system in Definition 4.

Definition 5. *Given a set of initial states $X_{in} \subset X$, a set of unsafe states $X_u \subset X$, and a finite time horizon $\mathcal{H} \in \mathbb{N}_0$, the system $\mathcal{S}$ is called safe if all trajectories of $\mathcal{S}$ that start from X_{in} never reach X_u within horizon $\mathcal{H}$. We denote this safety property by Ψ and its satisfaction by $\mathcal{S}$ is written as $\mathcal{S} \models_{\mathcal{H}} \Psi$.*

A state set X containing the initial and unsafe sets is illustrated in Fig. 3.1.

Since the system is stochastic and we do not know the distribution of w and the map f, we are interested in establishing a lower bound on the probability that the safety property Ψ is satisfied by the trajectories of $\mathcal{S}$ while using only a dataset of the form (3.2). Now, we state the main problem we are interested to solve here.

Problem 3. *Consider an unknown dt-SS $\mathcal{S}$ as in Definition 4. Provide a lower bound $(1-\rho) \in [0,1]$ on the probability of satisfying Ψ,* i.e.,

$$\mathbb{P}_w\big(\mathcal{S} \models_{\mathcal{H}} \Psi\big) \geq 1-\rho,$$

together with a confidence $(1-\beta) \in [0,1]$ using only a dataset $\mathcal{D}$ of the form (3.2). Moreover, establish a connection between the required size of dataset $\mathcal{D}$ and the desired confidence $1-\beta$.

Therefore, we are interested in finding a potentially tight lower bound. The confidence $1-\beta$ in the statement of the problem is with respect to the probability distribution of the dataset $\mathcal{D}$ and is seen from the frequentist interpretation of probability: any algorithm that solves this problem collects dataset $\mathcal{D}$ using a probability distribution; while running

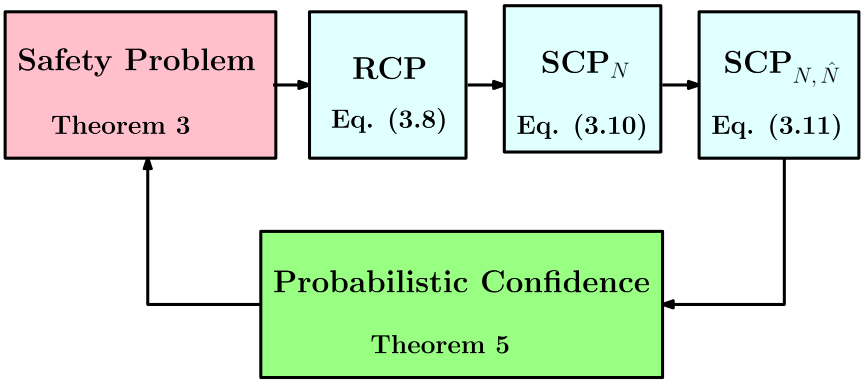


Figure 3.2: This figure shows an overview of the proposed scenario approach for verification of the safety specification.

the algorithm multiple times with different datasets $\mathcal{D}$, the algorithm gives wrong results (incorrect lower bound on the safety probability) in at most β portion of the algorithm runs.

Fig. 3.2 shows an overview of our approach. The block on the left represents a stochastic safety problem. The RCP block reformulates the safety problem as a robust optimization problem. Blocks SCP_N and $\mathrm{SCP}_{N,\hat{N}}$ solve the optimization problem introduced by the RCP block using finite number of samples. Finally, Theorem 5 connects SCP's solutions to the original safety problem.

3.2.4 Safety Verification via Barrier Certificates

Next we define the notion of barrier certificate (BC) for stochastic systems with known models.

Definition 6. *Given a dt-SS $\mathcal{S} = (X, V_w, w, f)$, a nonnegative function $\mathrm{B} : X \to \mathbb{R}_0^+$ is called a barrier certificate (BC) for $\mathcal{S}$ if there exist constants $\lambda > 1$ and $c \in \mathbb{R}_0^+$ such that*

$$\mathrm{B}(x) \leq 1, \qquad \forall x \in X_{in}, \tag{3.3}$$

$$\mathrm{B}(x) \geq \lambda, \qquad \forall x \in X_u, \tag{3.4}$$

$$\mathbb{E}\Big[\mathrm{B}(f(x,w)) \mid x\Big] \leq \ \mathrm{B}(x) + c, \qquad \forall x \in X, \tag{3.5}$$

where $X_{in} \subset X$ and $X_u \subset X$ are initial and unsafe sets corresponding to a given safety specification Ψ, respectively.

Next theorem, borrowed from [51], provides a lower bound on the probability of satisfaction of the safety specification for a dt-SS.

Theorem 3. *Consider a dt-SS $\mathcal{S}$ and a safety specification Ψ. Assume there exists a nonnegative barrier certificate $\mathrm{B}(x)$ which satisfies conditions (3.3)-(3.5) with constants λ and* *c. Then*

$$\mathbb{P}_w\big(\mathcal{S} \models_{\mathcal{H}} \Psi\big) \geq 1 - \frac{1 + c\,\mathcal{H}}{\lambda}, \tag{3.6}$$

with $\mathcal{H} \in \mathbb{N}_0$ being the finite time horizon associated with Ψ.

In this chapter, we consider polynomial-type barrier certificates denoted by $\mathrm{B}(b, x)$, where b is the vector containing the coefficients of the polynomial. Such a polynomial with degree $k \in \mathbb{N}_0$ has the form

$$\mathrm{B}(b, x) = \sum_{\iota_1=0}^{k} \dots \sum_{\iota_n=0}^{k} b_{\iota_1,\dots,\iota_n}(x_1^{\iota_1} \dots x_n^{\iota_n}), \tag{3.7}$$

with $b_{\iota_1,\dots,\iota_n} = 0$ for $\iota_1 + \ldots + \iota_n > k$. Hence, finding a polynomial barrier certificate reduces to determining the coefficients of the polynomial, namely $b_{\iota_1,\dots,\iota_n}$. In the next section, we provide our data-driven approach for the construction of polynomial-type barrier certificates.

3.3 Data-driven Safety Verification

We first cast the barrier-based safety problem in Theorem 3 as a robust convex programming (RCP). We then provide a scenario-based approach in order to solve the obtained RCP using data collected from the system.

Satisfying the conditions of Theorem 3 is equivalent to having a non-positive value for the optimal solution of the following RCP (i.e., $\mathcal{K} \leq 0$):

$$\text{RCP}: \begin{cases} \min\limits_{d} \quad \mathcal{K} \\ \text{s.t.} \quad \max_z \big(g_z(x, d)\big) \leq 0, z \in \{1, \dots, 5\}, \forall x \in X, \\ \qquad d = [\mathcal{K}; \lambda; c; b_{\iota_1,\dots,\iota_n}], \\ \qquad \mathcal{K} \in \mathbb{R},\ \lambda > 1,\ c \geq 0, \end{cases} \tag{3.8}$$

in which,

$$\begin{aligned} g_1(x, d) &= -\mathrm{B}(b, x) - \mathcal{K}, \\ g_2(x, d) &= (\mathrm{B}(b, x) - 1 - \mathcal{K})\mathbb{1}_{X_{in}}(x), \\ g_3(x, d) &= (-\mathrm{B}(b, x) + \lambda - \mathcal{K})\mathbb{1}_{X_u}(x), \\ g_4(x, d) &= \frac{1 + c\,\mathcal{H}}{\rho} - \lambda - \mathcal{K}, \\ g_5(x, d) &= \mathbb{E}\Big[\mathrm{B}(b, f(x, w)) \mid x\Big] - \mathrm{B}(b, x) - c - \mathcal{K}, \end{aligned} \tag{3.9}$$

where $(1 - \rho)$ is a given lower bound for the safety probability.

Remark 2. *The RCP* (3.8) *is in fact a robust convex optimization. It is a convex optimization since the constraints are convex with respect to decision variables in* d *and objective function. It is a robust optimization since the constraints have to hold for all* $x \in X$.

Remark 3. *The RCP* (3.8) *always has a feasible solution. For instance, by choosing coefficients of* $\mathrm{B}(b, x)$ *equal to zero,* $\lambda = 2$, $c = 0$, *and* $\mathcal{K} \geq \frac{1}{\rho} - 2$, *we get a feasible solution for the RCP. Moreover, the barrier certificate obtained from this RCP satisfies conditions* (3.3)-(3.5) *as long as* $\mathcal{K} \leq 0$.

Finding an optimal solution for the RCP in (3.8) is difficult in general because the map f is unknown, the probability measure $\mathbb{P}_w$ is also unknown (thus the expectation in g_5 cannot be computed analytically), and there are infinitely many constraints in the robust optimization since $x \in X$, where X is a continuous set. To tackle this, we first assign a probability distribution to the state set, take N i.i.d. samples $\{x_1, x_2, \ldots, x_N\}$ from this distribution, and replace the robust quantifier $\forall x \in X$ with $\forall x_i \in X$, $i \in \{1, 2, \ldots, N\}$. This results in the following scenario convex program denoted by SCP_{N}:

$$\mathrm{SCP}_{N} : \begin{cases} \min\limits_{d} & \mathcal{K} \\ \text{s.t.} & \max_z \; g_z(x_i, d) \leq 0, \;\; \forall i \in \{1, \ldots, N\}, \\ & \qquad z \in \{1, \ldots, 5\}, \\ & d = [\mathcal{K}; \lambda; c; b_{\iota_1, \ldots, \iota_n}], \\ & \mathcal{K} \in \mathbb{R}, \;\; \lambda > 1, \;\; c \geq 0. \end{cases} \tag{3.10}$$

To tackle the issue of unknown $\mathbb{P}_w$, we replace the expectation in g_5 with its empirical approximation by sampling $\hat{N}$ i.i.d. values w_j, $j \in \{1, \ldots, \hat{N}\}$, from $\mathbb{P}_w$ for each x_i, which gives the following scenario convex program denoted by $\mathrm{SCP}_{N,\hat{N}}$:

$$\mathrm{SCP}_{N,\hat{N}} : \begin{cases} \min\limits_{d} & \mathcal{K} \\ \text{s.t.} & \max_z \; \bar{g}_z(x_i, d) \leq 0, \;\; \forall i \in \{1, \ldots, N\}, \\ & \qquad z \in \{1, \ldots, 5\}, \\ & d = [\mathcal{K}; \lambda; c; b_{\iota_1, \ldots, \iota_n}], \\ & \mathcal{K} \in \mathbb{R}, \;\; \lambda > 1, \;\; c \geq 0, \end{cases} \tag{3.11}$$

where $\bar{g}_z := g_z$ for all $z \in \{1, 2, 3, 4\}$ and

$$\bar{g}_5(x_i, d) := \frac{1}{\hat{N}} \sum_{j=1}^{\hat{N}} \mathrm{B}(b, f(x_i, w_j)) - \mathrm{B}(b, x_i) - c + \delta - \mathcal{K}. \tag{3.12}$$

In $\mathrm{SCP}_{N,\hat{N}}$, $f(x_i, w_j)$ is the next state of the system from the current state x_i with the noise realization w_j. Therefore, the solution of the $\mathrm{SCP}_{N,\hat{N}}$ can be obtained using only the dataset $\mathcal{D}$ without the knowledge of f and $\mathbb{P}_w$. The optimal value for the objective function of $\mathrm{SCP}_{N,\hat{N}}$ is denoted by $\mathcal{K}^*(\mathcal{D})$. We also denote by $\hat{\mathrm{B}}(b, x \,|\, \mathcal{D})$ the barrier function constructed based on the solution of $\mathrm{SCP}_{N,\hat{N}}$ in (3.11).

Note that $\bar{g}_5(x_i, d)$ in (3.12) has an additional parameter $\delta > 0$ compared to g_5. This parameter is added to make the last inequality more conservative in order to capture the error coming from replacing the expectation with the empirical mean. We use Chebyshev's inequality [48] to quantify such an error with the associated confidence. Let us define the variance of the empirical approximation as

$$\sigma^2 := \mathrm{Var}\Big(\frac{1}{\hat{N}}\sum_{j=1}^{\hat{N}} \mathrm{B}(b, f(x, w_j))\Big), \tag{3.13}$$

where the variance is taken with respect to w_j. We assume that there is a bound $\hat{M}$ such that

$$\mathrm{Var}\big(\mathrm{B}(b, f(x, w)\big) \leq \hat{M}, \quad \forall x \in X. \tag{3.14}$$

This assumption gives us a bound for σ^2 in (3.13) as $\sigma^2 \leq \frac{\hat{M}}{\hat{N}}$ due to w_j being independent. The idea of replacing the expectation by the empirical mean in an optimization problem and relating the associated solutions based on Chebyshev's inequality is also used in [99]. Next theorem shows that the barrier certificate computed using the optimal solution of the $\mathrm{SCP}_{N,\hat{N}}$ is a feasible barrier certificate for SCP_N in (3.10) with a certain confidence.

Theorem 4. *Let $\hat{\mathrm{B}}(b, x \,|\, \mathcal{D})$ be a feasible solution of the $SCP_{N,\hat{N}}$ for some $\delta > 0$, and assume the inequality* (3.14) *holds with a given $\hat{M}$.Then for any $\beta_s \in (0, 1]$, we get*

$$\mathbb{P}_w\Big(\hat{\mathrm{B}}(b, x \,|\, \mathcal{D}) \models SCP_N\Big) \geq 1 - \beta_s, \tag{3.15}$$

provided that the number of samples in the empirical mean satisfies $\hat{N} \geq \frac{\hat{M}}{\delta^2\beta_s}$.

Proof. By the statement of the theorem, we have $\hat{\mathrm{B}}(b, x \mid \mathcal{D}) \models \mathrm{SCP}_{N,\hat{N}}$. The difference between the empirical mean in (3.12) and the expected value in (3.10) can be quantified by invoking the Chebyshev's inequality as:

$$\mathbb{P}_w\Big(|\mathbb{E}\big[\mathrm{B}(b, f(x, w)) \,|\, x\big] - \frac{1}{\hat{N}}\sum_{j=1}^{\hat{N}}\mathrm{B}(b, f(x, w_j))| \leq \delta\Big) \geq 1 - \frac{\sigma^2}{\delta^2}, \tag{3.16}$$

where $\delta \in \mathbb{R}^+$, and σ^2 is defined in (3.13) [48]. Since all the first four feasibility conditions are the same as in (3.10) and (3.11), $\hat{\mathrm{B}}(b, x \,|\, \mathcal{D})$ is a feasible solution for those conditions of SCP_N with probability one. The only remaining concern is the last feasibility condition. According to (3.16), one can deduce that $\hat{\mathrm{B}}(b, x \,|\, \mathcal{D})$ is a feasible solution for SCP_N with a confidence of at least $1 - \frac{\sigma^2}{\delta^2}$. Furthermore, we have $\sigma^2 \leq \frac{\hat{M}}{\hat{N}}$ by having $\mathrm{Var}(\mathrm{B}(b, f(x, w))) \leq \hat{M}$, and hence

$$\mathbb{P}_w\big(\hat{\mathrm{B}}(b, x \,|\, \mathcal{D}) \models \mathrm{SCP}_N\big) \geq 1 - \frac{\hat{M}}{\delta^2\hat{N}}.$$

By the above inequality, we get $\beta_s \geq \frac{\hat{M}}{\delta^2\hat{N}}$ and consequently $\hat{N} \geq \frac{\hat{M}}{\delta^2\beta_s}$. This completes the proof. □

Remark 4. *When the system has additive noise,* i.e.,

$$x(t+1) = f_a(x(t)) + w(t),$$

the condition (3.14) *can be established by having a bound on $f_a(\cdot)$ and bounds on moments of the noise w. For instance, in the case of one-dimensional systems (i.e., $n = 1$), we have* $\mathrm{B}(b,x) = \sum_{\iota=0}^{k} b_\iota x^\iota$ *and the variance of* $\mathrm{B}(\cdot)$ *can be expanded as follows:*

$$\begin{aligned}
&Var(\mathrm{B}(b, f(x,w))) = Var\Big(\sum_{\iota=0}^{k} b_\iota f(x,w)^\iota\Big)\\
&= Var\Big(\sum_{\iota=0}^{k} b_\iota (f_a(x)+w)^\iota\Big) = Var\Big(\sum_{\iota}^{k}\sum_{j=0}^{\iota} b_\iota \binom{\iota}{j} f_a(x)^{\iota-j} w^j\Big)\\
&= Var\Big(\sum_{j=1}^{k} \mathrm{g}_j(x) w^j\Big) \ \textit{with}\ \mathrm{g}_j(x) := \sum_{\iota=j}^{k} b_\iota \binom{\iota}{j} f_a(x)^{\iota-j}\\
&= \sum_{j=1}^{k}\sum_{z=1}^{k} \mathrm{g}_j(x)\mathrm{g}_z(x)(\mathbb{E}[w^{j+z}] - \mathbb{E}[w^j]\mathbb{E}[w^z]).
\end{aligned}$$

This means the variance can be bounded using upper bounds of $f_a(\cdot)$ and moments of w.

As it can be seen from Theorem 4, higher number of samples $\hat{N}$ is needed in order to have a smaller empirical approximation error δ, and to provide a better confidence bound. In fact, $\hat{N}$ and δ are required to solve the $\text{SCP}_{N,\hat{N}}$ in (3.11). Later in the next section, we show how the value of β_s affects the total confidence concerning the safety of the stochastic system.

Remark 5. *Note that our results presented in this chapter are valid for any choice of the probability distribution $\mathbb{P}$ with its support being the state set X that satisfies a regularity assumption formulated in the next section (cf. Assumption 5). This assumption holds for a wide range of distributions including uniform, truncated normal, and exponential distributions. From the algorithmic perspective, this distribution affects the collected data points x_i and the optimal solution of the SCP_N. The confidence formulated here is also with respect to this distribution. We choose $\mathbb{P}$ to be a uniform distribution in the case study section.*

3.4 Safety Guarantee over Unknown Stochastic Systems

In the previous section, we established the connection between the two optimizations SCP_N and $\text{SCP}_{N,\hat{N}}$, and showed that the solution of $\text{SCP}_{N,\hat{N}}$ is a feasible solution for SCP_N with a certain confidence if the number of samples $\hat{N}$ is chosen appropriately (cf. Theorem 4). In this section, we focus on the relation between the original RCP and the SCP$_{\scriptscriptstyle N}$ utilizing the fundamental result of [29] and provide an end-to-end safety guarantee over the unknown stochastic system with a priori guaranteed confidence. To do so, we need to raise the following regularity assumptions on the functions and the chosen probability measure $\mathbb{P}$.

Assumption 4. *Functions g_1, g_2, g_3, and g_5 are all Lipschitz continuous with respect to x with Lipschitz constants L_{x_1}, L_{x_2}, L_{x_3}, and L_{x_5}, respectively. Therefore, the Lipschitz constant $\mathrm{L}_x := \mathrm{L}_{x_1}+\mathrm{L}_{x_2}+\mathrm{L}_{x_3}+\mathrm{L}_{x_5}$ is a Lipschitz constant for $\max_z g_z(x,d), z \in \{1,\ldots,5\}\setminus\{4\}$. In addition, if g_1, g_2, g_3, and g_5 are analytic over a compact domain X, the Lipschitz constant of $\max_z g_z(x,d)$ is $\mathrm{L}_x := \max\left\{\mathrm{L}_{x_1},\mathrm{L}_{x_2},\mathrm{L}_{x_3},\mathrm{L}_{x_5}\right\}$.*

Lemma 4. *The maximum of Lipschitz continuous functions $f_i : X \to \mathbb{R}$, $i = 1, 2, \ldots, m$, is a Lipschitz continuous function. The Lipschitz constant of the maximum is the sum of the Lipschitz constants of f_i.*

Proof. Suppose that two Lipschitz continuous functions f_1 and f_2 have Lipschitz constants L_1 and L_2, respectively. One can rewrite $g = \max(f_1, f_2)$ as:

$$g = \max(f_1, f_2) = \frac{f_1 + f_2 + |f_1 - f_2|}{2}.$$

Then, we can use triangle inequality to show that

$$\begin{aligned}|g(x) - g(y)| \leq{}& \frac{1}{2}[|f_1(x) - f_1(y)| + |f_2(x) - f_2(y)|+\\ &\big||f_1(x) - f_2(x)| - |f_1(y) - f_2(y)|\big|]\\ &\leq \frac{1}{2}[L_1\|x - y\| + L_2\|x - y\| + |f_1(x) - f_1(y)|+\\ &|f_2(x) - f_2(y)|] \leq \frac{1}{2}[L_1\|x - y\| + L_2\|x - y\|+\\ &L_1\|x - y\| + L_2\|x - y\|] = (L_1 + L_2)\|x - y\|.\end{aligned}$$

Therefore, $\max(f_1, f_2)$ is also a Lipschitz continuous function with Lipschitz constant $L_1 + L_2$. This argument can be extended inductively to the maximum of every number of functions. □

Lemma 5. *For any two analytic functions $f_1 : X \to \mathbb{R}$ and $f_2 : X \to \mathbb{R}$ with a compact domain X, $L := \max(L_1, L_2)$ is a Lipschitz constant of $\max(f_1, f_2)$.*

Proof. Note that

$$g(x) = \max(f_1(x), f_2(x)) = \begin{cases} f_1(x) & \text{if} \quad f_1(x) - f_2(x) \geq 0\\ f_2(x) & \text{if} \quad f_1(x) - f_2(x) \leq 0.\end{cases}$$

The function $f_1 - f_2$ is also analytic, thus has a finite number of zeros in a compact domain. Let us denote the finite set of zeros as Z. We first show this for one-dimensional compact domains $X \subset \mathbb{R}$. Take two points $x, y \in X$ such that $x < y$, and define $Z \cap [x, y] = \{z_1, z_2, \ldots, z_m\}$ such that $z_i < z_{i+1}$ for any $i = 1, 2, \ldots, m-1$. Then we have

$$|g(y) - g(x)| = |f_{i_y}(y) - f_{i_m}(z_m) + f_{i_m}(z_m) - f_{i_{m-1}}(z_{m-1}) + \ldots \\ + f_{i_2}(z_2) - f_{i_1}(z_1) + f_{i_1}(z_1) - f_{i_x}(x)|,$$

for some appropriate choices of $i_x, i_y, i_1, \ldots, i_m$ all from the set $\{1, 2\}$. Since $g(z_j) = f_1(z_j) - f_2(z_j) = 0$, we can set the index of f to symbol that belongs to the set $\{1, 2\}$ when the function is evaluated at any z_j. Then, we have

$$\begin{aligned}
&|g(y) - g(x)| \\
&= |f_{i_y}(y) - f_{i_y}(z_m) + f_{i_m}(z_m) - f_{i_m}(z_{m-1}) + \ldots + \\
&f_{i_2}(z_2) - f_{i_2}(z_1) + f_{i_x}(z_1) - f_{i_x}(x)| \leq \\
&|f_{i_y}(y) - f_{i_y}(z_m)| + |f_{i_m}(z_m) - f_{i_m}(z_{m-1})| + \ldots + \\
&|f_{i_2}(z_2) - f_{i_2}(z_1)| + |f_{i_x}(z_1) - f_{i_x}(x)| \\
&\leq L_{i_y}(y - z_m) + L_{i_m}(z_m - z_{m-1}) + \ldots + \\
&L_{i_2}(z_2 - z_1) + L_{i_x}(z_1 - x) \leq \\
&L(y - z_m) + L(z_m - z_{m-1}) + \ldots + L(z_2 - z_1) + L(z_1 - x) \\
&= L(y - x),
\end{aligned}$$

where $L = \max(L_1, L_2) = \max(L_{i_y}, L_{i_x}, L_{i_1}, \ldots, L_{i_m})$. This concludes the proof for one-dimensional case.

We now prove the statement for multi-dimensional case. Take two points $x, y \in X \subset \mathbb{R}^n$ with $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$. The functions f_1, f_2 have Lipschitz constants L_1, L_2, which means

$$|f_i(y_1, \ldots, y_n) - f_i(x_1, \ldots, x_n)| \leq L_i \|(y_1 - x_1, \ldots, y_n - x_n)\|, \quad i \in \{1, 2\}. \tag{3.17}$$

Define the line segment that connects these two points as $D := \{\lambda y + (1 - \lambda)x \mid \lambda \in [0, 1]\}$. Let us now restrict the domain of the function g to D and define:

$$h : [0, 1] \to \mathbb{R}, \quad h(\lambda) := g(\lambda y + (1 - \lambda)x) = \\ \max(f_1(\lambda y + (1 - \lambda)x), f_2(\lambda y + (1 - \lambda)x)).$$

We can now apply the first part of the proof to get:

$$|h(1) - h(0)| \leq L'|1 - 0|, \tag{3.18}$$

where L' is the maximum of the Lipschitz constants of $f_1(\lambda y + (1 - \lambda)x)$ and $f_2(\lambda y + (1 - \lambda)x)$ with respect to λ. To get these Lipschitz constants, we use (3.17):

$$\begin{aligned}
&|f_i(\lambda_1 y + (1 - \lambda_1)x) - f_i(\lambda_2 y + (1 - \lambda_2)x)| \leq \\
&L_i \|(\lambda_1 - \lambda_2)(y - x)\| = L_i |\lambda_1 - \lambda_2| \, \|y - x\| \\
&= (L_i \|y - x\|) \, |\lambda_1 - \lambda_2|
\end{aligned}$$

Therefore, the Lipschitz constants of $f_1(\lambda y + (1-\lambda)x)$ for a given x, y with respect to λ is $L_i\|y-x\|$. Leveraging (3.18), we have

$$|g(y) - g(x)| \leq L' = \max(L_1\|y-x\|, L_2\|y-x\|) = \|y-x\| \max(L_1, L_2).$$

This completes the proof. □

Assumption 5. *There is a strictly increasing function $G : \mathbb{R}_0^+ \to [0,1]$, where $G(0) = 0$ such that*

$$\mathbb{P}[\mathrm{b}(x,r)] \geq G(r) \qquad \forall x \in X, \tag{3.19}$$

where $\mathrm{b}(x,r) \subset X$ is an open ball centered at point x with radius r.

Note that any probability distribution, for which the above lower bound function $G(r)$ can be computed, can be used in our approach for sampling.

Remark 6. *The probability distribution from which x_i is sampled must satisfy Assumption 5. This assumption requires having a strictly increasing function $G : \mathbb{R}_0^+ \to [0,1]$ that satisfies*

$$\mathbb{P}[\mathrm{b}(x,r)] \geq G(r), \qquad \forall x \in X.$$

Then, the probability distribution $\mathbb{P}$ should assign positive probability to any ball with positive radius. This means no ball $\mathrm{b}(x,r) \subset X$ could be excluded from sampling in the approach with some non-trivial probability.

Next, we introduce the main result which connects the safety of an unknown stochastic system directly to data collected from the system.

Theorem 5. *Consider an unknown dt-SS, as in (3.1), and safety specification Ψ. Let Assumptions 4 and 5 hold with Lipschitz constant L_x and function $G(r)$, respectively. Assume $\hat{N}$ is selected for the SCP$_{N,\hat{N}}$ as in Theorem 4 in order to provide confidence $1-\beta_s$. Denote by $\mathcal{K}^*(\mathcal{D})$ the optimal value of the optimization problem in (3.11) using N samples and parameter $\rho \in (0,1]$. For any $\beta \in [0,1]$, the following statement holds with a confidence of at least $(1-3\beta-\beta_s)$:*

$$\mathbb{P}_w\big(\mathcal{S} \models_{\mathcal{H}} \Psi\big) \geq 1-\rho,$$

if

$$\mathcal{K}^*(\mathcal{D}) + \mathrm{L}_x\, G^{-1}(\epsilon) \leq 0, \tag{3.20}$$

where function G defined in (3.19), and $\epsilon = \mathrm{I}^{-1}(1-\beta; \mathcal{Q}+3, N-\mathcal{Q}-2)$.

Proof. Denote the optimal values of the RCP and the $\mathrm{SCP}_{\scriptscriptstyle N}$ by $\mathcal{K}^*$ and $\mathcal{K}^*_{\mathsf{m}}(\mathcal{D})$, respectively. According to [29, Theorem 3.6], one has

$$\mathbb{P}\big(\mathcal{K}^*_{\mathsf{m}}(\mathcal{D}) \leq \mathcal{K}^* \leq \mathcal{K}^*_{\mathsf{m}}(\mathcal{D}) + \mathrm{L}_{sp} H(\epsilon)\big) \geq 1-\beta,$$

for a chosen ϵ and any $N \geq N(\epsilon, \beta)$ as in [29, Theorem 2.2]. Equivalently, the above inequality holds for a given N and $\epsilon \leq \mathrm{I}^{-1}(1-\beta; \mathrm{d}, N-\mathrm{d}+1)$. In this expression, d is the number of decision variables, and $H(\cdot)$ is a uniform level-set bound as defied in [29, Definition 3.1]. Constant L_{sp} is a Slater constant as defined in [29, equation (5)]. Since the original RCP in (3.8) is a min-max optimization problem, the constant L_{sp} can be selected as one according to [29, Remark 3.5]. By choosing $\mathrm{d} := \mathcal{Q}+3$, one obtains the parameters of the incomplete beta function in the theorem statement. Based on [29, Proposition 3.8], $H(\epsilon) = \mathrm{L}_x G^{-1}(\epsilon)$, where L_x is the Lipschitz constant of RCP as in Assumption 4, and $G(\cdot)$ as in (3.19). Now, one can readily deduce that

$$\mathbb{P}\big(\mathcal{K}^* \leq \mathcal{K}^*_{\mathsf{m}}(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon)\big) \geq 1-3\beta. \tag{3.21}$$

Confidence β is multiplied by 3 since the Lipschitz continuity is needed in (3.8) in three different regions and, hence, we leverage the results in [69] to deal with this issue by multiplying β by three. On the other hand, due to the particular selection of $\hat{N}$ and β_s according to Theorem 4, we know that (3.15) holds. Therefore,

$$\mathbb{P}\left(\mathcal{K}^*_{\mathsf{m}}(\mathcal{D}) \leq \mathcal{K}^*(\mathcal{D})\right) \geq 1-\beta_s. \tag{3.22}$$

Define the events $\mathcal{A} := \{\mathcal{D} \,|\, \mathcal{K}^* \leq \mathcal{K}^*_{\mathsf{m}}(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon)\}$, $\mathcal{B} := \{\mathcal{D} \,|\, \mathcal{K}^*_{\mathsf{m}}(\mathcal{D}) \leq \mathcal{K}^*(\mathcal{D})\}$, and $\mathcal{C} := \{\mathcal{D} \,|\, \mathcal{K}^*(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon) \leq 0\}$, where $\mathbb{P}(\mathcal{A}) \geq 1-3\beta$ and $\mathbb{P}(\mathcal{B}) \geq 1-\beta_s$. The inequalities in $\mathcal{A}$ and $\mathcal{B}$ satisfy

$$\mathcal{K}^* \leq \mathcal{K}^*_{\mathsf{m}}(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon) \leq \mathcal{K}^*(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon). \tag{3.23}$$

Note that any element $\mathcal{D}$ that belongs to $\mathcal{C}$ will make the right-hand side of (3.23) non-positive. In addition, if this element also belongs to $\mathcal{A} \cap \mathcal{B}$, the two inequalities in (3.23) will also hold, and we get $\mathcal{K}^* \leq 0$.

$$\mathbb{P}(\mathcal{K}^* \leq 0) \geq \mathbb{P}(\mathcal{A} \cap \mathcal{B}) \geq 1 - \mathbb{P}(\mathcal{A}^c) - \mathbb{P}(\mathcal{B}^c) \geq 1-3\beta-\beta_s.$$

This completes the proof since non-positiveness of $\mathcal{K}^*$ ensures a safety lower bound $(1-\rho)$ with confidence of at least $1-3\beta-\beta_s$. □

Corollary 1. *If samples are collected uniformly from a hyper rectangular state set with edges of length $\eta_x(i)$ in each dimension i, then one can compute $G(\epsilon)$ as $\frac{a\epsilon^n}{\prod_{i=1}^n \eta_x(i)}$, where $a = \dfrac{1}{2^n}\frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}$ with the Gamma function defined as $\Gamma(k) = 1 \times 2 \times 3 \ldots \times (k-1)$ and $\Gamma(k+\frac{1}{2}) = \frac{1}{2} \times \frac{3}{2} \times \ldots (k-\frac{3}{2})(k-\frac{1}{2})\pi^{\frac{1}{2}}$ for all positive integers.*

Proof. The probability distribution from which x_i is sampled must satisfy Assumption 5. This assumption requires having a strictly increasing function $G : \mathbb{R}_0^+ \rightarrow [0, 1]$ that satisfies

$$\mathbb{P}[\mathrm{b}(x, r)] \geq G(r), \qquad \forall x \in X.$$

Since we assume that samples are collected uniformly, $\mathbb{P}[\mathrm{b}(x, r)]$ for every small ball centered at every $x \in X$ with radius $r = \epsilon$ can be computed by dividing the volume of this ball by the whole state set volume. Given that one needs to find the maximum ball that is valid for $\forall x \in X$, and some points x lie on the border of the hyper-rectangular state set, the maximum ball is a semi-hypersphere in general, whose volume can be computed as $\dfrac{1}{2^n}\frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}\epsilon^n$ with the Gamma function defined as $\Gamma(k) = 1 \times 2 \times 3 \ldots \times (k-1)$ and $\Gamma(k+\frac{1}{2}) = \frac{1}{2} \times \frac{3}{2} \times \ldots (k-\frac{3}{2})(k-\frac{1}{2})\pi^{\frac{1}{2}}$ for all positive integers. Dividing this value by the whole state set volume, which is $\prod_{i=1}^{n} \eta_x(i)$ for $\eta_x(i)$ as the length of the edges in each direction, gives us $G(\epsilon)$. □

Corollary 2. *If the state set is an n-dimensional hypersphere with radius $\tilde{r}$ and the data is sampled uniformly, then one has*

$$G(\epsilon) = \frac{1}{2}\Big[\mathrm{I}(1 - \frac{c_1^2}{\tilde{r}^2}; \frac{n+1}{2}, \frac{1}{2}) + \frac{\epsilon^n}{\tilde{r}^n}\mathrm{I}(1 - \frac{c_2^2}{\epsilon^2}; \frac{n+1}{2}, \frac{1}{2}\Big],$$

where $c_1 = \frac{2\tilde{r}^2 - \epsilon^2}{2\tilde{r}}$, and $c_2 = \frac{\epsilon^2}{2\tilde{r}}$.

Proof. The proof is similar to the proof of Corollary 1. Here, the centered ball with the maximum volume is the intersection of the whole state set sphere and the small ball $r = \epsilon$ centered at any point on the border of the state set sphere. The volume of this intersection, which is the volume of two separate caps, can be computed as:

$$V_n^{cap}(\tilde{r}, \mathrm{c}_1) + \mathrm{V}_{\mathrm{n}}^{\mathrm{cap}}(\epsilon, \mathrm{c}_2),$$

where

$$V_n^{cap}(\tilde{r}, \mathrm{c}_1) = \frac{1}{2}\frac{\pi^{\frac{\mathrm{n}}{2}}}{\Gamma(\frac{\mathrm{n}}{2}+1)}\tilde{\mathrm{r}}^{\mathrm{n}}\mathrm{I}(1 - \frac{\mathrm{c}_1^2}{\tilde{\mathrm{r}}^2}; \frac{\mathrm{n}+1}{2}, \frac{1}{2}),$$

and

$$V_n^{cap}(\epsilon, \mathrm{c}_2) = \frac{1}{2}\frac{\pi^{\frac{\mathrm{n}}{2}}}{\Gamma(\frac{\mathrm{n}}{2}+1)}\epsilon^{\mathrm{n}}\mathrm{I}(1 - \frac{\mathrm{c}_2^2}{\epsilon^2}; \frac{\mathrm{n}+1}{2}, \frac{1}{2}),$$

for $\mathrm{c}_1 = \frac{2\tilde{\mathrm{r}}^2 - \epsilon^2}{2\tilde{\mathrm{r}}}$, and $\mathrm{c}_2 = \frac{\epsilon^2}{2\tilde{\mathrm{r}}}$. By dividing the intersection volume by the volume of the whole hypersphere state set, which is

$$V_n(\tilde{r}) = \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}\tilde{r}^n,$$

one can compute $G(\epsilon)$ as in Corollary 2. □

Remark 7. *For uniform sampling, the function $G(r)$ is proportional to r^n. Therefore, the sample complexity of the proposed approach is in the order of $(\frac{v\mathrm{L}_x}{\epsilon})^n$, where v is the volume of state set and n is the dimension of the state set.*

Remark 8. *The barrier function constructed based on the finite number of samples according to the above theorem together with the obtained parameters c and λ satisfies the conditions* (3.3)-(3.5) *in Definition 6 with a confidence of at least $1 - 3\beta - \beta_s$.*

Remark 9. *Note that the constraint g_4 in* (3.8) *enforces the constraint $\mathbb{P}(\mathcal{S} \models_{\mathcal{H}} \Psi) \geq 1 - \rho$ for a given ρ. When ρ is not fixed, one can eliminate this constraint from the optimization and guarantee directly the following inequality*

$$\mathbb{P}_w(\mathcal{S} \models_{\mathcal{H}} \Psi) \geq 1 - \frac{1 + c^*\mathcal{H}}{\lambda^*},$$

where c^* and λ^* are the optimal values of the $SCP_{N,\hat{N}}$. This increases the likelihood of getting a feasible optimization and gives the best possible lower bound on the safety probability.

For the sake of clarity, we present the steps required for applying Theorem 5 in Algorithm 2.

Algorithm 2 Safety verification of an unknown dt-SS $\mathcal{S} = (X, V_w, w, f)$ using collected data.

```
Input: Confidence parameters $\beta \in [0, 1]$ and $\beta_s \in [0, 1)$, parameters $\rho \in (0, 1]$, $\delta \in \mathbb{R}^+$, $\hat{M} \in \mathbb{R}^+$, $\mathrm{L}_x \in \mathbb{R}^+$, and the degree of barrier certificate $\mathcal{Q}$
Compute the number of samples $\hat{N} \geq \hat{M}/(\delta^2\beta_s)$ to be used for the empirical average (Theorem 4)
Choose the number of samples $N$
Compute $\epsilon = \mathrm{I}^{-1}(1 - \beta; \mathcal{Q} + 3, N - \mathcal{Q} - 2)$
Select a probability measure $\mathbb{P}$ for the state set $X$
Collect $N\hat{N}$ state pairs from the system
    $\mathcal{D} = \{(x_i, x_{ij}^+) \in X^2,\ x_{ij}^+ = f(x_i, w_{ij})\}_{i,j}$
Solve $\mathrm{SCP}_{N,\hat{N}}$ in (3.11) with $\mathcal{D}$ and obtain the optimal solution $\mathcal{K}^*(\mathcal{D})$
Output: If $\mathcal{K}^*(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon) \leq 0$, then $\mathbb{P}_w(\mathcal{S} \models_{\mathcal{H}} \Psi) \geq 1 - \rho$ with a confidence of at least $1 - 3\beta - \beta_s$.
```

Both Theorem 5 and Algorithm 2 require knowing an upper bound for Lipschitz constant L_x. The following lemma shows how to get this constant for quadratic barrier certificates and systems with additive noises. A similar reasoning can be used for other polynomial-type barrier certificates by casting them as quadratic functions of monomials.

Lemma 6. *Consider a nonlinear system with additive noise*

$$x(t+1) = f_a(x(t)) + w(t), \quad t \in \mathbb{N}_0, \tag{3.24}$$

and a bounded state set X *such that* $||x|| \leq \mathcal{L}$ *for all* $x \in X$*. Without loss of generality, we assume that the mean of noise is zero. Let* $||f_a(x)|| \leq L_1||x|| + L_2$ *and* $||\mathbf{J}_x|| \leq \hat{L}$ *for some* $L_1, L_2, \hat{L} \geq 0, \forall x \in X$*, where* $\mathbf{J}_x$ *is the Jacobian matrix of* $f_a(x)$*. Given a quadratic barrier function* $x^T\mathrm{P}x$ *with a symmetric positive definite matrix* P*, the Lipschitz constant* L_x *can be upper-bounded by*

$$2\|\mathrm{P}\|(L_1\mathcal{L}\hat{L} + L_2\hat{L} + \mathcal{L}).$$

Proof. We first compute the Lipschitz constant of g_5 in (3.5) as

$$L_{x_5} = \max\left\{\left\|\frac{\partial g_5(x)}{\partial x}\right\|, x \in X, \ \|x\| \leq \mathcal{L}\right\},$$

where

$$\begin{aligned}g_5(x) =& \mathbb{E}\big[(f^T(x(t)) + w^T(t))\mathrm{P}(f(x(t)) + w(t))\big]\\ &- x^T(t)\mathrm{P}x(t) - c\\ =& f^T(x(t))\mathrm{P}f(x(t)) - x^T(t)\mathrm{P}x(t) + \mathbb{E}\big[w^T(t)\mathrm{P}w(t)\big] - c.\end{aligned}$$

By considering $\mathbf{J}_x = [\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}]$, one has

$$\begin{aligned}L_{x_5} &= \max_x\|2(f(x(t))^T\mathrm{P}\ \mathbf{J}_x - x^T(t)\mathrm{P})\|\\ &\leq \max_x\ 2\|f(x(t))^T\|\|\mathrm{P}\|\|\mathbf{J}_x\| + 2\|x^T(t)\|\|\mathrm{P}\|\\ &\leq 2(L_1\mathcal{L} + L_2)\|\mathrm{P}\|\hat{L} + 2\mathcal{L}\|\mathrm{P}\|\\ &= 2\|\mathrm{P}\|(L_1\mathcal{L}\hat{L} + L_2\hat{L} + \mathcal{L}).\end{aligned}$$

Similarly, one can readily deduce that $\mathrm{L}_{x_1} = \mathrm{L}_{x_2} = \mathrm{L}_{x_3} = 2\mathcal{L}\|\mathrm{P}\|$, and $\mathrm{L}_{x_4} = 0$. Then $\mathrm{L}_x = \max(\mathrm{L}_{x_1}, \mathrm{L}_{x_2}, \mathrm{L}_{x_3}, \mathrm{L}_{x_4}, \mathrm{L}_{x_5}) = 2\|\mathrm{P}\|(L_1\mathcal{L}\hat{L} + L_2\hat{L} + \mathcal{L})$, which completes the proof. □

Remark 10. *Note that according to the above lemma, computing the upper bound for Lipschitz constant* L_x *depends on* $\|\mathrm{P}\|$*. On the other hand, computing the entries of* P *depends on Lipschitz constant* L_x*. In order to tackle this circulatory issue, we consider an upper bound for* $\|\mathrm{P}\|$ *and enforce it as an additional constraint while solving the SCP in* (3.11)*. If there is no solution with the selected upper bound, we iteratively increase the upper bound until we find a solution or a predefined maximum number of iterations is reached.*

Remark 11. *If the underlying dynamics is affine in the form of* $x(t+1) = Ax(t) + B + w(t)$ *with* $A \in \mathbb{R}^{n\times n}$ *and* $B \in \mathbb{R}^{n\times 1}$*, we can set* $L_1 = \hat{L}$ *as an upper bound on* $||A||$ *and* L_2 *as an upper bound on* $\|B\|$*.*

Remark 12. *The Lipschitz constant in Assumption 4 can also be estimated directly from the data using Extreme Value Theory with the estimation approach described in [109]. For instance, to estimate the Lipschitz constant of g_5 in* (3.9)*, we collect data*

$$\Big\{(x_{i1}, x_{i2}) \,|\, i_1, i_2 = 1, \ldots, \tilde{N}\Big\}$$

and compute

$$\hat{\mathrm{L}} = \max \frac{\|g_5(x_{i_1}) - g_5(x_{i_2})\|}{\|x_{i_1} - x_{i_2}\|}, \qquad i_1, i_2 \in \{1, \ldots, \tilde{N}\}. \tag{3.25}$$

The Lipschitz constant of g_5 is computed by fitting a Reverse Weibull distribution to the samples of the random variable $\hat{\mathrm{L}}$, and then computing the location parameter of that distribution.

3.5 Data-Driven Controller Synthesis

In this section, we study the problem of synthesizing a controller for an unknown stochastic control system using data to satisfy safety specifications. Our approach is to use *control barrier certificates*, fix a parameterized set of controllers, and design the parameters using an SCP. The stochastic control system is defined next.

Definition 7. *A discrete-time stochastic control system (dt-SCS) is a tuple $\mathcal{S} = (X, U, V_w, w, f)$, where X, V_w, w are as in Definition 4, $U \subset \mathbb{R}^m$ is the input set, and $f : X \times U \times V_w \rightarrow X$ is the state transition map. The evolution of the state is according to equation*

$$\mathcal{S} : x(t+1) = f(x(t), u(t), w(t)),\ t \in \mathbb{N}_0. \tag{3.26}$$

We assume that the map f and distribution of w is unknown but we can gather data (x_i, u_i, x_i^+) by initializing the system at x_i, applying the input u_i, and observing the next state of the system $x_i^+ = x_i(t+1)$. The collected dataset is

$$\mathcal{D} := \Big\{(x_i, u_i, f(x_i, u_i, w_j))\Big\}_{i,j} \subset X \times U \times X. \tag{3.27}$$

Now, we state the main problem we are interested to solve here.

Problem 4. *Consider an unknown dt-SCS $\mathcal{S}$ as in Definition 7, with a safety specification Ψ specified by the initial set X_{in}, unsafe set X_u, and time horizon $\mathcal{H}$. Using a dataset $\mathcal{D}$ of the form* (3.27)*, find a controller* $\mathrm{k} : X \rightarrow U$ *together with a constant* $\rho \in [0, 1)$ *and confidence* $(1 - \beta) \in [0, 1]$ *such that $\mathcal{S}$ under this controller satisfies Ψ with a probability of at least* $(1 - \rho)$, i.e.,

$$\mathbb{P}_w^{\mathrm{k}}\big(\mathcal{S} \models_{\mathcal{H}} \Psi\big) \geq 1 - \rho, \quad \forall x(0) \in X_{in},$$

with a confidence $1 - \beta$. Moreover, establish a connection between the required size of $\mathcal{D}$ and the confidence $1 - \beta$.

Similar to the verification problem discussed in the previous sections, we use the notion of control barrier certificates with a parameterized set of controllers [51] to get a characterization of the controller together with the lower bound on the safety probability.

Definition 8. *Given a dt-SCS $\mathcal{S} = (X, U, V_w, w, f)$ with $U \subset \mathbb{R}^m$, initial set $X_{in} \subset X$, and unsafe set $X_u \subset X$, a function $\mathrm{B} : X \to \mathbb{R}_0^+$ is called a control barrier certificate (CBC) for $\mathcal{S}$ if there exist constants $\lambda > 1$, $c \geq 0$, and functions $\mathscr{P}_\ell(x) : X \to \mathbb{R}_0^+$, $\ell \in \{1, 2, \ldots, m\}$, such that constraints in* (3.3) *and* (3.4) *hold, and*

$$\mathbb{E}\Big[\mathrm{B}(f(x,u,w)) \mid x, u\Big] + \sum_{\ell=1}^{m}(u_\ell - \mathscr{P}_\ell(x)) \leq \mathrm{B}(x) + c$$
$$\forall x \in X,\ \forall u = [u_1; \ldots; u_m] \in U. \tag{3.28}$$

Theorem 6. *A CBC $\mathrm{B}(x)$ as in Definition 8 guarantees that*

$$\mathbb{P}_w^{\mathrm{k}}\big(\mathcal{S} \models_{\mathcal{H}} \Psi\big) \geq 1 - \rho, \quad \forall x(0) \in X_{in},$$

under the controller $\mathrm{k}(x) = [\mathscr{P}_1(x); \mathscr{P}_2(x); \ldots; \mathscr{P}_m(x)]$, where $\rho = (1 + c\mathcal{H})/\lambda$ with $\mathcal{H}$ being the time horizon of the safety specification.

Let us consider polynomial-type CBC and controllers. The number of CBC coefficients is denoted by $\mathcal{Q}$. Polynomial $\mathscr{P}_\ell$ has the following form for some $k' \in \mathbb{N}_0$:

$$\mathscr{P}_\ell(p^\ell, x) = \sum_{\iota_1=0}^{k'} \cdots \sum_{\iota_n=0}^{k'} p^\ell_{\iota_1,\ldots,\iota_n}(x_1^{\iota_1} \ldots x_n^{\iota_n}), \tag{3.29}$$

with $p^\ell_{\iota_1,\ldots,\iota_n} = 0$ for $\iota_1 + \ldots + \iota_n > k'$.

The overall number of all coefficients of m polynomials $\mathscr{P}_\ell(p^\ell, x)$ is denoted by $\mathcal{P}$. We also assume that the input set U is a polytope of the form

$$U = \{u \in \mathbb{R}^m \,|\, \mathcal{A}u \leq \mathsf{b}\}, \tag{3.30}$$

for some $\mathcal{A} \in \mathbb{R}^{q \times m}$ and $\mathsf{b} \in \mathbb{R}^{q \times 1}$.

Under these assumptions, the inequalities in Definition 8 and Theorem 6 can be written as an RCP:

$$\text{RCP}: \begin{cases} \min\limits_{d} & \mathcal{K} \\ \text{s.t.} & \max_z \ \ g_z(x,u,d) \leq 0, \\ & z \in \{1, 2, \ldots, 5+q\}, \forall x \in X, \forall u \in U, \\ & d = [\mathcal{K}; \lambda; c; b_{\iota_1,\ldots,\iota_n}; p^\ell_{\iota_1,\ldots,\iota_n}], \\ & \mathcal{K} \in \mathbb{R},\ \lambda > 1,\ c \geq 0, \end{cases} \tag{3.31}$$

where $g_z(x,d), z \in \{1,\ldots,4\}$, are the same as (3.9), and

$$\begin{aligned}&g_5(x,u,d) = \mathbb{E}\Big[\mathrm{B}(b, f(x,u,w)) \mid x,u\Big] + \sum_{\ell=1}^{m}(u_\ell - \mathscr{P}_\ell(p^\ell, x))\\ &- \mathrm{B}(b,x) - c - \mathcal{K},\\ &[g_6(x,d);\ldots;g_{5+q}(x,d)] = \mathcal{A}\,[\mathscr{P}_1(p^1,x);\ldots;\mathscr{P}_m(p^m,x)] -\\ &\mathsf{b} - \mathcal{K}\mathbf{1}_{q\times 1}.\end{aligned} \tag{3.32}$$

Note that the last inequality in (3.32) encodes the fact that the control input should be inside the set U specified by the polytope (3.30).

The constraints in the RCP is always feasible. A solution can be constructed as follows. Set the coefficients of $\mathrm{B}(b,x)$ and $\mathscr{P}_\ell(p^\ell,x)$ equal to zero, $c = 0$, $\lambda = 2$, and $u_\ell = \mathscr{P}_\ell(p^\ell,x)\ \forall \ell \in \{1,\ldots,m\}$. Also select $\mathcal{K}$ large enough such that $\mathcal{K} \geq \frac{1}{\rho} - 2$ together with $\mathcal{K}\ \mathbf{1}_{m\times 1} \geq -\mathsf{b}$.

The RCP in (3.31) is in general hard to solve since the map f and the probability measure $\mathbb{P}_w$ are unknown. Hence, similar to the verification approach discussed in Section 3.3, we assign a probability distribution to both state and input sets, and collect N i.i.d pairs (x_i, u_i) from this assigned distribution, and replace the robust quantifiers $\forall x \in X$ and $\forall u \in U$ with $\forall x_i \in X$ and $\forall u_i \in U, i \in \{1,\ldots,N\}$, respectively. This results in a scenario convex program called SCP_{N}, which is not presented here for the sake of brevity.

To address the issue of unknown f and $\mathbb{P}_w$, the expectation in g_5 is replaced with its empirical approximation by sampling $\hat{N}$ i.i.d. values $w_j,\ j \in \{1,\ldots,\hat{N}\}$, from $\mathbb{P}_w$ for each pair of (x_i,u_i), which results in the following scenario convex program denoted by $\mathrm{SCP}_{N,\hat{N}}$:

$$\mathrm{SCP}_{N,\hat{N}}: \begin{cases} \min\limits_{d} & \mathcal{K}\\ \text{s.t.} & \max_z\ \bar{g}_z(x_i,u_i,d) \leq 0,\\ & z \in \{1,2,\ldots,5+q\},\\ & \forall x_i \in X,\ \forall u_i \in U, \forall i \in \{1,\ldots,N\},\\ & d = [\mathcal{K};\lambda;c;b_{\iota_1,\ldots,\iota_n};p^\ell_{\iota_1,\ldots,\iota_n}],\\ & \mathcal{K} \in \mathbb{R},\ \lambda > 1,\ c \geq 0,\end{cases} \tag{3.33}$$

where $\bar{g}_z := g_z$ for all $z \in \{1,2,\ldots,5+q\} \setminus \{5\}$, and

$$\begin{aligned}&\bar{g}_5(x_i,u_i,d) = \frac{1}{\hat{N}}\sum_{j=1}^{\hat{N}} \mathrm{B}(b, f(x_i,u_i,w_j)) +\\ &\sum_{\ell=1}^{m}(u_{i_\ell} - \mathscr{P}_\ell(p^\ell, x_i)) - \mathrm{B}(b,x_i) - c + \delta - \mathcal{K}.\end{aligned} \tag{3.34}$$

Using empirical approximation introduces an error which is demonstrated by δ in the above optimization problem. We denote by $\hat{\mathrm{B}}_u(b,x\,|\,\mathcal{D})$ the constructed control barrier certificate with coefficients computed by solving the $\mathrm{SCP}_{N,\hat{N}}$.

Remark 13. *Similar to Theorem 4, under the assumption*

$$Var\big(\mathrm{B}(b, f(x,u,w))\big) \leq \hat{M},$$

for some $\hat{M} > 0$, a desired confidence $\beta_s \in (0,1]$, and an error δ, one has

$$\mathbb{P}_w^{\mathrm{k}}\Big(\hat{\mathrm{B}}_u(b, x \mid \mathcal{D}) \models SCP_{\scriptscriptstyle N}\Big) \geq 1 - \beta_s, \tag{3.35}$$

provided that $\hat{N} \geq \frac{\hat{M}}{\delta^2 \beta_s}$.

To provide the main results here, we need the following assumptions.

Assumption 6. *Function g_5 is Lipschitz continuous with respect to (x,u) with Lipschitz constant L_5. Functions $g_1, g_2, g_3, g_6, \ldots, g_{5+q}$ are also Lipschitz continuous with respect to x with Lipschitz constants $\mathrm{L}_1, \mathrm{L}_2, \mathrm{L}_3, \mathrm{L}_6, \ldots, \mathrm{L}_{5+q}$, respectively. Then, the Lipshitz constat of maximum of these function is $\mathrm{L}_1 + \mathrm{L}_2 + \mathrm{L}_3 + \mathrm{L}_5 + \mathrm{L}_6 + \ldots + \mathrm{L}_{5+q}$. Furthermore, if all functions g are analytic over a compact domain $X \times U$, the Lipschitz constant of their maximum is $\max(\mathrm{L}_1, \mathrm{L}_2, \mathrm{L}_3, \mathrm{L}_5, \mathrm{L}_6, \ldots, \mathrm{L}_{5+q})$, which we denote it by $\mathrm{L}_{x,u}$.*

Assumption 7. *There is a strictly increasing function $G(r) : \mathbb{R}^+ \rightarrow [0,1]$ such that*

$$\mathbb{P}[\mathrm{b}(x,u,r)] \geq G(r) \qquad \forall (x,u) \in X \times U, \tag{3.36}$$

where $\mathrm{b}(x,u,r)$ is an open ball in the product space $X \times U$ centered at the point (x,u) with radius r.

Now, we have all the ingredients to propose the main results here.

Theorem 7. *Consider an unknown dt-SCS as in Definition 7 and a safety specification Ψ. Let Assumptions 6–7 hold with constant $\mathrm{L}_{x,u}$ and function $G(r)$. Suppose that $\mathcal{K}^*(\mathcal{D})$ is the optimal value of $SCP_{\scriptscriptstyle N,\hat{N}}$ in (3.33) with number of samples N, a given $\rho \in (0,1]$, and for $\hat{N}$ selected based on Remark (13) with confidence of $1 - \beta_s$. Suppose*

$$\mathcal{K}^*(\mathcal{D}) + \mathrm{L}_{x,u} G^{-1}(\epsilon) \leq 0, \tag{3.37}$$

where function G is defined in (3.36) and $\epsilon = \mathrm{I}^{-1}(1 - \beta; \mathcal{Q} + \ \mathcal{P} + 3, N - \mathcal{Q} - \mathcal{P} - 2)$ with confidence parameter $\beta \in [0,1]$, and $\mathcal{Q}$ and $\mathcal{P}$ being respectively the number of coefficients of the polynomial control barrier certificate and the overall number of coefficients of polynomials $\mathscr{P}_\ell(p^\ell, x)$ for m inputs. Then, the following statement is valid with a confidence of at least $1 - 3\beta - \beta_s$: the system $\mathcal{S}$ together with the constructed control input

$$\mathrm{k}(x) := [\mathscr{P}_1(p^1, x); \ldots; \mathscr{P}_m(p^m, x)],$$

for which coefficients $p^\ell, \ell \in \{1, \ldots, m\}$, are obtained from the solution of $SCP_{\scriptscriptstyle N,\hat{N}}$, is safe within the time horizon $\mathcal{H}$ with a probability of at least $1 - \rho$, i.e.,

$$\mathbb{P}_w^{\mathrm{k}}\big(\mathcal{S} \models_{\mathcal{H}} \Psi\big) \geq 1 - \rho. \tag{3.38}$$

Proof. The proof is similar to the proof of Theorem 5 by replacing $\mathbb{P}_w$ with $\mathbb{P}_w^{\mathrm{k}}$ for the RCP (3.31) and its associated SCPs. The function $G(\epsilon)$ is defined as in (3.36). The number of coefficients is $\mathcal{Q}+\mathcal{P}+3$ where $\mathcal{P}$ is the overall number of coefficients of m polynomials defining the controller, which results in the new arguments of the regularized incomplete beta function I in the theorem statement. □

Corollary 3. *If samples are collected uniformly from a hyper rectangular sets X and U, respectively, with edges of length $\eta_x(i)$ and $\eta_u(j)$ in each dimension i and j, then one can compute $G(\epsilon)$ as $\frac{a\epsilon^{n+m}}{\prod_{i=1}^{n}\eta_x(i)\prod_{j=1}^{m}\eta_u(j)}$, where $a=\frac{1}{2^{n+m}}\frac{\pi^{\frac{n+m}{2}}}{\Gamma(\frac{n+m}{2}+1)}$ with Gamma function defined in Corollary 1.*

Proof. The proof is similar to the proof of Corollary 1 based on the new definition of $G(r)$ in Assumption 7. □

Remark 14. *When ρ is not fixed, one can eliminate constraint g_4 from* (3.31) *and directly provide the following inequality*

$$\mathbb{P}_w^{\mathrm{k}}(\mathcal{S}\models_{\mathcal{H}}\Psi)\geq 1-\frac{1+c^*\mathcal{H}}{\lambda^*},$$

in which c^* and λ^* are the optimal solutions of $SCP_{N,\hat{N}}$ in (3.33). *This increases the likelihood of getting a feasible solution and gives the best possible lower bound on the safety probability for $\mathcal{S}$. A schematic overview of our synthesis approach is presented in Fig. 3.3.*

Algorithm 3 Data-driven synthesis for safety specification on an unknown dt-SCS $\mathcal{S}=(X,U,V_w,w,f)$.

```
Input: Confidence parameters $\beta \in [0,1]$, $\beta_s \in (0,1]$, parameters $\rho \in (0,1]$, $\delta \in \mathbb{R}^+$, $\hat{M} \in \mathbb{R}^+$, $\mathrm{L}_{x,u} \in \mathbb{R}^+$, degree of the barrier certificate $\mathcal{Q}$, and degree of the polynomial functions for the controller $\mathcal{P}$
Compute the number of samples $\hat{N} \geq \hat{M}/(\delta^2\beta_s)$ for the empirical average (Remark 13)
Choose the number of samples $N$
Compute $\epsilon = \mathrm{I}^{-1}(1-\beta; \mathcal{Q}+ \ \mathcal{P}+3, N-\mathcal{Q}-\mathcal{P}-2)$
Select a probability measure $\mathbb{P}$ for the state-input set $(X,U)$
Collect $N\hat{N}$ tuples from the system $\mathcal{D} := \{(x_i,u_i,x'_{ij}) \in X \times U \times X,\ x'_{ij} = f(x_i,u_i,w_{ij})\}_{i,j}$
Solve $\mathrm{SCP}_{N,\hat{N}}$ in (3.33) with $\mathcal{D}$ and obtain the optimal solution $\mathcal{K}^*(\mathcal{D})$
Output: If $\mathcal{K}^*(\mathcal{D}) + \mathrm{L}_{x,u}G^{-1}(\epsilon) \leq 0$, then $\mathbb{P}_w^{\mathrm{k}}(\mathcal{S} \models_{\mathcal{H}} \Psi) \geq 1-\rho$ with a confidence of at least $1-3\beta-\beta_s$ and with the controller $\mathrm{k}(x) := [\mathscr{P}_1(p^1,x);\ldots;\mathscr{P}_m(p^m,x)]$.
```

Next lemma provides an upper bound for Lipschitz constant $\mathrm{L}_{x,u}$, which is required in Theorem 7, in the case that the system is affected by an additive noise.

Lemma 7. *Consider a nonlinear dt-SCS as in Definition 7 which is affected by an additive noise as the following:*

$$x(t+1)=f_a(x(t),u(t))+w(t), \tag{3.39}$$

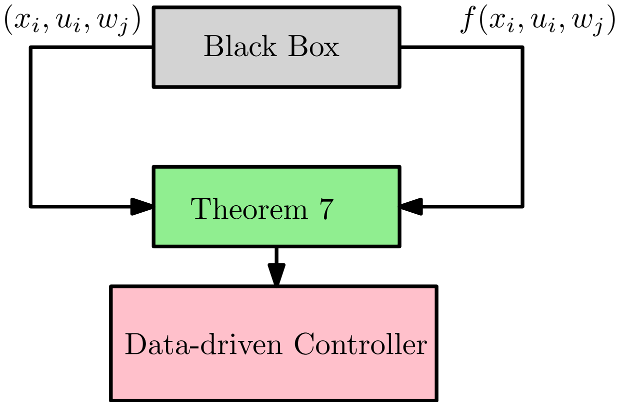


Figure 3.3: A schematic overview of the data-driven synthesis presented in Section 3.5.

and a bounded state set X and input set U such that $\|x\| \leq \mathcal{L}_x$ for all $x \in X$, and $\|u\| \leq \mathcal{L}_u$ for all $u \in U$. Without loss of generality, we assume that the mean of the noise is zero. Let $\|f_a(x,u)\| \leq L_1\|x\| + L_2\|u\| + L_3$, $||\mathbf{J}_x|| \leq \hat{L}_x$, and $||\mathbf{J}_u|| \leq \hat{L}_u$, for some $\mathcal{L}_x, \mathcal{L}_u, L_1, L_2, L_3, \hat{L}_x, \hat{L}_u \geq 0$, where $\mathbf{J}_x$ and $\mathbf{J}_u$ are Jacobian matrices of $f_a(x,u)$ with respect to x and u, respectively. Given a quadratic barrier function $x^T\mathrm{P}x$, and a set of quadratic functions $x^T\mathrm{P}_\ell x$, $\ell \in \{1,\ldots,m\}$, representing each of $\mathscr{P}_\ell(p^\ell, x)$ with symmetric matrices P and P_ℓ, the Lipschitz constant $\mathrm{L}_{x,u}$ can be upper-bounded by $\sqrt{\mathscr{L}_x^2 + \mathscr{L}_u^2}$, where

$$\begin{aligned}\mathscr{L}_x &= 2\mathcal{L}_x L_1 \hat{L}_x\|\mathrm{P}\| + 2\mathcal{L}_u L_2 \hat{L}_x\|\mathrm{P}\| + 2L_3\hat{L}_x\|\mathrm{P}\| \\ &\quad + \mathcal{L}_x\|\mathrm{P}\| + \mathcal{L}_x\sum_{\ell=1}^{m}\|\mathrm{P}_\ell\|, \\ \mathscr{L}_u &= 2\mathcal{L}_x L_1\hat{L}_u\ \|\mathrm{P}\| + 2\mathcal{L}_u L_2\hat{L}_u\ \|\mathrm{P}\| + 2L_3\hat{L}_u\ \|\mathrm{P}\| + \sqrt{m}.\end{aligned} \tag{3.40}$$

Proof. We first compute the Lipschitz constant regarding $g_5(x,u,d)$ in (3.32), where

$$\begin{aligned}g_5(x,u,d) = \ &\mathbb{E}\big[(f^T(x(t),u(t)) + w^T(t))\mathrm{P}(f(x(t),u(t)) + \\ &w(t))\big] + \sum_{\ell=1}^{m}(u_\ell - \mathscr{P}_\ell(p^\ell,x)) - x^T(t)\mathrm{P}x(t) - c.\end{aligned}$$

Considering $\mathbb{E}[w(t)] = 0$, we compute the upper bounds for Lipschitz constant with respect to x and u separately denoted by L_{5_x} and L_{5_u}, respectively. We define $\mathbf{J}_x = [\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}]$

and $\mathbf{J}_u = [\frac{\partial f}{\partial u_1}, \dots, \frac{\partial f}{\partial u_m}]$ as Jacobian matrices with respect to x and u, respectively.

$$\begin{aligned}
\mathrm{L}_{5_x} =& \max_{x,u} \| \frac{\partial g_5(x,u,d)}{\partial x} \| = \max_{x,u} \| 2(f(x(t),u(t))^T \mathrm{P}\ \mathbf{J}_x \\
&- x^T(t)\mathrm{P} - x^T(t) \sum_{\ell=1}^{m} \mathrm{P}_\ell \| \\
\leq & 2\mathcal{L}_x L_1 \hat{L}_x \|\mathrm{P}\| + 2\mathcal{L}_u L_2 \hat{L}_x \|\mathrm{P}\| + 2L_3 \hat{L}_x \|\mathrm{P}\| + \\
& \mathcal{L}_x \|\mathrm{P}\| + \mathcal{L}_x \sum_{\ell=1}^{m} \|\mathrm{P}_\ell\|,
\end{aligned}$$

and accordingly,

$$\begin{aligned}
\mathrm{L}_{5_u} &= \max_{x,u} \| \frac{\partial g_5(x,u,d)}{\partial u} \| \\
&= \| 2(f(x(t),u(t))^T \mathrm{P} \mathbf{J}_u + \mathbf{1}_m \| \\
&\leq 2\mathcal{L}_x L_1 \hat{L}_u \ \|\mathrm{P}\| + 2\mathcal{L}_u L_2 \hat{L}_u \ \|\mathrm{P}\| + 2L_3 \hat{L}_u \ \|\mathrm{P}\| + \sqrt{m}.
\end{aligned}$$

Now it can be deduced that

$$\mathrm{L}_5 \leq \sqrt{\mathrm{L}_{5_x}^2 + \mathrm{L}_{5_u}^2}.$$

Similar to the proof of Lemma 6, it is straightforward to compute the upper bounds of Lipschitz constants for other constraints in (3.32) and show that the computed upper bound is greater than all of them. We ignore this part for the sake of brevity. Then, $\mathrm{L}_{x,u} \leq \max\big(\mathrm{L}_i, i \in \{1, 2, \dots, 5{+}q\} \backslash \{4\}\big) = \sqrt{\mathrm{L}_{5_x}^2 + \mathrm{L}_{5_u}^2}$ which is equivalent to $\sqrt{\mathscr{L}_x^2 + \mathscr{L}_u^2}$ with $\mathscr{L}_x$ and $\mathscr{L}_u$ as in (3.40). □

Note that one can use similar results as in Remark 12 to estimate the Lipschitz constant via data.

3.6 Data-driven Barrier Certificates for Non-convex Setting

In this section, we extend the proposed result in Section 3.4 to a case of having non-convex constraints. We modify the constraint (3.5) in Definition 6 as follows:

$$\mathbb{E}\Big[\mathrm{B}(f(x,w)) \mid x\Big] \leq \ \kappa\, \mathrm{B}(x) + c, \quad \forall x \in X, \tag{3.41}$$

where $\kappa \in (0,1)$.

According to the fundamental results in [59], choosing κ in the interval $(0,1)$ provides a better lower bound for the probability of safety satisfaction in (3.6), namely:

$$\mathbb{P}_w\big(\mathcal{S} \models_{\mathcal{H}} \Psi\big) \geq 1 - \rho,$$

with

$$\rho = \begin{cases} 1-(1-\frac{1}{\lambda})(1-\frac{c}{\lambda}) & \text{if } \lambda \geq \frac{c}{\kappa} \\ \frac{1}{\lambda}(1-\kappa)^{\mathcal{H}} + \frac{c}{\kappa\lambda}\big(1-(1-\kappa)^{\mathcal{H}}\big) & \text{if } \lambda < \frac{c}{\kappa}, \end{cases} \tag{3.42}$$

where parameters c, λ, and $\mathcal{H}$ are the same as in Definition (6). Another advantage of choosing κ in the interval $(0,1)$ is that this new formulation can be utilized in the context of compositionality and interconnected systems [113, 102].

Replacing the last condition of RCP in (3.9) with the modified constraint in (3.41) leads to the following optimization problem which is not convex anymore:

$$\text{RP}: \begin{cases} \min\limits_{d} \quad \mathcal{K} \\ \text{s.t.} \quad \max_z \big(g_z(x,d)\big) \leq 0, \forall z \in \{1,2,3,4\}, \forall x \in X, \\ \qquad\; d = [\mathcal{K}; \lambda; c; b_{\iota_1,\ldots,\iota_n}; \kappa], \\ \qquad\; \mathcal{K} \in \mathbb{R},\ \lambda > 1,\ c \geq 0,\ \kappa \in (0,1), \end{cases} \tag{3.43}$$

in which $g_z(x,d), z \in \{1,2,3\}$, are the same as in (3.9), and

$$g_4(x,d) = \mathbb{E}\Big[\mathrm{B}(f(x,w)) \mid x\Big] \leq\ \kappa\,\mathrm{B}(x) + c, \quad \forall x \in X. \tag{3.44}$$

The non-convexity comes from the multiplication of κ and coefficients of barrier function $\mathrm{B}(b, x_i)$ in (3.41). With the same reasoning in Section (3.3), solving the above RP is not straightforward generally. Therefore, we construct an SP by taking samples and then connect the solution of the obtained scenario programming to the safety of the stochastic system in (3.1). By collecting i.i.d. samples $x_i,\ i \in \{1,\ldots,N\}$, from an assigned probability distribution over the state set, and approximating the expectation term in (3.41) results in a non-convex programming as the following:

$$\text{SP}_{N,\hat{N}}: \begin{cases} \min\limits_{d} \quad \mathcal{K} \\ \text{s.t.} \quad \max_z \bar{g}_z(x_i,d) \leq 0,\ \forall i \in \{1,\ldots,N\}, \\ \qquad\qquad \forall z \in \{1,2,3,4\}, \\ \qquad\; d = [\mathcal{K}; \lambda; c; b_{\iota_1,\ldots,\iota_n}; \kappa], \\ \qquad\; \mathcal{K} \in \mathbb{R},\ \lambda > 1,\ c \geq 0,\ \kappa \in (0,1), \end{cases} \tag{3.45}$$

where $\bar{g}_z := g_z$ for all $z \in \{1,2,3\}$ and

$$\bar{g}_4(x_i,d) = \frac{1}{\hat{N}} \sum_{j=1}^{\hat{N}} \mathrm{B}(b, f(x_i,w_j)) -\ \kappa\,\mathrm{B}(b,x_i) - c + \delta - \mathcal{K}. \tag{3.46}$$

Note that in this new scenario programming, we eliminated the constraint that forces a fixed probability lower bound $1-\rho$ on the safety of the stochastic system, namely, g_4 in (3.9). Instead, we are interested in providing the tightest possible lower bound of the safety probability according to Remark 9. The main issue underlying here is that by considering

$\kappa \in (0,1)$, the obtained scenario program is not convex anymore, and accordingly, one cannot naively utilize the results proposed in Theorems 5. Hence, one cannot solve the SP in (3.45) by simply applying bisection over κ, while still utilizing the proposed results in the previous sections.

Now we state the main problem we aim to address in this section.

Problem 5. *Consider an unknown dt-SS $\mathcal{S}$ as in Definition 4. Compute the largest lower bound* $(1-\rho) \in [0,1]$ *on the probability of satisfying* Ψ, i.e.,

$$\mathbb{P}_w\big(\mathcal{S} \models_{\mathcal{H}} \Psi\big) \geq 1-\rho,$$

according to (3.42) *together with a confidence* $(1-\beta) \in [0,1]$ *using a dataset $\mathcal{D}$ of the form* (3.2)*. Moreover, establish a connection between the required size of dataset $\mathcal{D}$, the cardinality of the set from which the parameter κ is selected, and the desired confidence $1-\beta$.*

In the next theorem, we present our solution to Problem 5 by proposing a new confidence bound which is always valid even for the non-convex scenario program in (3.45).

Theorem 8. *Consider an unknown dt-SS as in* (3.1) *together with the safety specification Ψ. Let* M *be the cardinality of a finite set from which κ takes value in (0,1). Suppose that Assumptions 4-5 hold for the RP in* (3.43) *with function $G(\cdot)$ and* $\mathrm{L}_x := \max\big(\mathrm{L}_{x_1}, \mathrm{L}_{x_2}, \mathrm{L}_{x_3}, \mathrm{L}_{x_4}\big)$*, where* $\mathrm{L}_{x_i}, i \in \{1,\dots,4\}$*, is an upper bound on the Lipschitz constant of the i^{th} constraint in* (3.43)*. Assume $\hat{N}$ is selected for the SP$_{N,\hat{N}}$ similar to Theorem 4 in order to provide confidence $1-\beta_s$. Suppose $\mathcal{K}^*(\mathcal{D})$ is the optimal value of the optimization problem in* (3.45) *using $\hat{N}$ and N. Furthermore,* $\epsilon = \mathrm{I}^{-1}(1-\mathrm{M}\beta; \mathcal{Q}+3, N-\mathcal{Q}-2)$ *for* $\beta \in [0,1]$*, where $\mathcal{Q}$ is the number of coefficients of the barrier certificate. Then the following statement holds with a confidence of at least $1-3\beta-\beta_s$: if $\mathcal{K}^*(\mathcal{D})+\mathrm{L}_x G^{-1}(\epsilon) \leq 0$, then*

$$\mathbb{P}_w(\mathcal{S} \models_{\mathcal{H}} \Psi) \geq 1-\rho^*, \tag{3.47}$$

where ρ^* is computed as in (3.42) *using optimal solutions of SP$_{N,\hat{N}}$, namely, c^*, λ^*, and κ^*. More importantly, with a confidence of at least $1-3\beta-\beta_s$,* $\mathrm{B}(b^*, x)$ *is a barrier certificate for S, satisfying* (3.3), (3.4), *and* (3.41)*, where b^* is the optimal solution of SP$_{N,\hat{N}}$.*

Proof. Denote the optimal values of the RP and its equivalent scenario programming before the empirical approximation of the expectation term in g_4, namely, SP$_N$, by $\mathcal{K}^*$ and $\mathcal{K}^*_{\mathsf{m}}(\mathcal{D})$, respectively. Similar to (3.21), one has

$$\mathbb{P}\big(\mathcal{K}^* \leq \mathcal{K}^*_{\mathsf{m}}(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon)\big) \geq 1-3\beta,$$

for any $N \geq \tilde{N}\big(\epsilon_1,\dots,\epsilon_{\mathrm{M}},\beta\big)$, where

$$\tilde{N}\big(\epsilon_1,\dots,\epsilon_{\mathrm{M}},\beta\big) := \\ \min\Big\{N \in \mathbb{N} \mid \sum_{z=1}^{\mathrm{M}} \sum_{i=0}^{\mathrm{d}-1} \binom{N}{i} \epsilon_z^{\,i}(1-\epsilon_z)^{N-i} \leq \beta\Big\}.$$

Alternatively, one can set $\epsilon := \epsilon_1 = \epsilon_2 = \ldots = \epsilon_{\mathrm{M}}$ in the above expression to get the inequality $\epsilon \leq \mathrm{I}^{-1}(1-\mathrm{M}\beta; \mathrm{d}, N-\mathrm{d}+1)$, where M is the cardinality of the set from which κ is selected, and d is the number of decision variables. By choosing $\mathrm{d} := \mathcal{Q}+3$, one gets the parameters of the incomplete beta function in the theorem statement. On the other hand, due to the particular selection of $\hat{N}$ and β_s similar to Theorem 4, it can be deduced that

$$\mathbb{P}_w\Big(\hat{\mathrm{B}}(b, x \,|\, \mathcal{D}) \models \mathrm{SP}_{\scriptscriptstyle N}\Big) \geq 1-\beta_s,$$

where $\hat{\mathrm{B}}(b, x \,|\, \mathcal{D})$ is the barrier function whose coefficients are the optimal solution of $\mathrm{SP}_{\scriptscriptstyle N}$. Therefore, we have

$$\mathbb{P}\left(\mathcal{K}^*_{\mathsf{m}}(\mathcal{D}) \leq \mathcal{K}^*(\mathcal{D})\right) \geq 1-\beta_s. \tag{3.48}$$

By defining events $\mathcal{A} := \{\mathcal{D} \,|\, \mathcal{K}^* \leq \mathcal{K}^*_{\mathsf{m}}(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon)\}$, $\mathcal{B} := \{\mathcal{D} \,|\, \mathcal{K}^*_{\mathsf{m}}(\mathcal{D}) \leq \mathcal{K}^*(\mathcal{D})\}$, and $\mathcal{C} := \{\mathcal{D} \,|\, \mathcal{K}^*(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon) \leq 0\}$, where $\mathbb{P}(\mathcal{A}) \geq 1-3\beta$ and $\mathbb{P}(\mathcal{B}) \geq 1-\beta_s$, it is easy to conclude using the same reasoning as in the second part of proof of Theorem (5) that

$$\mathbb{P}(\mathcal{K} \leq 0) \geq 1-3\beta-\beta_s,$$

which ensures safety of the stochastic system with a lower bound $1-\rho$ and a confidence of at least $1-3\beta-\beta_s$. □

3.7 Numerical Examples

The simulations of this section are performed on an iMac 3.5 GHz Quad-Core Intel Core i7. The optimizations are solved by CVX Toolbox [37] with Mosek [5] as the solver.

3.7.1 Temperature Verification for Three Rooms

Consider a temperature regulation problem for three rooms characterized by the following discrete-time stochastic system:

$$\begin{aligned}
\mathrm{T}_1(t+1) =& \big(1-\tau_s(\alpha+\alpha_e)\big)\mathrm{T}_1(t) + \tau_s\alpha\mathrm{T}_2(t) + \\
& \tau_s\alpha_e T_e + w_1(t) \\
\mathrm{T}_2(t+1) =& \big(1-\tau_s(2\alpha+\alpha_e)\big)\mathrm{T}_2(t) + \tau_s\alpha(\mathrm{T}_1(t)+\mathrm{T}_3(t)) + \\
& \tau_s\alpha_e T_e + w_2(t) \\
\mathrm{T}_3(t+1) =& \big(1-\tau_s(\alpha+\alpha_e)\big)\mathrm{T}_3(t) + \tau_s\alpha\mathrm{T}_2(t) + \\
& \tau_s\alpha_e T_e + w_3(t),
\end{aligned} \tag{3.49}$$

where $\mathrm{T}_1(t)$, $\mathrm{T}_2(t)$, and $\mathrm{T}_3(t)$ are temperatures of three rooms, respectively. Terms $w_1(t)$, $w_2(t)$, and $w_3(t)$ are additive zero-mean Gaussian noises with standard deviations of 0.01, which model the environmental uncertainties. Parameter $T_e = 10°C$ is the ambient temperature. Constants $\alpha_e = 8 \times 10^{-3}$ and $\alpha = 6.2 \times 10^{-3}$ are heat exchange coefficients between rooms and the ambient, and individual rooms, respectively. The model for each room is adapted from [36] discretized by $\tau_s = 5$ minutes. Let us consider the regions of interest for each room as $X_{in} = [17°C, 18°C]$, $X_u = [29°C, 30°C]$, and $X = [17°C, 30°C]$. We assume the model of the system and the distribution of the noise are unknown. The main goal is to verify whether the temperature of each room remains in the comfort zone $[17, 29]$ for the time horizon $\mathcal{H} = 3$ which is equivalent to 15 minutes, with a priori confidence of 99%.

Let us consider a barrier certificate with degree $k = 2$ in the polynomial form as $[T1; T2; T3]^T \mathrm{P}[T1; T2; T3] = b_0 T_1^2 + b_1 T_2^2 + b_2 T_3^2 + b_3 T_1 T_2 + b_4 T_1 T_3 + b_5 T_2 T_3 + b_6 T_1 + b_7 T_2 + b_8 T_3 + b_9$, where

$$\mathrm{P} = \begin{bmatrix} b_0 & \frac{b_3}{2} & \frac{b_4}{2} & \frac{b_6}{2} \\ \frac{b_3}{2} & b_1 & \frac{b_5}{2} & \frac{b_7}{2} \\ \frac{b_4}{2} & \frac{b_5}{2} & b_2 & \frac{b_8}{2} \\ \frac{b_6}{2} & \frac{b_7}{2} & \frac{b_8}{2} & b_9 \end{bmatrix}. \tag{3.50}$$

According to Algorithm 2, we first choose the desired confidence parameters β and β_s as $\frac{0.005}{3}$ and 0.005, respectively. The value of empirical approximation error is selected as $\delta = 0.05$. We choose $\rho = 0.2$. The Lipschitz constant is computed as 1.5 according to Remark 12. By enforcing $\hat{M} = 0.005$, the required number of samples for the approximation of the expected value in (3.11) is $\hat{N} = 400$. Now, we solve the scenario problem $\mathrm{SCP}_{N,\hat{N}}$ with the number of samples $N = 6 \times 10^6$ and the computed $\hat{N} = 400$, which gives us the optimal objective value $\mathcal{K}^*(\mathcal{D}) = -0.46$. The computation time is about 5 minutes. For $N = 6 \times 10^6$ and $\beta = \frac{0.005}{3}$, ϵ is computed as 4.36×10^{-6}. Function $G^{-1}(\epsilon)$ is also computed as $16.09\epsilon^{\frac{1}{3}}$ according to Corollary 1.

Since $\mathcal{K}^*(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon) = -0.066 \leq 0$, according to Theorem 5, one can conclude:

$$\mathbb{P}_w(\mathcal{S} \models_3 \Psi) \geq 1 - \rho = 0.80,$$

with a confidence of at least $1 - 3\beta - \beta_s = 0.99$. The barrier certificate constructed from solving $\mathrm{SCP}_{N,\hat{N}}$ is as follows:

$$\begin{aligned} \hat{\mathrm{B}}(b, T_1, T_2, T_3 \mid \mathcal{D}) = {} & 0.112T_1^2 + 0.112T_2^2 + 0.112T_3^2 \\ & - 0.004T_1T_2 - 0.005T_1T_3 - 0.002T_2T_3 \\ & - 3.761T_1 - 3.815T_2 - 3.803T_3 + 99.93. \end{aligned} \tag{3.51}$$

The computed optimal values for c and λ are 0.627 and 14.872, respectively. The scatter plot of the obtained barrier certificate is illustrated in Fig. 3.4. As can be seen in this figure, the barrier certificate has less values in the initial set while it has larger values in the unsafe region.

We remark that the conservatism of our approach is originating from two sources. (a) The first one is that we are using barrier certificates for computing the lower bound. A barrier certificate with a fixed template (polynomial of a certain degree) gives a lower bound that could have a gap with the best lower bound on the safety probability. (b) Our sampling approach requires making the optimization more conservative to account for going from robust programs over continuous (uncountable) domains to a scenario program with finite number of samples. If one assumes that the model is known in this case study, the synthesized barrier certificate has the parameters $c = 0.9767$ and $\lambda = 31.51$. This gives the lower bound 0.875 on the safety probability. Therefore, our approach provides a more conservative lower bound 0.80 since it assumes no knowledge of the model.

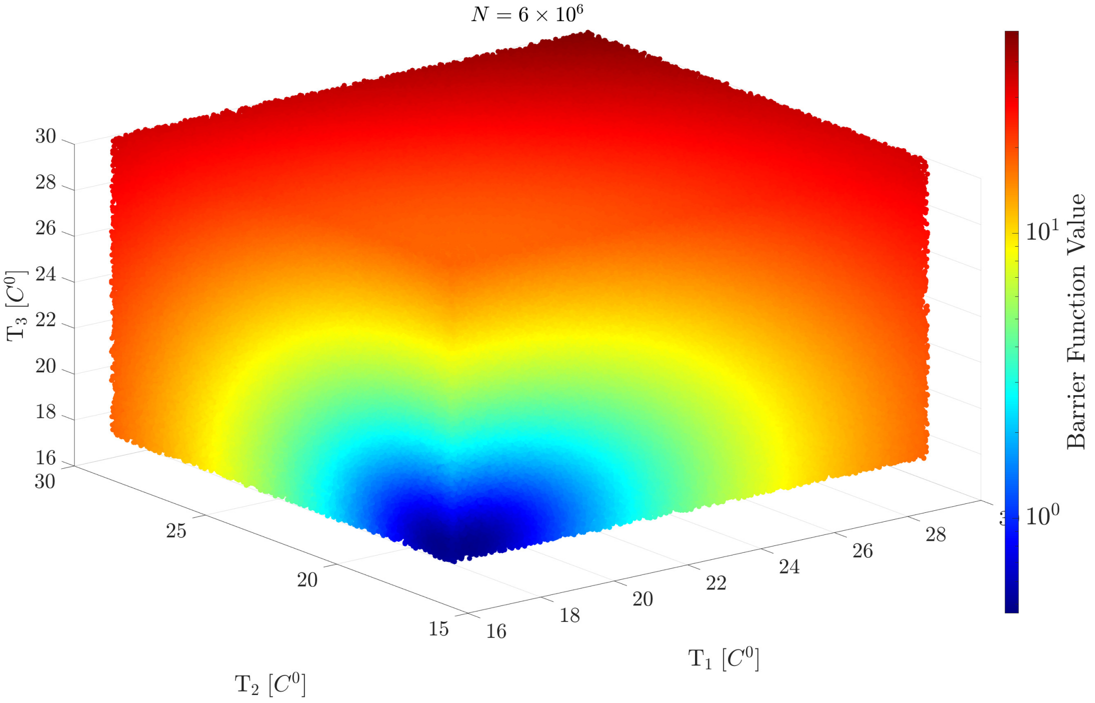


Figure 3.4: Scatter plotting of the barrier certificate indicating portions of the state set where the inequalities in (3.11) are enforced for 6×10^6 sampled data.

3.7.2 Lane Keeping System

Lane keeping assist system is a future development of the modern lane departure warning system embedded in the current vehicles. This system usually assists the driver through electronic assistance with the steering force. The characteristics of this support depends on the distance of the vehicle from the edge of the lane among other factors such as uncertainties[27]. One of the key challenges in such assisting systems is verifying the obtained performance which can be defined as a safety problem.

In this subsection, it is supposed that the model of the vehicle and the distribution of noise are unknown, and one only has access to a finite number of samples. This unknown system is characterized by a simplified kinematic single-track model of BMW320i which is adapted from [4] by discretization of the model and adding noise to imitate the uncertainties.

The nonlinear stochastic difference equation is as follows:

$$\begin{aligned} &x(t+1) = x(t) + \tau_s v \;\cos(\psi(t) + \mathrm{b}) + w_1(t) \\ \mathcal{S} : \; &y(t+1) = y(t) + \tau_s v \;\sin(\psi(t) + \mathrm{b}) + w_2(t) \\ &\psi(t+1) = \psi(t) + \frac{\tau_s v}{l_r} \sin(\mathrm{b}) + w_3(t), \end{aligned} \tag{3.52}$$

where $\mathrm{b} = \frac{l_r}{l_r + l_f} \tan^{-1}(\delta_f)$ with $\delta_f = 5$ degrees as the steering angle. Parameters $l_r = 1.384$ and $l_f = 1.384$ are the distances between the center of gravity of the vehicle to the rear and front axles, respectively. Variables x, y, and ψ denote horizontal movement, vertical movement, and the heading angle, respectively. This system is considered to be affected by zero-mean additive noises w_1, w_2, and w_3 which are related to uncertainties of position x, position y, and the heading angle ψ with standard deviation of 0.01, 0.01, and 0.001 respectively. Other parameters are the sampling time ($\tau_s = 0.1s$), and the velocity ($v = 5m/s$).

The state set is considered as $X = [1, 10] \times [-7, 7] \times [-0.05, 0.05]$. The regions of interest are $X_{in} = [1, 2] \times [-0.5, 0.5] \times [-0.005, 0.005]$, $X_{u_1} = [1, 10] \times [-7, -6] \times [-0.05, 0.05]$, and $X_{u_2} = [1, 10] \times [6, 7] \times [-0.05, 0.05]$. Now, the goal is to verify if the vehicle does not enter the unsafe regions of the lane for the time horizon of $\mathcal{H} = 3$ or equivalently 0.3 s with a desired confidence of 90%.

We consider a barrier certificate of degree $k = 2$ in the polynomial form as

$$[x; y; \psi]^T \mathrm{P} [x; y; \psi] = b_0 x^2 + b_1 y^2 + b_2 \psi^2 + b_3 xy + b_4 x\psi + b_5 y\psi + b_6 x + b_7 y + b_8 \psi + b_9,$$

where the matrix P is as in (3.50).

We follow Algorithm 2 to find the barrier certificate and providing a probabilistic guarantee on the safety of stochastic system. First, the desired confidence parameters β and β_s are chosen as $\frac{.095}{3}$ and 0.005, respectively. We also select the empirical approximation error $\delta = 0.02$. The desired lower bound of safety probability is selected as $1 - \rho = 0.80$. The Lipschitz constant is computed as $\mathrm{L}_x = 10$ according to Remark 12. By enforcing $\hat{M} = 0.006$, the required number of samples for the approximation of the expected value in (3.11) is $\hat{N} = 3000$. Now, we solve the scenario problem $\mathrm{SCP}_{N,\hat{N}}$ with an arbitrary sample number $N = 6 \times 10^6$ and $\hat{N}$ which gives us the optimal value $\mathcal{K}^*(\mathcal{D}) = -0.4518$. The computation time is about 5 minutes. For those values of samples N and β, ϵ is computed as 3.41×10^{-6}. Using Corollary 1, $G^{-1}(\epsilon)$ is computed as $2.92\epsilon^{\frac{1}{3}}$.

Since $\mathcal{K}^*(\mathcal{D}) + 2.92\ \mathrm{L}_x \epsilon^{\frac{1}{3}} = -0.01 \leq 0$, according to Theorem 5, one can deduce that

$$\mathbb{P}_w(\mathcal{S} \models_3 \Psi) \geq 1 - \rho = 0.80,$$

with a confidence of at least $1 - 3\beta - \beta_s = 90\%$. The barrier certificate constructed from solving $\mathrm{SCP}_{N,\hat{N}}$ is represented as:

$$\begin{aligned} \hat{\mathrm{B}}(b, x, y, \psi \mid \mathcal{D}) = &0.39y^2 + 0.15\psi^2 + 0.009x\psi \\ &- 0.007y\psi - 0.015\psi + 0.452. \end{aligned} \tag{3.53}$$

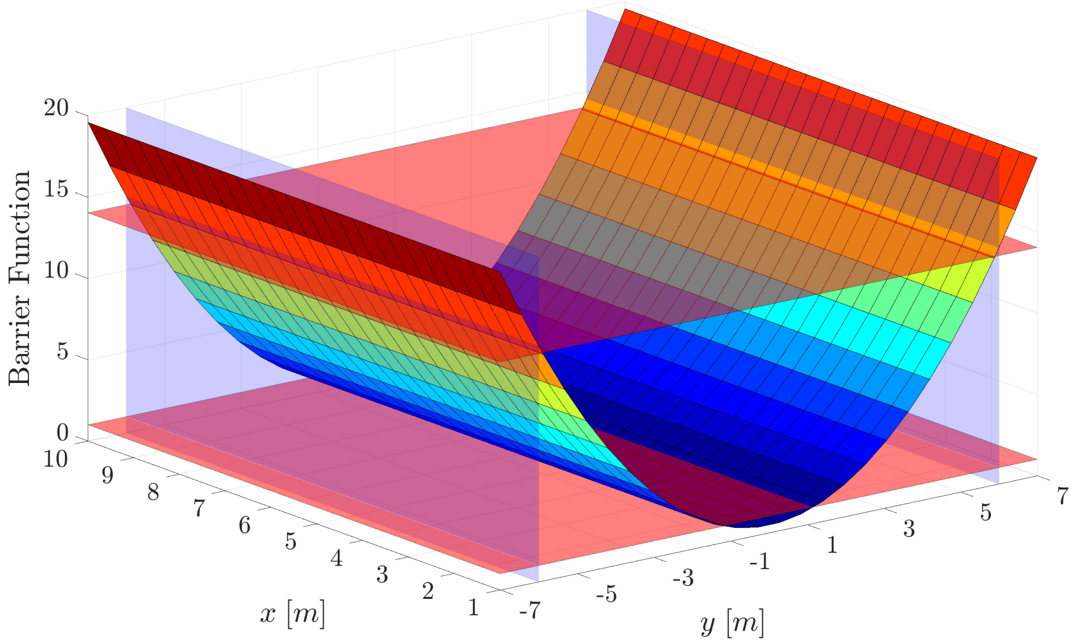


Figure 3.5: Surface plot of the barrier certificate $\mathrm{B}(x, y, \psi)$ with respect to x and y for fixed $\psi = 0$.

The optimal values of c and λ are 0.57 and 14.04, respectively. The exact value of the coefficients are reported in Table 3.1.

The surface plot of the barrier certificate $\mathrm{B}(x, y, \psi) = \hat{\mathrm{B}}(b, x, y, \psi \mid \mathcal{D})$ with respect to x and y for a fixed value of $\psi = 0$ is depicted in Fig. 3.5. The blue transparent planes separate unsafe region on y, while the lower and upper red transparent planes demonstrate the thresholds in constraints (3.3) and (3.4), respectively. Satisfaction of the first and second condition of barrier certificate in Definition 6 can be observed in Fig. 3.5. The satisfaction of the third condition is illustrate in Fig. 3.6.

3.7.3 Synthesizing a Temperature Controller

Consider a temperature regulation problem for a room using a heater characterized by

$$\begin{aligned}\mathcal{S}:\ \mathrm{T}(t+1) =& \mathrm{T}(t) + \tau_s\big(\alpha_e(T_e - \mathrm{T}(t)) + \\ & \alpha_h(T_h - \mathrm{T})u(t)\big) + w(t),\end{aligned} \tag{3.54}$$

where $w(t)$ is a zero-mean Gaussian noise with standard deviation of 0.05. Parameters are $T_e = 15$, $T_h = 45$, $\alpha_e = 8 \times 10^{-3}$, $\alpha_h = 3.6 \times 10^{-3}$, and $\tau_s = 5$. Regions of interest are defined as $X_{in} = [22°C, 23°C]$, $X_{u_1} = [27°C, 28°C]$, $X_{u_2} = [16.5°C, 17.5°C]$, and $X = [16.5°C, 28°C]$. The input region is $[0, 1]$. We assume that the model of the system and the

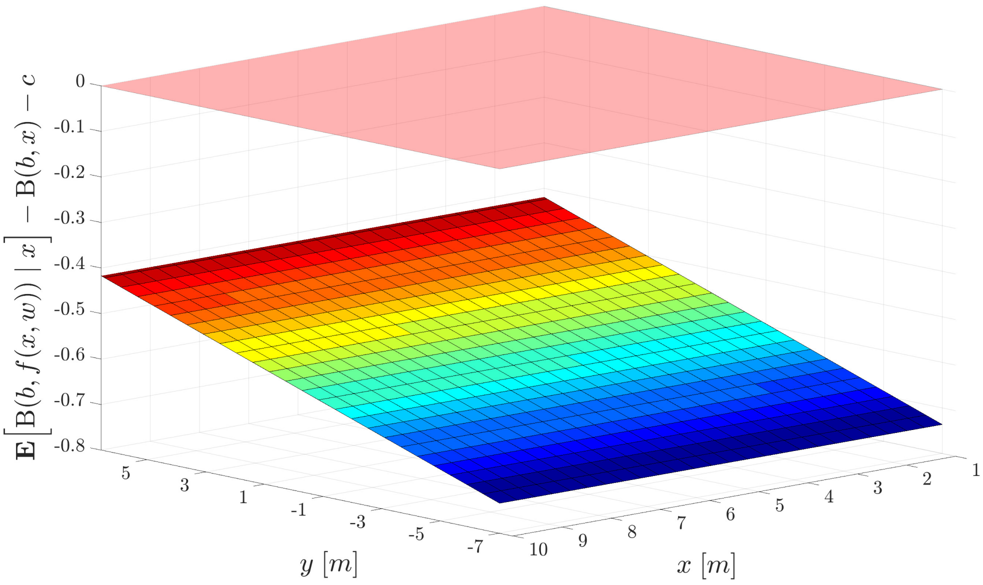


Figure 3.6: Satisfaction of the third condition in Definition 6 (for $\psi = 0$) $\mathrm{B}(x, y, \psi)$ based on collected data.

distribution of the noise are unknown. The main goal is to design a controller that forces the temperature to remain in the comfort zone $[17.5, 27]$ for the time horizon $\mathcal{H} = 60$, which is equivalent to 300 minutes, with a priori confidence of 95%.

Let us fix a control barrier certificate with degree $k = 4$ in the polynomial form as $T^T \mathrm{P} T = b_0 T^4 + b_1 T^3 + b_2 T^2 + b_3 T + b_4$ with $b_0, b_1, b_2, b_3, b_4 \in \mathbb{R}$. The structure of the controller is considered to be a polynomial of degree $k' = 4$ as $u(p^1, T) = T^T \mathrm{P}_u T = p_0 T^4 + p_1 T^3 + p_2 T^2 + p_3 T + p_4$. Matrices P and P_u can be represented as:

$$\mathrm{P} = \begin{bmatrix} b_0 & \frac{b_1}{2} & \frac{b_2}{3} \\ \frac{b_1}{2} & \frac{b_2}{3} & \frac{b_3}{2} \\ \frac{b_2}{3} & \frac{b_3}{2} & b_4 \end{bmatrix}, \mathrm{P}_u = \begin{bmatrix} p_0 & \frac{p_1}{2} & \frac{p_2}{3} \\ \frac{p_1}{2} & \frac{p_2}{3} & \frac{p_3}{2} \\ \frac{p_2}{3} & \frac{p_3}{2} & p_4 \end{bmatrix}. \tag{3.55}$$

According to Algorithm 3, we first choose the desired confidences β and β_s as $\frac{0.005}{3}$ and 0.045 respectively. We also select the approximation error $\delta = 2$. The Lipschitz constant $\mathrm{L}_{x,u}$ is computed as 12 according to Remark 12. By considering $\hat{M} = 1.5 \times 10^5$, the required number of samples for the approximation of the expected value in (3.11) is $\hat{N} = 833330$. Now, we solve the scenario problem $\mathrm{SCP}_{N,\hat{N}}$ with the selected number of samples $N = 1.5 \times 10^6$ and $\hat{N}$ which gives us the optimal value $\mathcal{K}^*(\mathcal{D}) = -0.41$. The computation time is about 2 minutes. For $N = 1.5 \times 10^6$ and $\beta = \frac{0.005}{3}$, value of ϵ is computed as 1.7424×10^{-5}. Using Corollary 3, $G^{-1}(\epsilon)$ is computed as $4.91\epsilon^{\frac{1}{2}}$.

Since $\mathcal{K}^*(\mathcal{D}) + \mathrm{L}_{x,u} G^{-1}(\epsilon) = -0.164 \leq 0$, one has

$$\mathbb{P}^{\mathrm{p}}_{w}(\mathcal{S} \models_{60} \Psi) \geq 1 - \rho = 0.80,$$

with a confidence of at least $1-3\beta-\beta_s = 95\%$. The computed values for λ and c are 4817 and 16.04, respectively. The control barrier certificate constructed from solving $\mathrm{SCP}_{N,\hat{N}}$ is:

$$\hat{\mathrm{B}}(b, T \mid \mathcal{D}) = 11.89\, T^4 - 1.07 \times 10^3\, T^3 + 3.61 \times 10^4\, T^2 \\ - 5.42 \times 10^5 + 3.05 \times 10^6.$$

The obtained controller is:

$$\mathscr{P}_1(p^1, T \mid \mathcal{D}) = 1.45 \times 10^{-5} T^3 + 0.012 T^2 + 0.355.$$

The temperature trajectories for 15 different realizations of noise from three different initial temperature in the range [22°, 23°] is illustrated in Fig. 3.7. As can be seen, the temperature in the collected trajectories do not enter the unsafe set, which is in gray color. We also ran the system to get 10^4 trajectories, all of them remain safe. This confirms the theoretical lower bound computed by our approach.

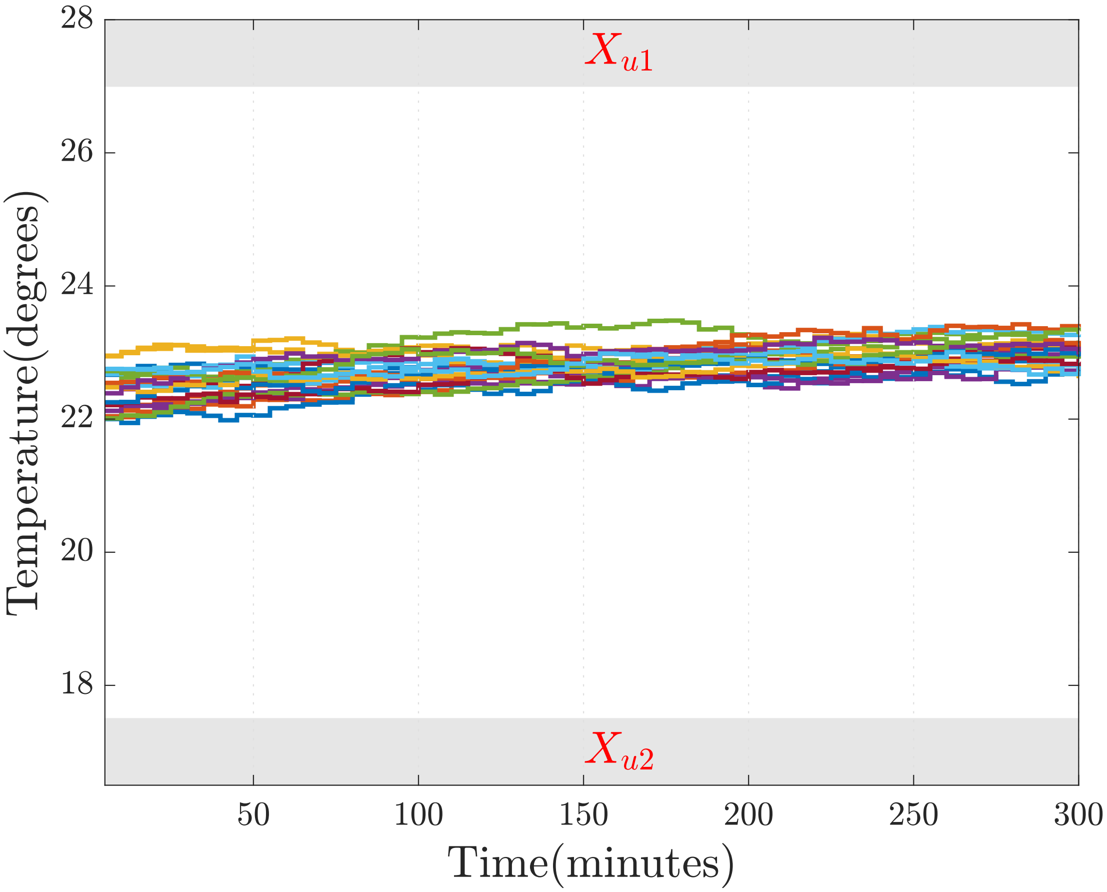


Figure 3.7: The temperature trajectories of 15 different realizations of noise for three different initial temperature in the range [22°, 23°].

In Table 3.1, coefficients of polynomial barrier certificates in three case studies are presented. The values in first two columns from top to the bottom are $\{b_0, \ldots, b_9\}$ in respective case studies. The values in the the third column from top to the bottom are $\{b_0, \ldots, b_4\}$ in the last case study.

Table 3.1: Obtained coefficients of BCs in the case studies

Temperature Verification for three Rooms	Lane Keeping System	Synthesizing a Controller
$1.118824712343290 \times 10^{-1}$	$2.200050812923097 \times 10^{-4}$	$1.189325015407815 \times 10$
$1.121295401333170 \times 10^{-1}$	$3.901846347425760 \times 10^{-1}$	$-1.070392322770013 \times 10^{3}$
$1.122576531449860 \times 10^{-1}$	$1.480240596483330 \times 10^{-1}$	$3.612276124685787 \times 10^{4}$
$-3.751401155407000 \times 10^{-3}$	$-2.825312554914731 \times 10^{-4}$	$-5.417521260597183 \times 10^{5}$
$-4.728480781000000 \times 10^{-3}$	$9.905388481691000 \times 10^{-3}$	$3.046603167514221 \times 10^{6}$
$-2.284303936564000 \times 10^{-3}$	$-6.672383448890000 \times 10^{-3}$	-
$-3.761231117922648 \times 10^{0}$	$-6.918249590565419 \times 10^{-4}$	-
$-3.815332731044874 \times 10^{0}$	$4.678025224577894 \times 10^{-4}$	-
$-3.803570830339135 \times 10^{0}$	$-1.539512818952500 \times 10^{-2}$	-
$9.993049903406006 \times 10$	$4.518033593474370 \times 10^{-1}$	-

3.8 Discussion

We proposed a formal verification and synthesis procedure for discrete-time continuous-space stochastic systems with unknown dynamics against safety specifications. Our approach is based on the notion of barrier certificate and uses sampled trajectories of the unknown system. We first casted the computation of the barrier certificate as a robust convex program (RCP) and approximated its solution with a scenario convex program (SCP) by replacing the unknown dynamics with the sampled trajectories. We then established that the optimal solution of the SCP gives a feasible solution for the RCP with a given confidence, and formulated a lower bound on the required number of samples. Our approach provided a lower bound on the safety probability of the stochastic unknown system when the number of sampled data is larger than a specific lower bound that depends on the desired confidence. We extended the results to a class of non-convex barrier-based safety problems and showed the applicability of our proposed approach using three case studies.

Chapter 4

Sample Complexity Reduction

4.1 Introduction

In this chapter, we introduce three approaches in order to reduce the number of samples required to provide the concrete guarantee over the safety of stochastic systems. In Section 4.1, the motivation and contributions are discussed. The problem statement and preliminaries are introduced in Section 4.2. Three proposed approaches are discussed in detail in Sections 4.3, 4.4, and 4.5, respectively.

4.1.1 Motivation

The data-driven approach that we introduced in Chapter 3 requires a large number of data in order to provide a guarantee over safety of stochastic systems. The number of required data grows exponentially with increasing the dimension of the system. This curse of dimensionality limits the application of our proposed approach to real cyber-physical systems.

4.1.2 Contributions

In this chapter, we develop three approaches to reduce number of the required samples while we provide similar guarantee on safety of stochastic systems introduced in Chapter 3.

- **Wait and Judge Approach.** We provide a data-driven approach equipped with a formal guarantee for verifying the safety of stochastic systems with unknown dynamics. First, using a notion of barrier certificates, the safety verification for a stochastic system is cast as a robust convex program (RCP). Solving this optimization program is hard because the model of the stochastic system, which is unknown, appears in one of the constraints. Therefore, we construct a scenario convex program (SCP) by collecting a number of samples from trajectories of the system. Then, under some condition over the optimal value of the resulted SCP, we are able to relate its optimal decision variables to the safety of the original stochastic system and provide a formal out-of-sample performance guarantee. Particularly, we propose a so-called wait-and-judge approach which a posteriori checks some condition over the optimal value of the SCP for a fixed number of sampled data. If the condition is satisfied, then the safety specification is satisfied with some probability lower bound and a desired confidence.

- **Repetitive Scenario Approach.** We develop a *data-driven* approach for the safety verification of stochastic systems with unknown dynamics. First, we use a notion of barrier certificates in order to cast the safety verification as a robust convex program (RCP). Solving this optimization program is difficult because the model of the stochastic system, which is unknown, appears in one of the constraints. Therefore, we construct a scenario convex program (SCP) by collecting a number of samples from trajectories of the system. Then, we develop a repetition-based scenario framework to provide an out-of-sample performance guarantee for the constructed SCP. In particular, we iteratively solve an SCP for a given number of samples, and then check its feasibility using a certain number of new samples after substituting the optimal decision variables from solving the SCP. We continue the iterations until a desired violation error is achieved. Eventually, a safety condition is checked on top of the feasibility problem. If the safety condition is fulfilled, then we can provide a lower bound on the probability of safety satisfaction for the original stochastic system by leveraging the optimal solution of the successful iteration.

- **Wait, Judge, and Repeat Approach.** In this chapter, we develop a data-driven approach for the safety verification of stochastic systems with unknown dynamics. First, we use a notion of barrier certificates in order to cast the safety verification as a robust convex program (RCP). Solving this optimization program is difficult because the model of the stochastic system, which is unknown, appears in one of the constraints. To tackle this issue, we select a finite number of samples and construct a scenario convex program (SCP). We solve the acquired SCP iteratively until a feasibility condition on its optimizer is satisfied. The feasibility condition is based on the number of computed support constraints at each iteration. Support constraints are those whose elimination affects the optimal value of the optimization problem. When the feasibility condition is satisfied, a safety condition is then checked over the optimal value of the successful iteration. If this condition is satisfied, then one can conclude that the system is safe with a probability lower bound computed using the optimizer of the successful iteration.

I need to mention that the results presented in this chapter appear in the publications [88, 89]. The first result has been presented at the 4th annual conference on learning for dynamics and control conference. The second result has been published in the IEEE control systems letters. This work has also been presented at the 61th IEEE conference on decision and control. The author of the thesis has established the results and written the drafts. Majid Zamani supervised the work.

4.2 Problem Statement and Preliminaries

4.2.1 Notation

The sample space of random variables is denoted by Ω. The Borel σ-algebra on a set X is denoted by $\mathfrak{B}(X)$. The measurable space on X is denoted by $(X, \mathfrak{B}(X))$. We have two probability spaces in this work. The first one is represented by $(X, \mathfrak{B}(X), \mathbb{P})$ which is the probability space defined over the state set X with $\mathbb{P}$ as a probability measure. The second one, $(V_w, \mathfrak{B}(V_w), \mathbb{P}_w)$, defines the probability space over V_w for the random variable w affecting the system as the process noise with $\mathbb{P}_w$ as its probability measure. With a slight abuse of formulation, we use the same notation for $\mathbb{P}$ and $\mathbb{P}_w$ when the product measures are needed. We define a so-called beta-Bionomial distribution as $f_{bb}(q, \alpha, \beta; i) = \binom{q}{i} B(i+\alpha, q-i+\beta)/B(\alpha, \beta)$ for $i = \{0, 1, \ldots, q\}$, where $B(\alpha, \beta)^{-1} = \alpha\binom{\alpha+\beta-1}{\beta-1}, \forall \alpha, \beta \in \mathbb{N}$. $F_{beta}(\alpha, \beta; w)$ denotes the regularized incomplete beta function, and for $\alpha, \beta \in \mathbb{N}, w \in [0, 1]$, it can be expressed as $\sum_{i=\alpha}^{\alpha+\beta-1} \binom{\alpha+\beta-1}{i} w^i (1-w)^{\alpha+\beta-1-i}$. All other notations are the same as the ones in Chapter 3.

4.2.2 System Definition

We deal with discrete-time stochastic systems as in the next definition.

Definition 9. *Consider a discrete-time stochastic system (dt-SS), denoted by*

$$S = (X, V_w, w, f),$$

described by:

$$S \colon x(t+1) = f(x(t), w(t)), \quad t \in \mathbb{N}_0, \tag{4.1}$$

where X and V_w are Borel σ-algebras on the set $\mathbb{R}^n$ and the uncertainty space, respectively.

4.2.3 Problem Statement

First, we formally define what it means for a system to satisfy a safety specification.

Definition 10. *Consider a dt-SS S as in* (4.1) *and a safety specification denoted by the tuple $\Psi = (X_{in}, X_u, H)$, where $X_{in}, X_u \subseteq X$ and $H \in \mathbb{N}_0$. System S satisfies Ψ, denoted by $S \models_H \Psi$, if all trajectories of S started from initial set $X_{in} \subseteq X$ never reach unsafe set $X_u \subseteq X$ within the time horizon H.*

We are interested in solving a safety problem as presented next.

Problem 6. *Consider a dt-SS S as in Definition 9, where f and $\mathbb{P}_w$ are* unknown, *and a safety specification Ψ as in Definition 10. With a confidence of at least $(1-\beta) \in [0, 1]$, provide a lower bound $(1-\Delta) \in [0, 1]$ on the probability with which S satisfies Ψ, i.e., $\mathbb{P}_w\big(S \models_H \Psi\big) \geq 1 - \Delta$, using data collected from trajectories of S.*

4.2.4 Safety Verification of Stochastic Systems

Here, we again explain a notion of barrier certificates and its application in the safety verification of stochastic systems. Let us first formally define a barrier certificate.

Definition 11. *Consider a dt-SS S as in Definition 9 and a safety specification Ψ as in Definition 10. A non-negative function $\mathrm{B} : X \to \mathbb{R}_0^+$ is called a barrier certificate (BC) for S if there exist constants $\lambda > 1$, and $c \in \mathbb{R}$ such that*

$$\begin{aligned}
&\mathrm{B}(x) \leq 1, && \forall x \in X_{in}, && (4.2)\\
&\mathrm{B}(x) \geq \lambda, && \forall x \in X_{u}, && (4.3)\\
&\mathbb{E}\Big[\mathrm{B}(f(x,w)) \mid x\Big] \leq \mathrm{B}(x) + c, && \forall x \in X, && (4.4)
\end{aligned}$$

where $X_{in} \subset X$ and $X_u \subset X$ are initial and unsafe sets, respectively.

Next theorem, borrowed from [51], provides a lower bound on the probability of safety satisfaction for a dt-SS.

Theorem 9. *Consider a dt-SS S and safety specification Ψ as in Definitions 9 and 10, respectively. Suppose there exists a barrier certificate* B *satisfying conditions* (4.2)-(4.4)*. Then, one has*

$$\mathbb{P}_w\big(S \models_H \Psi\big) \geq 1 - \frac{1 + \max\{0, c\}\ H}{\lambda}, \tag{4.5}$$

where $H \in \mathbb{N}_0$ is the finite time horizon associated with Ψ.

According to the results in Chapter 3, a barrier-based safety verification as in Theorem 9 together with Definition 11 can be reformulated as a robust convex program (RCP):

$$\mathrm{RCP}\!:\begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \quad \max\big(g_z(x,d)\big) \leq 0, \forall z \in \{1,\ldots,4\}, \forall x \in X, \\ \qquad\quad \lambda > 1, \quad d = [K;\lambda;c;b], \end{cases} \tag{4.6}$$

where

$$\begin{aligned}
g_1(x,d) &= -\mathrm{B}(b,x) - K,\\
g_2(x,d) &= \mathrm{B}(b,x)\mathbb{1}_{X_{in}}(x) - 1 - K,\\
g_3(x,d) &= -\mathrm{B}(b,x)\mathbb{1}_{X_u}(x) + \lambda - K,\\
g_4(x,d) &= \mathbb{E}\Big[\mathrm{B}(b, f(x,w)) \mid x\Big] - \mathrm{B}(b,x) - c - K.
\end{aligned} \tag{4.7}$$

In the following three sections, Sections 4.3, 4.4, and 4.5, we show how the solution of an $\mathrm{SCP}_{N,\hat{N}}$ for an N and $\hat{N}$ is related to the safety of a stochastic system with an unknown model. We introduce three methods in an attempt to alleviate the sample complexity that arises in the baseline approach in Chapter 3.

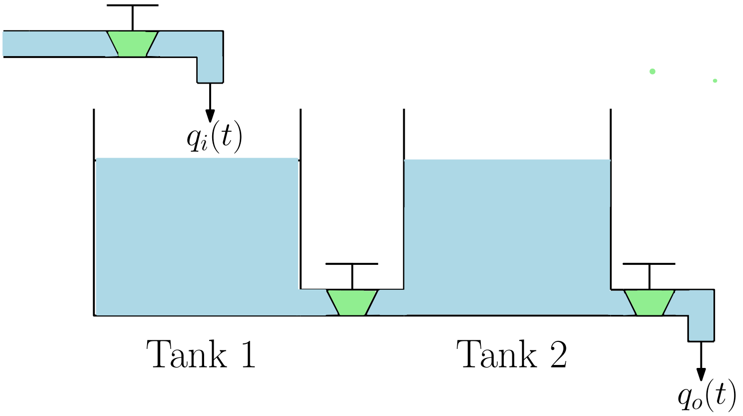


Figure 4.1: Two-Tank system

4.2.5 Two-Tank System

We apply our proposed methods in this chapter to a two-tank system to show their effectiveness and also to compare the results.

Consider a two-tank system in Fig. 4.1 characterized by the following discrete-time stochastic system:

$$\begin{aligned}
\mathrm{h}_1(t+1) &= (1-\tau_s\frac{\alpha_1}{A_1})\ \mathrm{h}_1(t) + \tau_s\frac{q_i(t)}{A_1} + w_1(t)\\
\mathrm{h}_2(t+1) &= \tau_s\frac{\alpha_1}{A_2}\ \mathrm{h}_1(t) + (1-\tau_s\frac{\alpha_2}{A_2})\ \mathrm{h}_2(t) + \tau_s\frac{q_o(t)}{A_2} + w_2(t),
\end{aligned} \tag{4.8}$$

where $\mathrm{h}_1(t)$ and $\mathrm{h}_2(t)$ are heights of two tanks, respectively. Terms $w_1(t)$ and $w_2(t)$ are additive zero-mean Gaussian noises with standard deviations of 0.01, which model the environmental uncertainties. Parameters α_i and A_i, $i \in \{1,2\}$, are valve coefficients and the area of tank i. Variables $q_i(t)$ and $q_0(t)$ are inflow rate entering the first tank and outflow rate exiting the second one at time t, respectively. The model for this two-tank system is adapted from [77] discretized by $\tau_s = 0.1$ seconds. We consider $[\mathrm{h}_1(t+1); \mathrm{h}_2(t+1)] = A_\tau[\mathrm{h}_1(t); \mathrm{h}_2(t)] + b_\tau + [w_1(t); w_2(t)]$, where $A_\tau = [1-\tau_s, 0; \tau_s, 1-\tau_s]$ and $b_\tau = [4.5\tau_s; -3\tau_s]$ in the situation in which input and output valves are fully open, and two constant-rate feeding and retaining pumps ensure constant flows of $q_i(t)$ and $q_o(t)$ with values of $4.5m^3/s$ and $3m^3/s$, respectively. Let us consider $X_{in} = [1.75m, 2.25m]^2$, $X_u = [9m, 10m]^2$, and $X = [1m, 10m]^2$ as the initial, unsafe and the overall state sets, respectively. We assume the model of the system and the distribution of the noise are unknown.

4.3 Wait and Judge Approach

4.3.1 Overview

To tackle Problem 6, we first construct a scenario convex program (SCP) from (4.6) with the help of data collected from the system. Eventually, we provide a result in Subsection 4.3.2 which addresses Problem 6. Fig. 4.2 shows of our approach for solving Problem 6 by connecting the related optimizations and results in this chapter.

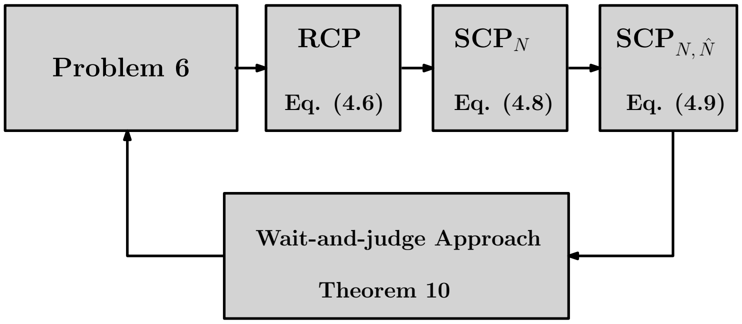


Figure 4.2: An overview of the proposed wait-and-judge approach in this work

In general, finding an optimal solution for the RCP in (4.6) is hard because the map f and the probability measure $\mathbb{P}_w$ are both unknown. Furthermore, there are infinitely many constraints in the RCP since $x \in X$, where X is a continuous set. To tackle this issue, we collect N i.i.d samples $\mathcal{D}_N := \{x_i, f(x_i, w)\} \subset X^2$, for $i \in \{1, \dots, N\}$, using an assigned probability distribution over the state set. Substituting these samples in the RCP in (4.6) results in the following scenario convex program denoted by SCP_{N}:

$$\text{SCP}_{N} : \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \quad \max\big(g_z(x_i, d)\big) \leq 0, z \in \{1, \dots, 4\}, \forall i \in \{1, \dots, N\}, \\ \qquad d = [K; \lambda; c; b], \\ \qquad K \in \mathbb{R},\ \lambda > 1,\ c \geq 0, \end{cases} \tag{4.9}$$

where $g_z(x, d),\ z \in \{1, \dots, 4\}$, are as in (4.7). To address the issue of not knowing $\mathbb{P}_w$ and the expectation term in g_4 (4.7), we replace the expectation term with its empirical mean approximation by sampling $\hat{N}$ i.i.d. values w_j from $\mathbb{P}_w$ for each x_i: $\mathcal{D}_{\hat{N}} := \{x_i, w_j, f(x_i, w_j)\} \subset X \times V_w \times X,\ \forall j \in \{1, \dots, \hat{N}\}$, which results in the following SCP denoted by $\text{SCP}_{N,\hat{N}}$:

$$\text{SCP}_{N,\hat{N}} : \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \quad \max\big(g_z(x_i, d), \bar{g}_4(x_i, d)\big) \leq 0,\ z \in \{1, 2, 3\}, \\ \qquad \forall x_i \in X, \forall i \in \{1, \cdots, N\}, \\ \qquad d = [K; \lambda; c; b], \\ \qquad K \in \mathbb{R},\ \lambda > 1,\ c \geq 0, \end{cases} \tag{4.10}$$

where

$$\bar{g}_4(x_i, d) = \frac{1}{\hat{N}} \sum_{j=1}^{\hat{N}} \mathrm{B}(b, f(x_i, w_j)) - \mathrm{B}(b, x_i) - c - K + \delta. \tag{4.11}$$

We denote by $K^*_{N,\hat{N}}$ and $\hat{\mathrm{B}}(b, x|\mathcal{D}_N, \mathcal{D}_{\hat{N}})$, respectively, the optimal value of $\mathrm{SCP}_{N,\hat{N}}$ and the barrier function constructed based on solution of $\mathrm{SCP}_{N,\hat{N}}$. Note that the expectation term in g_4 (4.9) is approximated by the empirical mean in (4.11). This approximation introduces an error which is denoted by δ in (4.11).

Remark 15. *In this section, N is selected arbitrarily. According to Chapter 3, $\hat{N}$ can be computed as $\hat{N} \geq \frac{\hat{M}}{\delta^2 \beta_s}$ for a desired confidence value $\beta_s \in (0,1)$. This is the confidence that a solution of $SCP_{N,\hat{N}}$ is a feasible solution for SCP_N, i.e., $\mathbb{P}_w\big(\hat{\mathrm{B}}(b, x|\mathcal{D}_N, \mathcal{D}_{\hat{N}}) \models SCP_N\big) \geq 1 - \beta_s$. In this inequality, $\hat{M}$ is a positive constant defined as $Var\big(\mathrm{B}(b, f(x, w)\big) \leq \hat{M}$, $\forall x \in X$, and δ is the approximation error in* (4.11).

4.3.2 Safety Verification of Stochastic Systems via Wait-and-judge Approach

Here, we aim to establish a probabilistic bridge between the solution of the SCP in (4.10) and the safety of a dt-SS as in Definition (9). To do so, we need to assume that all constraints in (4.7) are Lipschitz continuous with respect to x. Next theorem connects the safety of a stochastic system to the optimal solution of the SCP resulted from substituting N number of samples by the number of so-called support constraints. Given N number of constraints, support constraints are those whose elimination affects the optimal value *considerably.*

Theorem 10. *Consider a stochastic system* S *as in* (9)*, where f and $\mathbb{P}_w$ are* unknown*, a safety specification Ψ, and a finite time horizon H. Assume that all constraints in* (4.7) *are Lipschitz continuous with respect to x with a Lipschitz constant* $\mathrm{L_x}$*. Select an arbitrary number of samples N and confidence $\beta \in (0,1)$. Choose $\hat{N}$ as in Remark 15 to achieve a given confidence $1 - \beta_s$, $\beta_s \in (0,1)$. Let us denote by $K^*_{N,\hat{N}}$ and $d^*_{N,\hat{N}} = [\lambda^*; c^*; b^*]$, the optimal value and the optimal solution of $SCP_{N,\hat{N}}$ in* (4.10)*, respectively. If*

$$K^*_{N,\hat{N}} + \mathrm{L_x}\, G^{-1}(1 - T_{N^*}) \leq 0, \tag{4.12}$$

where T_{N^*} is the unique solution of

$$\frac{\beta}{N+1} \sum_{m=N^*}^{N} \binom{m}{N^*} T_{N^*}^{m-N^*} - \binom{N}{N^*} T_{N^*}^{N-N^*} = 0, \tag{4.13}$$

with N^* as the number of support constraints, then the following statement holds true with a confidence of at least $1 - \beta - \beta_s$:

$$\mathbb{P}_w(\mathrm{S} \models_H \Psi) \geq 1 - \frac{1 + c^* H}{\lambda^*}, \tag{4.14}$$

Proof. From the robust convex program in (4.6), one can construct a chance constraint program (CCP) as follows:

$$\mathrm{CCP}_\epsilon: \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \quad \mathbb{P}\Big(\max\big(g_z(x,d)\big)\leq 0\Big) \geq 1-\epsilon,\ z\in\{1,\ldots,4\}, \\ \qquad\ d=[K;\lambda;c;b], \\ \qquad\ K\in\mathbb{R},\ \lambda>1,\ c\geq 0, \end{cases} \tag{4.15}$$

for some $\epsilon > 0$, where $g_z(x,d)$, $z \in \{1,\ldots,4\}$, are defined in (4.7). According to [19, Theorem2], for any $\beta \in (0,1)$ and an arbitrary number of samples N, one has:

$$\mathbb{P}\big(d^*_{\scriptscriptstyle N} \models \mathrm{CCP}_{\epsilon(k)}\big) \geq 1-\beta, \tag{4.16}$$

where $d^*_{\scriptscriptstyle N}$ is the optimal solution of the $\mathrm{SCP}_{\scriptscriptstyle N}$ in (4.9) and $\epsilon(k) := 1-t(k)$, with $t(k)$ as the unique solution of

$$\frac{\beta}{N+1}\sum_{m=k}^{N}\binom{m}{k}\,t^{\,m-k}-\binom{N}{k}\,t^{\,N-k}=0, \tag{4.17}$$

for $k = \{0,\ldots,|d|\}$, where $|d|$ is the number of decision variables d. Let us construct a relaxed version of RCP in (4.6) in amount of $h(\epsilon)$ as the following:

$$\mathrm{RCP}_{h(\epsilon(k))}: \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \quad \max\big(g_z(x,d)\big)\leq h(\epsilon(k)), z\in\{1,\ldots,4\}, \forall x\in X, \\ \qquad\ d=[K;\lambda;c;b], \\ \qquad\ K\in\mathbb{R},\ \lambda>1,\ c\geq 0, \end{cases} \tag{4.18}$$

where $h(\epsilon)$ is a uniform level-set bound as defied in [29, Definition 3.1]. According to [29, Lemma 3.2], one can deduce from (4.16) that $\mathbb{P}\big(d^*_{\scriptscriptstyle N} \models \mathrm{RCP}_{h(\epsilon(k))}\big) \geq 1-\beta$ which leads to:

$$\mathbb{P}(K^*_{\mathrm{RCP}_{h(\epsilon(k))}} \leq K^*_{\scriptscriptstyle N}) \geq 1-\beta, \tag{4.19}$$

where $K^*_{\scriptscriptstyle N}$ is the optimal value of $\mathrm{SCP}_{\scriptscriptstyle N}$ in (4.9). Using Lemma 3.4 in [29], we have:

$$K^*_N \leq K^*_{\mathrm{RCP}} \leq K^*_{\mathrm{RCP}_{h(\epsilon(k))}} + \mathcal{L}_{sp}h(\epsilon(k)), \tag{4.20}$$

where $\mathcal{L}_{sp}$ is the slater constant which is defined in [29, Assumption 3.3]. Combination of (4.19) and (4.20) results in:

$$\mathbb{P}\Big(K^*_N \leq K^*_{\mathrm{RCP}} \leq K^*_N + \mathcal{L}_{sp}h(\epsilon(k))\Big) \geq 1-\beta. \tag{4.21}$$

Since the optimization problem in (4.6) is a min-max problem, $\mathcal{L}_{sp}$ can be chosen as 1 according to Remark 3.5 in [29]. Uniform level-set bound $h(\epsilon(k))$ can be computed as $\mathrm{L_x}\sqrt[n]{\epsilon(k)}$ as stated in [29, Remark 3.8], where $\mathrm{L_x}$ is the Lipschitz constant of constraints in (4.7). From now on, we use ϵ instead of $\epsilon(k)$ for $k = N^*$, where N^* is the number of support constraints. Therefore, (4.21) can be written as:

$$\mathbb{P}\Big(K_N^* \leq K_{\text{RCP}}^* \leq K_N^* + \mathrm{L_x}\,\epsilon^{\frac{1}{n}}\Big) \geq 1 - \beta. \tag{4.22}$$

By writing $1-T_{N^*}$ instead of $\epsilon = 1-t(k)$ for $k = N^*$, the above inequality can be re-written as:

$$\mathbb{P}\Big(K_N^* \leq K_{\text{RCP}}^* \leq K_N^* + \mathrm{L_x}\,(1 - T_{N^*})^{\frac{1}{n}}\Big) \geq 1 - \beta. \tag{4.23}$$

By denoting the optimal solution of the $\text{SCP}_{N,\hat{N}}$ in (4.10) by $d_{N,\hat{N}}^*$, one obtains $\mathbb{P}\big(d_{N,\hat{N}}^* \models \text{SCP}_N\big) \geq 1 - \beta_s$ according to [83, Theorem 3.3] which implies:

$$\mathbb{P}\big(K_N^* \leq K_{N,\hat{N}}^*\big) \geq 1 - \beta_s. \tag{4.24}$$

By defining two events $A := \{K_N^* \leq K_{\text{RCP}}^* \leq K_N^* + \mathrm{L_x}\,(1-T_{N^*})^{\frac{1}{n}}\}$ and $B := \{K_N^* \leq K_{N,\hat{N}}^*\}$ with $\mathbb{P}(A) \geq 1 - \beta$ and $\mathbb{P}(B) \geq 1 - \beta_s$, it is easy to see that $(A \cap B) \subseteq (K_{\text{RCP}}^* \leq K_{N,\hat{N}}^* + \mathrm{L_x}(1 - T_{N^*})^{\frac{1}{n}})$. By assumption, we have $K_{N,\hat{N}}^* + \mathrm{L_x}(1 - T_{N^*})^{\frac{1}{n}} \leq 0$ and, hence, one can deduce:

$$\mathbb{P}(K_{\text{RCP}}^* \leq K_{N,\hat{N}}^* + \mathrm{L_x}(1 - T_{N^*})^{\frac{1}{n}} \leq 0) \geq \mathbb{P}(A \cap B) \geq 1 - \mathbb{P}(A^c) - \mathbb{P}(B^c) \geq 1 - \beta - \beta_s. \tag{4.25}$$

This concludes the proof because the non-positiveness of K_{RCP}^* guarantees that the feasible solution of RCP in (4.6) satisfies with a confidence of at least $1-\beta-\beta_s$ the barrier conditions in Theorem 9. □

Remark 16. *There is an upper-bound on the number of support constraints, i.e, $N^* \leq |d| + 1$, where $|d|$ is the number of decision variables in $SCP_{N,\hat{N}}$ (4.10). Note that the value of $1 - T_{N^*}$ is increasing with respect to N^*. As a result, one can use this upper-bound instead of the actual number of support constraints N^* in Theorem 10.*

The steps required for applying Theorem 10 are presented in Algorithm 4. The inputs are the desired confidence, and the Lipschitz constant of constraints in (4.7). The output is a lower bound on the safety of the stochastic system in (4.1) based on the solution of the SCP in (4.10) with an a priori guaranteed confidence. The coefficients of the barrier certificate satisfying conditions (4.2)-(4.4) are obtained in step 5 of Algorithm 4.

4.3.3 Two-Tank System Safety Verification: A Wait and Judge Solution

The main goal is to verify that the heights of tanks stay away from the unsafe region within the time horizon $H = 5$ with an a priori confidence 99%. Let us consider a barrier

Algorithm 4 Data-driven safety verification of a stochastic system via wait-and-judge approach

```
Require: Parameters $\beta \in (0,1)$, $\beta_s \in (0,1)$, $\mathrm{L_x} \in \mathbb{R}^+$, and the degree of the barrier
    certificate
1: Compute the number of noise realization $\hat{N}$ according to Remark 15
2: Choose an arbitrary number of samples $N$
3: Select a probability measure $\mathbb{P}$ over the state set $X$
4: Collect $N\hat{N}$ pairs $\big(x_i, f(x_i, w_{ij})\big)_{i,j} \in X^2$ from the system
5: Solve the $\mathrm{SCP}_{N,\hat{N}}$ in (4.10) with the data-set in Step 4 and obtain $K^*_{N,\hat{N}}$
6: Compute the actual number of support constraints $N^*$ or the upper bound on it (see
    Remark 16)
7: Compute the parameter $T_{N^*}$ according to (4.13)
Ensure: If $K^*_{N,\hat{N}} + \mathrm{L_x}\,(1 - T_{N^*})^{\frac{1}{n}} \leq 0$, then $\mathbb{P}_w(S \models_H \Psi) \geq 1 - \frac{1+c^*H}{\lambda^*}$ with a confidence of
    at least $1 - \beta - \beta_s$.
```

certificate with degree $k = 2$ in the polynomial form as $[\mathrm{h}_1; \mathrm{h}_2; 1]^T \mathrm{P} [\mathrm{h}_1; \mathrm{h}_2; 1] = b_0\mathrm{h}_1^2 + b_1\mathrm{h}_2^2 + b_2\mathrm{h}_1\mathrm{h}_2 + b_3\mathrm{h}_1 + b_4\mathrm{h}_2 + b_5$, where

$$\mathrm{P} = \begin{bmatrix} b_0 & \frac{b_3}{2} & \frac{b_2}{2} \\ \frac{b_3}{2} & b_1 & \frac{b_4}{2} \\ \frac{b_2}{2} & \frac{b_4}{2} & b_5 \end{bmatrix}. \tag{4.26}$$

By having $\|x\| \leq \sqrt{2} \times 10$ and enforcing $\|P\| \leq 0.2$, the Lipschitz constant can be computed as $\mathrm{L}_x = 11.03$ using [83, Lemma 1]. The value of empirical approximation error in (4.11) is selected as $\delta = 0.05$. By enforcing $\hat{M} = 0.001$, the required number of samples for the approximation of the expected value in (4.10) is computed as $\hat{N} = 400$ according to Remark 15 in order to provide a confidence of $1 - \beta_s$, where $\beta_s = 0.001$.

To show the effectiveness of our approach in allowing us to have a much lower number of samples, we first solve the safety verification problem for the two-tank system via the approach proposed in the literature and then we apply our proposed wait-and-judge approach here. We show that our approach provides the same formal guarantee with a significantly lower number of samples.

4.3.4 Safety Verification using the baseline approach

We choose $\epsilon = 0.04$ and $\Delta = 0.1$ in [83, Algorithm 1]. We also select the confidence parameter β as 0.009. The minimum number of samples needed for solving $\mathrm{SCP}_{N,\hat{N}}$ in (4.10) is computed as $N = 1337297$ using [83, equation (17)]. $\hat{N}$ is computed as 400 for a confidence value of $\beta_s = 0.001$. Now, we solve the scenario problem $\mathrm{SCP}_{N,\hat{N}}$ with acquired values of N and $\hat{N}$ which gives us the optimal value $K^*_{N,\hat{N}} = -0.1025$. Since $K^*_{N,\hat{N}} + \epsilon =$

$-0.0625 \leq 0$, according to [83, Theorem 4], one can conclude: $\mathbb{P}_w(S \models_5 \Psi) \geq 1 - \Delta = 0.90$ with a confidence of at least $1 - \beta - \beta_s = 99\%$.

4.3.5 Safety Verification via the Proposed Wait-and-Judge Approach

We select the desired confidence parameter $\beta = 0.009$. There is no need to fix ϵ a priori in our proposed approach here. We initially select an arbitrary number of samples $N = 500$. Number of support constraints is computed as $N^* = 7$. Parameter $1 - T_{N^*}$ is computed using (4.13) as 0.0087. The optimal value $K^*_{N,\hat{N}}$ is computed for $N = 500$ and $\hat{N} = 400$ as -0.1871. Then, the condition in (4.12) is not satisfied, i.e., $K^*_{N,\hat{N}} + \mathrm{L}_x(1 - T_{N^*})^{\frac{1}{2}} = 0.8417 \not\leq 0$. Therefore, we cannot say anything about the safety of the two-tank system based on Theorem 10. By computing T_{N^*} for several numbers of samples according to (4.13), the appropriate number of samples to satisfy (4.12) is computed as $N = 70000$. Since the value of $1 - T_{N^*}$ is increasing with respect to the number of support constraints N^*, and there is an upper-bound on it, we use this upper-bound in our experiment. One has $N^* \leq |d| + 1$, where $|d|$ is the number of decision variables in (4.10). Here, we select the upper-bound on N^* as 10, given that the number of decision variables is 9. The optimal value $K^*_{N,\hat{N}}$ is computed for $N = 70000$ and $\hat{N} = 400$ as -0.1065. In this case, $1 - T_{N^*}$ is computed as 0.6653×10^{-4}. Now the condition in (4.12) is satisfied, i.e., $K^*_{N,\hat{N}} + \mathrm{L}_x(1 - T_{N^*})^{\frac{1}{2}} = -0.0165 \leq 0$, hence one can obtain $\mathbb{P}_w(\mathrm{S} \models_5 \Psi) \geq 0.90$ with a confidence of at least $1 - \beta - \beta_s = 99\%$. The barrier certificate constructed from solving $\mathrm{SCP}_{N,\hat{N}}$ is as follows:

$$\hat{\mathrm{B}}\big(b, \mathrm{p}_1, \mathrm{p}_2 \,|\, \mathcal{D}_N, \mathcal{D}_{\hat{N}}\big) = 0.0648\mathrm{p}_1^2 + 0.1784\mathrm{p}_2^2 + 0.0145\mathrm{p}_1\mathrm{p}_2 - 0.1687\mathrm{p}_1 - 0.0321\mathrm{p}_2 + 0.0486.$$

The computed optimal values for c and λ are 0.1804 and 19.1280, respectively. It should be noted that the same desired confidence is achieved here as in the approach proposed in [83] using a significantly lower number of samples, i.e., 70000 compared to 1337297, which is the main benefit of our approach. In terms of computation time, our approach is much more faster than the one in [83]. Computing the optimal value and checking the condition over the optimal value for the approach in [83] takes about 2 hours on a MacBook 2.8 GHz Quad-Core Intel Core i7, while it only takes less than 30 seconds using our proposed approach.

4.4 Repetitive Scenario Approach

4.4.1 Overview

The overview of our proposed repetitive scenario approach for solving Problem 6 is depicted in Fig. 4.3, which connects the related optimizations and results throughout the section. First, a stochastic safety problem is reformulated as a scenario convex program (SCP) by collecting N samples from the state set, and $\hat{N}$ samples from the realization of the noise. The constructed scenario program is solved, and the obtained optimal solution is sent to a feasibility checker called a feasibility oracle. In this oracle, the feasibility of the SCP is assessed for N_0 new test samples by checking the constraints after substituting the optimal decision variables from the previous step. The violation of constraints is measured through an empirical mean over the violated constraints. These two steps, namely solving the SCP for collected samples and feasibility oracle, are executed for a specific number of iterations, until the violation error is less than a desired threshold. Finally, a safety condition is checked on top of the feasibility oracle. If the safety condition is satisfied, with an a-priori fixed confidence, one can conclude that the original stochastic system with unknown dynamic is safe with a probability lower bound computed using the optimal solution coming from the successful iteration.

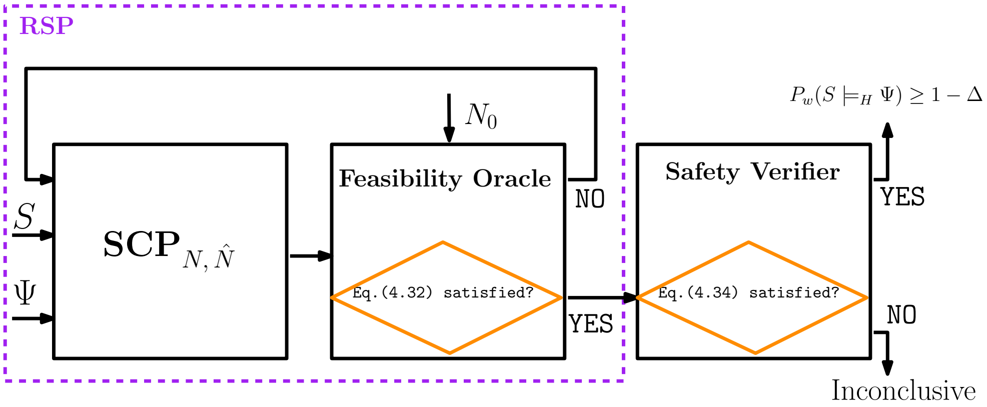


Figure 4.3: An overview of our repetition-based scenario approach. The block on the left solves a scenario program SCP_{N} using $N\hat{N}$ samples collected from the system at each iteration. The resulted optimizer of this scenario program is fed into a feasibility oracle, which assesses the feasibility of the computed optimizer for N_0 new test samples. Finally, the block on the right checks a condition whose satisfaction ensures Ψ is satisfied with a probability lower-bound computed using the optimal solution of the successful iteration.

In general, finding an optimal solution for the RCP in (4.6) is difficult (or even impossible) because the map f and the probability measure $\mathbb{P}_w$ are both unknown. Furthermore, there are infinitely many constraints in the RCP since $x \in X$, where X is a continuous set. To address the issue of unknown $\mathbb{P}_w$ and the expectation term in g_4 in (4.7), we replace the expectation term with its empirical mean approximation by collecting $\hat{N}$ i.i.d. samples w_j, $j \in \{1, \ldots, \hat{N}\}$, from $\mathbb{P}_w$ and construct a new RCP denoted by $\mathrm{RCP}_{\hat{N}}$ as follows:

$$\mathrm{RCP}_{\hat{N}}\colon\begin{cases}\min\limits_{d} \quad K\\ \text{s.t.} \;\; \max\big(g_z(x,d), \bar{g}_4(x,w_j,d)\big) \leq 0, z \in \{1,\ldots,3\},\\ \qquad j \in \{1,\ldots,\hat{N}\}, \forall x \in X, \lambda > 1, d = [K;\lambda;c;b],\end{cases} \tag{4.27}$$

where

$$\bar{g}_4(x,w_j,d) = \frac{1}{\hat{N}}\sum_{j=1}^{\hat{N}} \mathrm{B}(b,f(x,w_j)) - \mathrm{B}(b,x) - c - K + e. \tag{4.28}$$

Notice that the expectation term in g_4 in (4.7) is approximated by the empirical mean in (4.28). This approximation introduces an error which is introduced by e in (4.28). Next theorem, borrowed from [84, Theorem 3.4], shows that the optimal solution of the $\mathrm{RCP}_{\hat{N}}$ is a feasible solution for the RCP in (4.6) with a certain confidence.

Theorem 11. *Let d_s^* be a feasible solution of the $RCP_{\hat{N}}$ for some $e > 0$, and assume $Var\big(\mathrm{B}(b,f(x,w))\big) \leq \hat{M}$, $\forall x \in X$ with a given positive $\hat{M}$. Then, for any $\beta_s \in (0,1)$, one has $\mathbb{P}(d_s^* \models RCP) \geq 1-\beta_s$, if the number of samples in the empirical mean satisfies $\hat{N} \geq \frac{\hat{M}}{e^2\beta_s}$.*

Now, one can assign a probability distribution over the state set and collect N i.i.d. samples to solve $\mathrm{RCP}_{\hat{N}}$ in (4.27). The data-set is denoted by:

$$\begin{aligned}\mathcal{D}_{N,\hat{N}} := \big\{ (x_i, w_j, f(x_i,w_j)) \subset X \times V_w \times X \mid \\ i \in \{1,\dots,N\}, j \in \{1,\dots,\hat{N}\}\big\}.\end{aligned} \tag{4.29}$$

By substituting these samples in $\mathrm{RCP}_{\hat{N}}$ in (4.27) results in the following SCP denoted by $\mathrm{SCP}_{N,\hat{N}}$:

$$\mathrm{SCP}_{N,\hat{N}}: \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \ \ \max\left(g_z(x_i,d), \bar{g}_4(x_i,w_j,d)\right) \leq 0, \\ \qquad \lambda > 1, z \in \{1,2,3\}, i \in \{1,\dots,N\}, \\ \qquad j \in \{1,\dots,\hat{N}\}, d = [K;\lambda;c;b]. \end{cases} \tag{4.30}$$

4.4.2 Repetitive Scenario Program

Inspired by the the idea of repetitive scenario design in [16], we aim at constructing an RSP for the stochastic safety problem. The main idea is to solve an $\mathrm{SCP}_{N,\hat{N}}$ in (4.30) for several iterations. At each iteration, the obtained optimal values denoted by $d^*_{N,\hat{N}}$ are used to construct a feasibility problem denoted by $\mathrm{SCP}_{N_0,\hat{N}}$ using N_0 new test samples.

The violation criteria for the constraints using the k^{th} sampled data, where $k \in \{1,\dots,N_0\}$, in the constructed feasibility problem at each iteration can be quantified as:

$$v_{N,\hat{N}}(k) = \begin{cases} 1 & \min\big(-g_z(x_k,d^*_{N,\hat{N}}), -\bar{g}_4(x_k,w_j,d^*_{N,\hat{N}})\big) \leq 0, \\ & z \in \{1,2,3\}, j \in \{1,\dots,\hat{N}\}, \\ 0 & \text{otherwise}. \end{cases} \tag{4.31}$$

Now, we define the concept of *successful iteration*.

Definition 12. *The overall violation error for N_0 test samples can be computed by applying an empirical mean over all violated constraints at each iteration and can be upper bounded by a given desired value:*

$$\frac{\sum_{k=1}^{N_0} v_{N,\hat{N}}(k)}{N_0} \leq \epsilon'. \tag{4.32}$$

We call the first iteration at which the above condition is satisfied the successful iteration.

Now, we introduce Algorithm 5 to systematically construct an RSP. The optimal solution of the RSP resulted from Algorithm 5 is denoted by d^*.

Algorithm 5 Repetitive Scenario Program (RSP Algorithm)

```
Require: Number of samples ($N$, $\hat{N}$, and $N_0$) and the desired violation error $\epsilon'$
1: Collect $\hat{N}$ samples $w_j, j \in [1, \dots, \hat{N}]$ from $\mathbb{P}_w$
2: Collect $N$ samples $x_i, i \in [1, \dots, N]$ from the state set
3: Solve the SCP$_{N,\hat{N}}$ in (4.30) using the collected data in Step 1 and Step 2, and obtain
   the optimizer $d^*_{N,\hat{N}}$
4: Feasibility Oracle: Construct the feasibility problem SCP$_{N_0,\hat{N}}$ using $N_0$ new samples by
   feeding the optimal values from Step 3 to the scenario program in (4.30)
5: Compute $\frac{\sum_{k=1}^{N_0} v_{N,\hat{N}}(k)}{N_0}$ for $v_{N,\hat{N}}(k)$ as in (4.31)
6: If (4.32) is satisfied, then $d^* = d^*_{N,\hat{N}}$, otherwise go to Step 2.
```

Remark 17. *According to [16, Theorem 3], Algorithm 5 terminates within* $(1-H_{1,\epsilon'.}(N))^{-1}$ *iterations with probability one, where* $H_{1,\epsilon'}(N) = 1 - \sum_{i=0}^{\lfloor \epsilon' N_0 \rfloor} f_{bb}(N_0, |d|, N+1-|d|; i)$, f_{bb} *is the beta-Binomial distribution, and* $|d|$ *is the number of decision variables in* (4.30). *Furthermore, for the large values of* N_0, *the expected number of iterations in order to satisfy* (4.32), *and accordingly termination of the algorithm, is approximated by*

$$\frac{1}{1-\beta_{\epsilon'}(N)}, \tag{4.33}$$

where $\beta_{\epsilon'}(N) = 1 - \sum_{i=|d|}^{N} \binom{N}{i} \epsilon'^{i} (1-\epsilon')^{N-i}$. *For the sake of simple presentation, we use this approximation in the rest of the section.*

In the next subsection, we relate the optimal solution of an RSP to that of RCP in (4.6) and finally to the safety of stochastic systems.

4.4.3 Safety Verification of Stochastic Systems- A Repetitive Scenario Approach

Here, we provide a probabilistic connection between the optimal value of a repetitive scenario optimization program RSP as in Algorithm 5 and the safety of stochastic systems with unknown dynamics in Definition 4.1. The next theorem provides the relation between the solution of a repetitive scenario program and the original safety problem.

Theorem 12. *Consider a stochastic system S as in* (9)*, where f and $\mathbb{P}_w$ are* unknown*, and a safety specification Ψ as in Definition 10. Assume all constraints in* (4.7) *are Lipschitz continuous*[1] *with respect to x and with a Lipschitz constant $\mathrm{L_x}$. Let $\epsilon, \epsilon' \in [0,1], \epsilon' \leq \epsilon$. Choose $\hat{N}$ as in Theorem 11 based on a given confidence $1-\beta_s, \beta_s \in (0,1)$. Suppose that for a given N and N_0, there is a successful iteration (cf. Definition 12) for RSP in Algorithm 1, for which the optimal solution is $d^* = [K^*; \lambda^*; c^*; b^*]$. If*

$$K^* + \mathrm{L_x}\, G^{-1}(\epsilon) \leq 0, \tag{4.34}$$

then

$$\mathbb{P}_w(\mathrm{S} \models_H \Psi) \geq 1 - \frac{1+c^*H}{\lambda^*}, \tag{4.35}$$

with a confidence of at least $1-\bar{\beta}_{\epsilon,\epsilon'}(N,N_0)-\beta_s$, where

$$\bar{\beta}_{\epsilon,\epsilon'}(N,N_0) = 1 - \textstyle\sum_{i=\lfloor |d|+\epsilon' N_0 - 1\rfloor + 1}^{N+N_0} \binom{N+N_0}{i} \epsilon^i (1-\epsilon)^{N+N_0-i},$$

and $|d|$ is the number of decision variables in (4.30)*.*

Proof. From the robust convex program $\mathrm{RCP}_{\hat{N}}$ in (4.27), one can construct a chance constraint program as:

$$\mathrm{CCP}_\epsilon\!:\!\begin{cases} \min\limits_{d} \quad K \\ \text{s.t. } \mathbb{P}\left(\max\left(g_z(x,d), \bar{g}_4(x,w_j,d)\right) \leq 0\right) \geq 1-\epsilon, \\ \qquad j \in \{1,\ldots,\hat{N}\}, z \in \{1,\ldots,3\}, \\ \qquad \lambda > 1, d = [K;\lambda;c;b], \end{cases} \tag{4.36}$$

for some $\epsilon > 0$, where $g_z(x,d),\ z \in \{1,\ldots,3\}$, and $\bar{g}_4$ are defined in (4.7) and (4.41), respectively. Using Theorem 3 in [16] and for a given N and N_0, one obtains

$$\mathbb{P}\left(d^* \models \mathrm{CCP}_\epsilon\right) \geq 1 - \bar{\beta}_{\epsilon,\epsilon'}(N,N_0), \tag{4.37}$$

for some $\epsilon' \leq \epsilon$, where $d^* = [K^*;\lambda^*;c^*;b^*]$ is the optimal solution of the RSP in Algorithm 1. Now, we construct a relaxed version of $\mathrm{RCP}_{\hat{N}}$ in (4.27) as follows:

$$\mathrm{RCP}_{h(\epsilon)}:\begin{cases} \min\limits_{d} \quad K \\ \text{s.t. } \max\left(g_z(x,d), \bar{g}_4(x,w_j,d)\right) \leq h(\epsilon), \\ \qquad j \in \{1,\ldots,\hat{N}\}, z \in \{1,\ldots,3\}, \forall x \in X, \\ \qquad \lambda > 1,\ d = [K;\lambda;c;b], \end{cases} \tag{4.38}$$

[1] We only need to consider Lipschitz continuity of g_2 and g_3 inside X_{in} and X_u, respectively.

where $h(\epsilon)$ is a uniform level-set bound as defined in [29, Definition 3.1]. According to [16], N_0 can be selected such that $\bar{\beta}_{\epsilon,\epsilon'}(N, N_0) \leq \beta_\epsilon(N)$. As a result, one can use Lemma 3.2 in [29] and conclude from (4.37) that $\mathbb{P}\big(d^* \models \mathrm{RCP}_{h(\epsilon)}\big) \geq 1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0)$, which readily results in $\mathbb{P}(K^*_{\mathrm{RCP}_{h(\epsilon)}} \leq K^*) \geq 1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0)$. The last inequality is true mainly because $K^*_{\mathrm{RCP}_{h(\epsilon)}}$ is the optimal value of $\mathrm{RCP}_{h(\epsilon)}$ in (4.38), whereas K^* is just the optimization value for a feasible solution (i.e. d^*). Using Lemma 3.4 in [29], we obtain $K^* \leq K^*_{\mathrm{RCP}_{\hat{N}}} \leq K^*_{\mathrm{RCP}_{h(\epsilon)}} + \mathcal{L}_{sp} h(\epsilon)$, where $K^*_{\mathrm{RCP}_{\hat{N}}}$ is the optimal value of $\mathrm{RCP}_{\hat{N}}$ in (4.27), and $\mathcal{L}_{sp}$ is the Slater constant defined in [29, Assumption 3.3]. Therefore, one can deduce $\mathbb{P}\Big(K^* \leq K^*_{\mathrm{RCP}_{\hat{N}}} \leq K^* + \mathcal{L}_{sp} h(\epsilon)\Big) \geq 1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0)$. Since the optimization problem in (4.27) is a min-max problem, $\mathcal{L}_{sp}$ can be chosen as 1 according to Remark 3.5 in [29]. Uniform level-set bound $h(\epsilon)$ can be computed as $\mathrm{L_x} \sqrt[n]{\epsilon}$ as stated in [29, Remark 3.8], where $\mathrm{L_x}$ is the Lipschitz constant of constraints. Therefore, we have $\mathbb{P}\Big(K^* \leq K^*_{\mathrm{RCP}_{\hat{N}}} \leq K^* + \mathrm{L_x}\, \epsilon^{\frac{1}{n}}\Big) \geq 1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0)$. Let us denote the optimal solution of the RCP in (4.27) by $d^*_{\mathrm{RCP}_{\hat{N}}}$. We get $\mathbb{P}\big(d^*_{\mathrm{RCP}_{\hat{N}}} \models \mathrm{RCP}\big) \geq 1 - \beta_s$ for a specific $\hat{N}$ according to Theorem 11. This inequality implies $\mathbb{P}\big(K^*_{\mathrm{RCP}} \leq K^*_{\mathrm{RCP}_{\hat{N}}}\big) \geq 1 - \beta_s$, where K^*_{RCP} is the optimal value of the RCP in (4.6). By defining events $\mathcal{A} := \{K^* \leq K^*_{\mathrm{RCP}_{\hat{N}}} \leq K^* + \mathrm{L_x}\, \epsilon^{\frac{1}{n}}\}$ and $\mathcal{B} := \{K^*_{\mathrm{RCP}} \leq K^*_{\mathrm{RCP}_{\hat{N}}}\}$, where $\mathbb{P}(\mathcal{A}) \geq 1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0)$ and $\mathbb{P}(\mathcal{B}) \geq 1 - \beta_s$, it is easy to see that $(\mathcal{A} \cap \mathcal{B}) \subseteq (K^*_{\mathrm{RCP}} \leq K^* + \mathrm{L_x}\, \epsilon^{\frac{1}{n}})$. By the assumption of the theorem, we have $K^* + \mathrm{L_x}\, \epsilon^{\frac{1}{n}} \leq 0$. Hence, one obtains $\mathbb{P}(K^* + \mathrm{L_x}\, \epsilon^{\frac{1}{n}} \leq 0) \geq \mathbb{P}(\mathcal{A} \cap \mathcal{B}) \geq 1 - \mathbb{P}(\mathcal{A}^c) - \mathbb{P}(\mathcal{B}^c) \geq 1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0) - \beta_s$. This concludes the proof since $K^*_{\mathrm{RCP}} \leq 0$ implies that the feasible solution of RCP in (4.6) satisfies the barrier conditions in Theorem 9 with a confidence of at least $1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0) - \beta_s$. □

Remark 18. *According to [16, Remark 2], for a given number of samples N, the desired level of confidence β, number of decision variables $|d|$, and $\delta = \epsilon - \epsilon'$, a lower bound for N_0 can be computed as*

$$N_0 \geq \frac{\frac{\epsilon}{\delta}\ \ln \beta^{-1} + |d| - 1 - N(\frac{\delta}{2} + \epsilon')}{\delta}, \tag{4.39}$$

to ensure $\bar{\beta}_{\epsilon,\epsilon'}(N, N_0) \leq \beta$.

Based on the results in Theorem 12, we provide Algorithm 6 to systematically verify the safety of a stochastic system with an unknown dynamic. The coefficients of the barrier certificate satisfying conditions (4.2)-(4.4) are obtained in Step 4 of Algorithm 6.

Remark 19. *Remark that there is a trade off (pareto curve) between the expected number of iterations in* (4.33) *and the number of samples N (cf. Figure 4.4 in the case study). Hence, the user can decide how to pick N based on the number of expected iterations within which Algorithm 5 terminates.*

Algorithm 6 Data-driven safety verification

```
Require: Parameters $\beta \in (0, 1)$, $\beta_s \in (0, 1)$, $\epsilon, \epsilon' \in [0, 1]$, $\epsilon' \leq \epsilon$, $\mathrm{L_x} \in \mathbb{R}^+$, and the degree
    of the barrier certificate
1: Choose the number of samples $N$ according to Remark 19
2: Compute the number of test samples $N_0$ according to (4.39)
3: Compute $\hat{N}$ according to Theorem 11
4: Call Algorithm 5 to get $d^* = [K^*; \lambda^*; c^*; b^*]$
5: Safety Verifier: If $K^* + \mathrm{L_x}\epsilon^{\frac{1}{n}} \leq 0$, then $\mathbb{P}_w(S \models_H \Psi) \geq 1 - \frac{1+c^*H}{\lambda^*}$ with a confidence of
    at least $1 - \bar{\beta}_{\epsilon,\epsilon'}(N, N_0) - \beta_s$.
```

4.4.4 Two-Tank System Safety Verification: A Repetitive Scenario Solution

The main goal is to verify that the heights of both tanks stay away from the unsafe region within the time horizon $H = 5$ with an a-priori confidence 99%. Let us consider a barrier certificate with degree $k = 2$ in the polynomial form as $[\mathrm{h}_1; \mathrm{h}_2; 1]^T\mathrm{P}[\mathrm{h}_1; \mathrm{h}_2; 1] = b_0\mathrm{h}_1^2 + b_1\mathrm{h}_2^2 + b_2\mathrm{h}_1\mathrm{h}_2 + b_3\mathrm{h}_1 + b_4\mathrm{h}_2 + b_5$, where P is a matrix containing the coefficients of the barrier certificate. By enforcing $\|\mathrm{P}\| \leq 0.2$ and since $\|x\| \leq \sqrt{2} \times 10$, the Lipschitz constant is $\mathrm{L}_x = 11.03$ [83, Lemma 1].

We use Algorithm 6 to apply our proposed approach to this example. We select $\epsilon = 0.65 \times 10^{-4}$, $\epsilon' = 0.7\epsilon = 0.45 \times 10^{-4}$, $\beta_s = 0.001$, and $\beta = 0.009$. Then, one needs to select the number of samples N. This can be done by considering the trade-off between N and the number of the required iterations according to Remark 19 (cf. Fig. 4.4). For example, for 10^6, 10^5, and 5×10^4 number of samples, the expected required iterations are 1, 59, and 8283, respectively. Here, we select $N = 70000$ for which the expected number of iterations is 636. The number of test samples is computed as $N_0 = 1017100$ using (4.39). The value of $\hat{N}$ is computed as 400 according to Theorem 11 by considering the approximation error in (4.41) as $e = 0.05$ and enforcing $\hat{M} = 0.001$. The value of $\hat{M}$ was checked a posteriori using enough number of data. This provides a confidence of $1 - \beta_s$, where $\beta_s = 0.001$. In Step 4, we run Algorithm 5. The algorithm terminates in only 5 iterations, which is much less than the expected one (i.e. 636). This shows that our proposed approach is even more scalable in practice, and the theoretical upper bound is too conservative to cover the worst-case scenarios. The obtained optimal value of the successful iteration is $K^* = -0.1119$. According to Step 5 in Algorithm 6, since $K^* + \mathrm{L_x}\epsilon^{\frac{1}{n}} = -0.0230 \leq 0$, one can conclude that the water levels remain in the safe zone with a probability lower bounded of 0.90, and this statement is true with a confidence of at least 0.9985. Remark that the number of samples, which is 70000 here, is much less than 1337297, based on the results in [83] and [84], while our approach provides an even *better confidence* (i.e. 0.9985 in comparison to 0.99). The numerical experiments were conducted using CVX [37] under MATLAB. The total computation time here was 22 seconds, which is much less than 2 hours needed to run an SCP, as in [83] and [84], for 1337297 number of samples. Furthermore, Step 4 in Algorithm 6, the most expensive part of the algorithm, is natively parallelizable. Hence, our approach can be applied to large-scale systems.

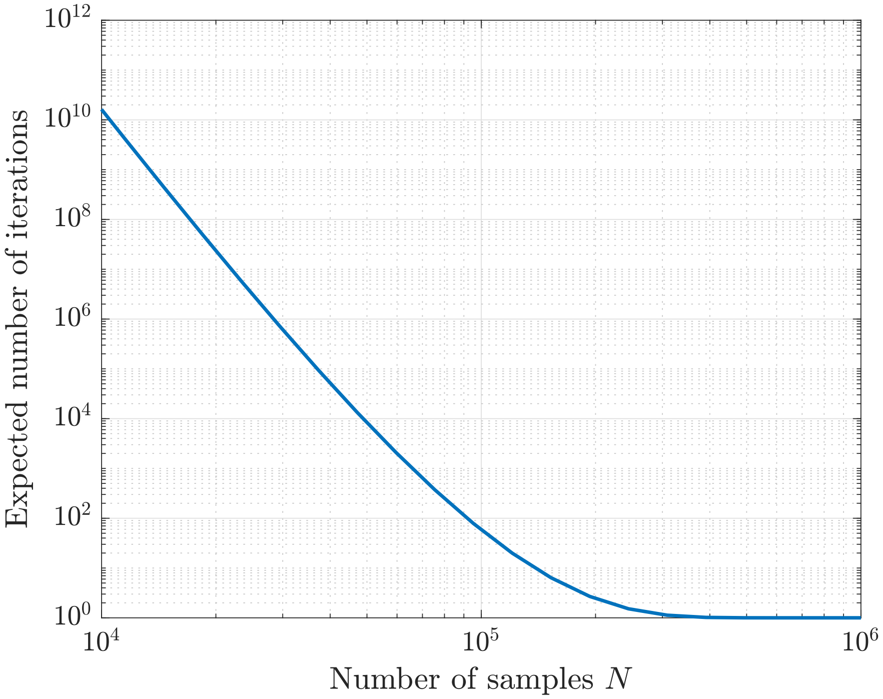


Figure 4.4: Pareto diagram of expected number of iterations versus N.

4.4.5 Discussion

We developed a data-driven verification approach based on the idea of repetitive scenario design. First, we constructed a repetitive scenario program based on an RCP characterizing the main safety problem as an optimization one. At each iteration of the proposed repetitive scheme, we first solve an SCP, then feed the optimizer to a feasibility oracle to check the feasibility of the SCP for a certain number of new samples before checking a rigorous safety condition on top of the feasibility one. Once both conditions (feasibility and safety) are satisfied, a lower bound can be computed for the probability of the safety of the stochastic system with unknown model by leveraging the optimal solutions of the successful iteration. Finally, the effectiveness of our approach in comparison with the existing results in [83, 84] was illustrated via a two-tank system.

4.5 Wait, Judge, and Repeat Approach

4.5.1 Overview

The overview of our approach for solving Problem 6 is depicted in Fig. 4.5. First, the stochastic safety problem is reformulated as a scenario convex program (SCP) by collecting N samples from the state set, and $\hat{N}$ samples from the realization of the noise. The constructed scenario program is solved, and the optimizer is assessed for N_0 new test samples. This assessment is done by checking the constraints after substituting the optimal solution of the SCP. An empirical mean over the violated constraints is computed as a violation measure. Solving the SCP for the collected samples and the feasibility assessment are executed for a specific number of iterations until the violation error is less than a desired threshold, which itself is less than an a posteriori computed violation probability. This a posteriori violation probability is calculated based on the exact number of support constraints. The process of solving SCP and checking its optimizer's feasibility continues until the feasibility condition is satisfied. Finally, a safety condition is checked on top of the feasibility assessment. If the safety condition is satisfied, the safety oracle tells us that the original stochastic system with unknown dynamic is safe with a probability lower bound computed using the optimizer achieved from the successful iteration. This probability lower bound is valid with a confidence, which is computed a posteriori as well using the number of support constraints.

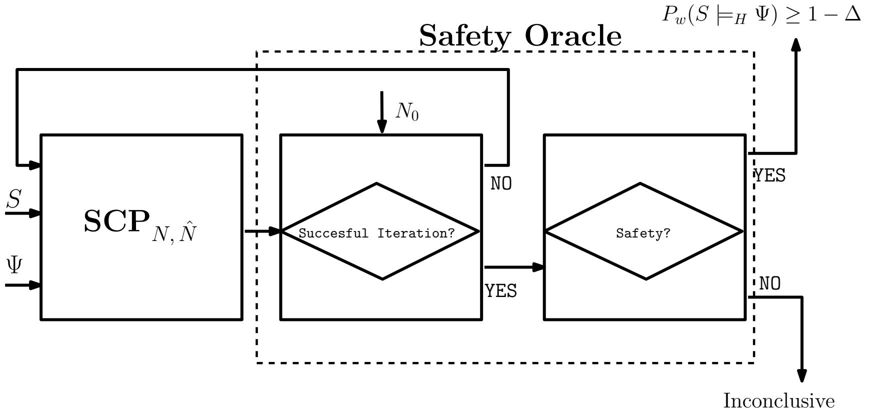


Figure 4.5: An overview of our wait, judge and repeat data-driven approach: The block on the left solves a scenario program $\mathrm{SCP}_{N,\hat{N}}$ using $N\hat{N}$ samples collected from the system at each iteration. The resulted optimizer of this scenario program is verified using N_0 new test samples in the middle block. The block on the right checks a condition whose satisfaction provides a probabilistic safety for the original stochastic system.

Finding an optimal solution for the RCP in (4.6) is too difficult because the map f and the probability measure $\mathbb{P}_w$ are both unknown. Furthermore, there are infinitely many constraints in the RCP since $x \in X$, where X is a continuous set. To address the issue of unknown $\mathbb{P}_w$ and the expectation term in g_4 in (4.7), we replace the expectation term with its empirical mean approximation by collecting $\hat{N}$ i.i.d. samples w_j, $j \in \{1, \dots, \hat{N}\}$, from $\mathbb{P}_w$ and construct a new RCP denoted by $\text{RCP}_{\hat{N}}$ as follows:

$$\text{RCP}_{\hat{N}}\colon \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \;\; \max\big(g_z(x,d), \bar{g}_4(x,w_j,d)\big) \leq 0, z \in \{1,\dots,3\}, \\ \qquad j \in \{1,\dots,\hat{N}\}, \forall x \in X, \lambda > 1, d = [K;\lambda;c;b], \end{cases} \tag{4.40}$$

where

$$\bar{g}_4(x,w_j,d) = \frac{1}{\hat{N}} \sum_{j=1}^{\hat{N}} \mathrm{B}(b, f(x,w_j)) - \mathrm{B}(b,x) - c - K + e. \tag{4.41}$$

Notice that the expectation term in (4.7) is approximated by the empirical mean in (4.41). This approximation introduces an error, which is introduced by e in (4.41).

Now, one can assign a probability distribution over the state set and collect N i.i.d. samples to solve $\text{RCP}_{\hat{N}}$ in (4.40). The data-set is denoted by:

$$\begin{aligned} \mathcal{D}_{N,\hat{N}} := \big\{ \, (x_i, w_j, f(x_i,w_j)) \subset X \times V_w \times X \mid \\ i \in \{1,\dots,N\}, j \in \{1,\dots,\hat{N}\} \big\}. \end{aligned} \tag{4.42}$$

Substituting these samples in $\text{RCP}_{\hat{N}}$ in (4.40) results in the following SCP denoted by $\text{SCP}_{N,\hat{N}}$:

$$\text{SCP}_{N,\hat{N}}\colon \begin{cases} \min\limits_{d} \quad K \\ \text{s.t.} \;\; \max\left(g_z(x_i,d), \bar{g}_4(x_i,w_j,d)\right) \leq 0, \\ \qquad \lambda > 1, z \in \{1,2,3\}, i \in \{1,\dots,N\}, \\ \qquad j \in \{1,\dots,\hat{N}\}, d = [K;\lambda;c;b]. \end{cases} \tag{4.43}$$

In the next section, we develop an approach to connect the solution of the SCP in (4.43) to the safety of stochastic system defined in Definition 9. In the next subsection, we show how a safety problem is cast as a repetitive scenario program (RSP) based on the SCP formulation in this subsection.

4.5.2 Wait, Judge, and Repeat Approach for Safety Verification of Stochastic Systems

The results in [89] develop an approach, which repeatedly solves an SCP and checks a condition over the optimal value of the SCP. If this condition is satisfied, the solution of the SCP is directly connected to the safety of the system. The main idea of this section is to judge the results before the repetition at each iteration, i.e., the user can compute a probability of violation a posteriori which potentially results in a lower number of samples. The confidence is computed a posteriori which is less conservative with respect to the approaches in [83], [88], and [89] (cf. Fig. 4.6).

We need to solve $\mathrm{SCP}_{N,\hat{N}}$ in (4.43) for several iterations. The obtained optimal values at each iteration, denoted by $d^*_{N,\hat{N}}$, are used to construct a feasibility problem denoted by $\mathrm{SCP}_{N_0,\hat{N}}$ using N_0 new test samples. At each iteration, a probability of violation is computed based on the exact number of support constraints at that iteration, which we denote it by ϵ_{wjr}. Now, we can define the successful iteration in the context of our proposed approach.

Definition 13. *An iteration is called a successful iteration, when the following condition is satisfied:*

$$\frac{\sum_{k=1}^{N_0} v_{N,\hat{N}}(k)}{N_0} \leq \epsilon_{wjr} \in [0, 1 - t_{\tilde{N}}], \tag{4.44}$$

where $t_{\tilde{N}}$ is the unique solution of

$$\frac{\beta}{N+1} \sum_{m=\tilde{N}}^{N} \binom{m}{\tilde{N}} t_{\tilde{N}}^{m-\tilde{N}} - \binom{N}{\tilde{N}} t_{\tilde{N}}^{N-\tilde{N}} = 0, \tag{4.45}$$

with $\tilde{N}$ being the number of support constraints, and $v_{N,\hat{N}}(k)$ being 1 if the k^{th} constraint, $k \in \{1, \ldots, N_0\}$, in $SCP_{N_0,\hat{N}}$ is not satisfied. Otherwise, it is 0. The optimizer of the successful iteration is denoted by d^*.

Next theorem, borrowed from [84, Theorem 3.4], shows that the optimal solution of the $\mathrm{RCP}_{\hat{N}}$ is a feasible solution for the RCP in (4.6) with a certain confidence.

Theorem 13. *Let d^*_s be a feasible solution of the $RCP_{\hat{N}}$ for some $e > 0$, and assume $Var\big(\mathrm{B}(b, f(x,w)\big) \leq \hat{M}$, $\forall x \in X$ with a given positive $\hat{M}$. Then, for any $\beta_s \in (0,1)$, one has $\mathbb{P}(d^*_s \models RCP) \geq 1 - \beta_s$, if the number of samples in the empirical mean satisfies $\hat{N} \geq \frac{\hat{M}}{e^2 \beta_s}$.*

Now, we construct a probabilistic bridge between the optimal value of the successful iteration according to Definition 13 and the safety of stochastic systems with unknown dynamics in Definition 4.1.

The next theorem connects the solution of a successful iteration and the original safety problem, and computes the violation probability and the confidence for this probability a posteriori.

Theorem 14. *Consider a stochastic system S as in (9), where f and $\mathbb{P}_w$ are* unknown, *and a safety specification Ψ as in Definition 10. Assume all functions in (4.7) are Lipschitz continuous with respect to x and with a Lipschitz constant $\mathrm{L_x}$. Choose $\hat{N}$ as in Theorem 13 based on a given confidence $1 - \beta_s, \beta_s \in (0,1)$. Suppose that for a given N and N_0, there is a successful iteration (cf. Definition 13), for which the optimal solution is $d^* = [K^*; \lambda^*; c^*; b^*]$. If*

$$K^* + \mathrm{L_x}\, G^{-1}(1 - t_{\tilde{N}}) \ \leq 0, \tag{4.46}$$

then the lower bound on the safety of the stochastic system is $1-\frac{1+c^*H}{\lambda^*}$ *with a confidence of at least* $1-\bar{\beta}(N,N_0,\tilde{N})-\beta_s$*, where* $t_{\tilde{N}}$ *is computed according to* (4.45)*, and*

$$\begin{aligned}\bar{\beta}(N,N_0,\tilde{N}) = & F_{beta}(N+(1-\epsilon_{wjr})N_0-\tilde{N}+1,\\ & \tilde{N}+\epsilon_{wjr}N_0; 1-\epsilon_{wjr}),\end{aligned}$$

where $\tilde{N}$ *is the number of support constraints for the successful iteration, and* ϵ_{wjr} *is a design parameter* $\epsilon_{wjr}\in[0,1-t_{\tilde{N}}]$.

Proof. A chance constraint program (CCP) can be constructed from the robust convex program $\text{RCP}_{\tilde{N}}$ in (4.40) as:

$$\text{CCP}_{\epsilon}\text{:}\begin{cases}\min\limits_{d} \quad K\\ \text{s.t. } \mathbb{P}\left(\max\left(g_z(x,d),\bar{g}_4(x,w_j,d)\right)\leq 0\right)\geq 1-\epsilon,\\ \qquad j\in\{1,\ldots,\hat{N}\}, z\in\{1,\ldots,3\},\\ \qquad \lambda>1, d=[K;\lambda;c;b],\end{cases} \tag{4.47}$$

for some violation probability $\epsilon>0$, where $g_z(x,d),\ z\in\{1,\ldots,3\}$, and $\bar{g}_4$ are defined in (4.7) and (4.28), respectively. According to [19], a probability violation is computed for an arbitrary number of samples N containing k support constraints as $\epsilon(k)=1-t(k)$, where $t(k)$ is the unique solution of

$$\frac{\beta}{N+1}\sum_{m=k}^{N}\binom{m}{k}\,t(k)^{\,m-k}-\binom{N}{k}\,t(k)^{\,N-k}=0.$$

for $k=\{0,\ldots,|d|\}$, where $|d|$ is the number of decision variables. For $k=\tilde{N}$, $\epsilon(\tilde{N})$ is represented by $1-t_{\tilde{N}}$ for the sake of simplicity. We formally define the probability of violation $V(d^*)$ as

$$\mathbb{P}\left(\max\left(g_z(x,d),\bar{g}_4(x,w_j,d)\right)>0\right).$$

Note that $V(d^*)$ is a random variable, for which the cumulative distribution function (CDF) is defined as:

$$F_v(w)=F_{beta}(\tilde{N},N-\tilde{N}-1;w),\ w\in[0,1], \tag{4.48}$$

for $\tilde{N}$ being the number of support constraints according to [16, Eq. (4)], where If we replace the CDF in the proof of Lemma 1 in [16] with (4.48), a new upper bound is computed for

$$\mathbb{P}\Big(\frac{\sum_{k=1}^{N_0}v_{N,\tilde{N}}(k)}{N_0}\leq\epsilon_{wjr}\ \wedge\ V(d^*)>1-t_{\tilde{N}}\Big)$$

as $\bar{\beta}(N, N_0, \tilde{N})(1 - H_{1,\epsilon_{wjr}}(N, N_0, \tilde{N}))$, where $\bar{\beta}(N, N_0, \tilde{N})$ is defined in the statement of the theorem, and

$$H_{1,\epsilon_{wjr}}(N, N_0, \tilde{N}) = 1 - \sum_{i=0}^{\lfloor \epsilon_{wjr} N_0 \rfloor} f_{bb}(N_0, \tilde{N}, N - \tilde{N} + 1; i).$$

Substituting this new upper bound in the proof of Theorem 3 in [16] results in

$$\mathbb{P}\big(d^* \models \mathrm{CCP}_{1-t_{\tilde{N}}}\big) \geq 1 - \bar{\beta}(N, N_0, \tilde{N}),$$

where $d^* = [K^*; \lambda^*; c^*; b^*]$ is the optimal solution of the successful iteration. The rest of the proof is similar to that of Theorem 3 in [89] by substituting $1 - t_{\tilde{N}}$ for ϵ.

□

Remark 20. *Similar to the reasoning in [18, Section 5] for a given number of samples N, a desired level of confidence β, number of support constraints $\tilde{N}$, and $\delta = 1 - t_{\tilde{N}} - \epsilon_{wjr}$, a lower bound for N_0 can be computed as*

$$N_0 \geq \frac{\frac{\epsilon}{\delta}\ \ln \beta^{-1} + \tilde{N} - 1 - N(\frac{\delta}{2} + \epsilon_{wjr})}{\delta}, \tag{4.49}$$

to ensure $\bar{\beta}(N, N_0, \tilde{N}) \leq \beta$.

The next corollary provides an upper bound on the number of iterations required for the satisfaction of (4.44).

Corollary 4. *For large values of N_0, the expected number of iterations in order to satisfy* (4.44) *is approximated by*

$$\frac{1}{1 - \beta_{\epsilon_{wjr}}(N, N_0, \tilde{N})}, \tag{4.50}$$

where $\beta_{\epsilon_{wjr}}(N, N_0, \tilde{N}) = 1 - \sum_{i=\tilde{N}}^{N} \binom{N}{i} {\epsilon_{wjr}}^i (1 - \epsilon_{wjr})^{N-i}$.

Proof. By substituting $\tilde{N}$ and ϵ_{wjr} for the number of decision variables d and $\epsilon' \in [0, \epsilon]$, respectively, the upper bound on the expected number of iterations is computed as $\frac{1}{1 - H_{1,\epsilon_{wjr}}(N, N_0, \tilde{N})}$ according to the proof of Theorem 3 in [16]. Then similar to the proof of Corollary 1 in [16], one can readily see that for large values of N_0, $1 - H_{1,\epsilon_{wjr}}(N, N_0, \tilde{N})$ converges to $F_{beta}(\tilde{N}, N - \tilde{N} + 1; \epsilon_{wjr}) = 1 - \beta_{\epsilon_{wjr}}(N, N_0, \tilde{N})$. □

Based on the results in Theorem 14, we provide Algorithm 7 to systematically verify the safety of a stochastic system with an unknown dynamics.

A pareto curve can be plotted for the expected number of iterations versus the number of samples N using (4.50). This enables the user to pick N based on the number of expected iterations within which (4.44) is satisfied.

Algorithm 7 Wait, Judge, and Repeat (WJR) Algorithm

```
Require: Number of samples $N$
1: Compute $\hat{N}$ based on Theorem 13 for a desired confidence parameter $\beta_s$
2: Collect $\hat{N}$ samples $w_j, j \in [1, \dots, \hat{N}]$, from $\mathbb{P}_w$
3: Collect $N$ samples $x_i, i \in [1, \dots, N]$, from the state set
4: Compute number of support constraints $\tilde{N}$
5: Compute the probability violation $1 - t_{\tilde{N}}$ according to Definition 13
6: Solve the $\text{SCP}_{N,\hat{N}}$ in (4.43) using the collected data in Step 1 and Step 2, and obtain
   the optimizer $d^*_{N,\hat{N}}$
7: Compute the number of test samples $N_0$ according to (4.39)
8: Construct the feasibility problem $\text{SCP}_{N_0,\hat{N}}$ using $N_0$ new samples by feeding the optimal
   values from Step 6 to the scenario program in (4.43)
9: Check $\frac{\sum_{k=1}^{N_0} v_{N,\hat{N}}(k)}{N_0} \leq \epsilon_{wjr}$
10: If the above inequality is satisfied, then $d^* = d^*_{N,\hat{N}}$, otherwise go to Step 2.
11: Safety Oracle: If $K^* + \mathrm{L}_{\mathrm{x}}(1 - t_{\tilde{N}})^{\frac{1}{n}} \leq 0$, then $\mathbb{P}_w(S \models_H \Psi) \geq 1 - \frac{1+c^*H}{\lambda^*}$ with a confidence
    of at least $1 - \bar{\beta}(N, N_0, \tilde{N}) - \beta_s$.
```

4.5.3 Two-Tank System Safety Verification: A Wait, Judge, and Repeat Solution

The main goal is to verify that the heights of both tanks stay away from the unsafe region within the time horizon $H = 5$ with an a-priori confidence 99%. Let us consider a barrier certificate with degree $k = 2$ in the polynomial form as $[\mathrm{h}_1; \mathrm{h}_2; 1]^T \mathrm{P} [\mathrm{h}_1; \mathrm{h}_2; 1] = b_0 \mathrm{h}_1^2 + b_1 \mathrm{h}_2^2 + b_2 \mathrm{h}_1 \mathrm{h}_2 + b_3 \mathrm{h}_1 + b_4 \mathrm{h}_2 + b_5$, where P is a 3×3 matrix. By enforcing $\|P\| \leq 0.2$ and since $\|x\| \leq \sqrt{2} \times 10$, the rquired Lipschitz constant can be computed as $\mathrm{L}_x = 10.03$ [83, Lemma 1].

We use Algorithm 7 to apply our proposed approach to this example. We select $N = 70000$. For chosen 100 number of samples, the number of support constraints is computed as $\tilde{N} = 2$, so the violation probability is computed a posteriori as 0.1129×10^{-3}. The value of $\hat{N}$ is computed as 400 according to Theorem 13 by considering the approximation error in (4.28) as $e = 0.05$ and enforcing $\hat{M} = 0.001$. This provides a confidence of $1 - \beta_s$, where $\beta_s = 0.001$. The number of test samples is computed as $N_0 = 294780$ using (4.39). It is much less than 1017100 reported in [89]. This is because the lower bound in (4.39) uses the exact value of support constraints rather than the total number of decision variables. It results in faster runs of the algorithm at each iteration. The number of required iterations based on Corollary 4 is computed as 3, which is much lower than 636 in [89]. The obtained optimal value of the successful iteration, which occurs only after one iteration, is $K^* = -0.1093$. According to Step 11 in Algorithm 7, since $K^* + \mathrm{L}_{\mathrm{x}} \epsilon^{\frac{1}{n}} = -0.004 \leq 0$, one can conclude that the water levels remain in the safe zone with a probability lower bound of 0.90 and a confidence of at least 0.9999, which is better than 0.9985 in [89] and than

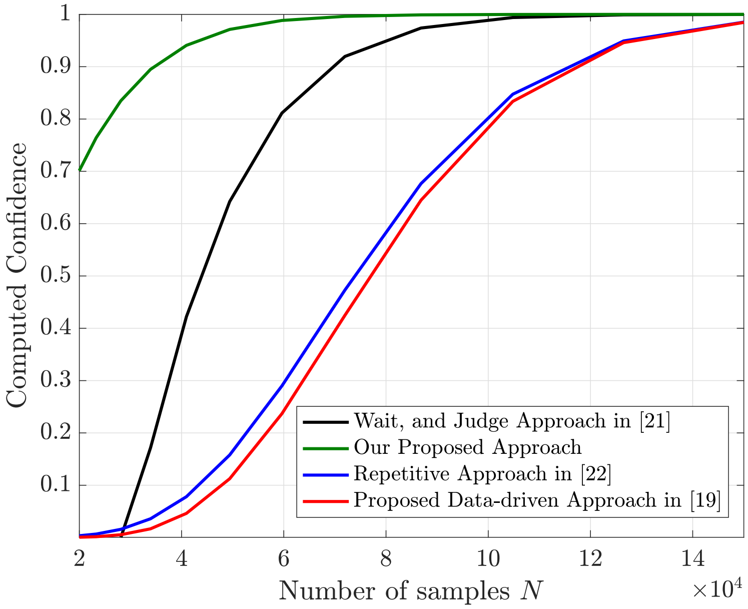


Figure 4.6: Computed confidence versus number of samples N.

0.99 in [84] and [88]. For the sake of fair comparison between the calculated confidences in the mentioned results, the computed confidence against number of samples is illustrated in Fig 4.6 for fixed $\epsilon = 0.1129 \times 10^{-3}$. As it can be seen, computed confidence using our approach outperforms significantly those in [84, 88, 89]. The numerical experiments were performed using CVX [37] under MATLAB. The total computation time here was 5 seconds, which is less than 2 hours needed to run the SCP in [83] and [84] for 1337297 number of samples, and less than 22 seconds reported in [88].

4.5.4 Discussion

We developed a data-driven verification approach based on a so-called wait, judge, and repeat framework. We iteratively solved an SCP resulted from substituting a finite number of samples in an RCP, which is equivalent to a safety problem. A feasibility condition is checked at each iteration over the optimizer of the SCP in that iteration. If this condition is satisfied, a concrete safety condition is checked over the optimal value of the successful iteration. If the safety condition is satisfied too, a lower bound is computed for the safety probability of the stochastic system with unknown model using the optimizer of the successful iteration. Both confidence and violation probability were computed a posteriori in this framework. Finally, the effectiveness of our approach was shown via a two-tank system.

Chapter 5

Conclusions and Future Works

5.1 Conclusions

In this thesis, we discuss the development of data-driven and machine learning techniques to either verify temporal specifications, including safety, on the behavior of unknown or partially unknown stochastic dynamical systems or synthesize controllers to enforce these specifications on the system's behavior.

In Chapter 2, we proposed a two-layer probabilistic framework to provide a measure of satisfaction for signal temporal logic properties when we only have access to a partially known parameterized model of a stochastic system. First, we leveraged an machine learning algorithm called Bayesian inference, to update our prior knowledge of the unknown parameters using collected data. Then, we computed the satisfaction measure by integrating the updated distribution over the feasible set of parameters for which the desired STL specification is guaranteed to be satisfied.

In Chapter 3, we investigated the satisfaction of the safety property for a fully unknown stochastic system. First, we reformulated a safety problem for stochastic systems as an RCP. Solving this RCP was not straightforward since the state resides in an infinite set, furthermore there is an expectation term in one of the constraints. We collected data from the system and constructed an SCP using this finite number of samples. Then, we developed a theorem to establish a connection between the solution of the obtained SCP and the safety of the original stochastic system.

Finally, in Chapter 4, we developed three approaches to mitigate the sample complexity of the proposed technique introduced in Chapter 3. First, we developed a so-called wait and judge approach, where we evaluate a safety condition on the optimizer of the SCP for an arbitrary low number of samples. This condition is based on the number of support constraints. Support constraints are the ones that affect the optimal value of an optimization problem. Second, we solved an SCP repeatedly until a feasibility condition on its optimizer was satisfied. It is guaranteed that always there is a successful iteration. A safety condition is then checked on the optimizer of the successful iteration. If this condition is satisfied, a lower bound on the safety of the stochastic system is computed by leveraging the optimizer of the successful iteration. Third, we combined the above methods and developed a so-called wait, judge, and repeat approach that significantly reduces number of required samples.

5.2 Future Directions

Next, we will explore potential directions that are related to data-driven and machine learning techniques for conducting verification and synthesis tasks. We strongly believe that these directions have the potential to drive forward research in safety-critical system design.

- **Alleviating the sample complexity.** The method developed in Chapter 3 is data-hungry as it incorporates the maximum Lipschitz constant of the constraints in the equivalent RCP (Robust Convex Programming) of the safety problem, aiming to cover worst-case scenarios. We proposed three techniques in Chapter 4 in order to reduce the sample complexity. We believe that further reduction in sample complexity is still possible, both theoretically and in terms of implementation. One potential direction is adaptive sampling, where samples are taken only when necessary to satisfy the constraints in different partitions of the state set. Another potential direction would be developing approaches to reduce the number of samples required to connect the solution of an SCP to its CCP equivalent of an RCP. This can significantly lower the number of samples needed in our proposed approach. Furthermore, the development of optimization algorithms that efficiently solve optimization problems subject to a large number of constraints holds great promise. One potential approach could involve converting an optimization problem with a large number of constraints into several optimization problems, each subject to a reduced number of constraints. One can investigate how to reach the global minimum using these individual solutions. From an implementation point of view, two of our proposed methods in Chapter 4, namely the repetitive approach in Section 4.4 and the wait, judge, and repeat approach in Section 4.5, are highly parallelizable. Therefore, parallelization algorithms and the utilization of multi-core CPUs and GPUs have the potential to greatly enhance their efficiency.

- **Developing data-driven closure certificates.** Significant improvements have been made to the application of barrier certificates, now encompassing temporal specifications expressed as ω-automata. This enhanced approach, referred to as the state-triplet approach, leverages barrier certificates to create a clear distinction between successive transitions involving three states within the ω-automaton, thus preventing the occurrence of accepting runs. Moreover, the state-triplet approach has found practical utility in the realms of verification and synthesis across a broader range of dynamical systems. To enable the search for these transition invariants, the concept of closure certificates is introduced as a functional analog. Closure certificates can be searched using SOS programming and SMT solvers, similar to transition invariants, and provide a means to verify and synthesize systems against ω-regular properties. The application of these techniques necessitates knowledge of the system's model, which is often unavailable in numerous real-world applications. Therefore, computing these closure certificates using only data is a valuable direction that has the potential to extend our proposed data-driven techniques to a wide range of properties, including even more complicated specifications.

- **Data-Driven Verification of Stochastic Nonlinear Systems with Signal Temporal Logic Constraints** Given a prior density function over the set of parameters, denoted by $p(\theta)$ and an input-output data set $\mathcal{D}$, a posterior distribution $p(\theta \mid \mathcal{D})$ can be inferred for θ by

  $$p(\theta \mid \mathcal{D}) = \frac{p(\mathcal{D} \mid \theta)\, p(\theta)}{\int_{\Theta} p(\mathcal{D} \mid \theta)\, p(\theta) d\theta},$$

  where $p(\mathcal{D} \mid \theta)$ is

  $$p(\mathcal{D} \mid \theta) = \frac{1}{|\Sigma_{\tilde{\mathbf{y}}}(\theta)|^{\frac{1}{2}} (2\pi)^{\frac{m\mathrm{N}_{\mathrm{exp}}}{2}}} \exp\left\{ -\frac{1}{2} (\tilde{\mathbf{y}} - \bar{\mathbf{y}}(\theta))^T \, \Sigma_{\tilde{\mathbf{y}}}(\theta)^{-1} (\tilde{\mathbf{y}} - \bar{\mathbf{y}}(\theta)) \right\}.$$

  However, computing $\bar{\mathbf{y}}(\theta)$ and $\Sigma_{\tilde{\mathbf{y}}}(\theta)$ as defined in Proposition 1, is challenging when the original system is a nonlinear system. Therefore, it is worth investigating how one can tackle this challenge.

- **Data-Driven Verification of Stochastic Systems with Signal Temporal Logic Constraint under Unknown Noise Distribution** In Chapter 2, we assumed that measurement noise and process noise have zero-mean Gaussian distributions. Eliminating this assumption can affect some parts of our proposed approach, including computing $p(\theta \mid \mathcal{D})$. Therefore, it is valuable to explore how one can solve the verification and synthesis problem when the distribution of noise is unknown. Another interesting research direction is to study the robustness of the computations with respect to uncertainties in the distribution of random variables that affect the system's evolution.

- **Software development to implement data-driven approaches** There have been substantial activities related to software development and benchmarking the tools on stochastic systems. Examples of these tools include FAUST [95], StocHy [20], Amytiss [61], SySCoRe [105], and Genie [65]. Such tools on stochastic systems are participating in the ARCH friendly competition [3] to apply the tools on standard benchmarks. There is also a demand to develop efficient software tools that implement data-driven approaches and apply them on a standard set of benchmarks to demonstrate and compare their efficiency.

- **Extending data-driven approaches for simultaneous safety and security of unknown CPSs.** There have been model-based approaches in the literature that consider designing secure cyber-physical systems using the notion of a barrier certificate when the system model is known. For example, the results in [64] demonstrate a model-based approach developed by the authors to design confidentially secure cyber-physical systems. One potential direction is to design a data-driven framework that tackles both safety and security problems in CPSs simultaneously by utilizing data collected from the system.

Bibliography

[1] Alessandro Abate. Formal verification of complex systems: model-based and data-driven methods. In *Proceedings of the 15th ACM-IEEE International Conference on Formal Methods and Models for System Design*, pages 91–93. ACM, 2017.

[2] Alessandro Abate, Daniele Ahmed, Mirco Giacobbe, and Andrea Peruffo. Formal synthesis of lyapunov neural networks. *IEEE Control Systems Letters*, 5(3):773–778, 2020.

[3] Alessandro Abate, Henk Blom, Joanna Delicaris, Sofie Haesaert, Arnd Hartmanns, Birgit van Huijgevoort, Abolfazl Lavaei, Hao Ma, Mathis Niehage, Anne Remke, et al. Arch-comp22 category report: Stochastic models. In *Proceedings of 9th International Workshop on Applied*, volume 90, pages 113–141, 2022.

[4] Matthias Althoff, Markus Koschi, and Stefanie Manzinger. Commonroad: Composable benchmarks for motion planning on roads. In *2017 IEEE Intelligent Vehicles Symposium (IV)*, pages 719–726. IEEE, 2017.

[5] Erling D Andersen and Knud D Andersen. The mosek interior point optimizer for linear programming: an implementation of the homogeneous algorithm. In *High performance optimization*, pages 197–232. Springer, 2000.

[6] Christel Baier and Joost-Pieter Katoen. *Principles of model checking.* MIT press, 2008.

[7] Ezio Bartocci, Luca Bortolussi, and Guido Sanguinetti. Data-driven statistical learning of temporal logic properties. In *International Conference on Formal Modeling and Analysis of Timed Systems*, pages 23–37. Springer, 2014.

[8] Calin Belta, Boyan Yordanov, and Ebru Aydin Gol. *Formal methods for discrete-time dynamical systems*, volume 15. Springer, 2017.

[9] Julian Berberich, Johannes Köhler, Matthias A Muller, and Frank Allgower. Data-driven model predictive control with stability and robustness guarantees. *IEEE Transactions on Automatic Control*, 2020.

[10] Dirk Beyer, Matthias Dangl, and Philipp Wendler. A unifying view on SMT-based software verification. *Journal of Automated Reasoning*, 60(3):299–335, 2018.

[11] Dirk Beyer and M Erkan Keremoglu. CPAchecker: A tool for configurable software verification. In *International Conference on Computer Aided Verification*, pages 184–190. Springer, 2011.

[12] Christopher M. Bishop. *Pattern Recognition and Machine Learning*. Springer, 2006.

[13] Sergiy Bogomolov, Christian Schilling, Ezio Bartocci, Gregory Batt, Hui Kong, and Radu Grosu. Abstraction-based parameter synthesis for multiaffine systems. In *Haifa Verification Conference*, pages 19–35. Springer, 2015.

[14] Urs Borrmann, Li Wang, Aaron D Ames, and Magnus Egerstedt. Control barrier certificates for safe swarm behavior. *IFAC-PapersOnLine*, 48(27):68–73, 2015.

[15] Olivier Bouissou, Eric Goubault, Sylvie Putot, Aleksandar Chakarov, and Sriram Sankaranarayanan. Uncertainty propagation using probabilistic affine forms and concentration of measure inequalities. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 225–243. Springer, 2016.

[16] Giuseppe C Calafiore. Repetitive scenario design. *IEEE Transactions on Automatic Control*, 62(3):1125–1137, 2016.

[17] Giuseppe C Calafiore and Marco C Campi. The scenario approach to robust control design. *IEEE Transactions on automatic control*, 51(5):742–753, 2006.

[18] Giuseppe Carlo Calafiore. Random convex programs. *SIAM Journal on Optimization*, 20(6):3427–3464, 2010.

[19] Marco C Campi and Simone Garatti. Wait-and-judge scenario optimization. *Mathematical Programming*, 167(1):155–189, 2018.

[20] Nathalie Cauchi and Alessandro Abate. Stochy-automated verification and synthesis of stochastic processes. In *Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control*, pages 258–259, 2019.

[21] Ya-Chien Chang, Nima Roohi, and Sicun Gao. Neural Lyapunov control. In *Advances in Neural Information Processing Systems*, pages 3240–3249, 2019.

[22] Yi Chou and Sriram Sankaranarayanan. Bayesian parameter estimation for nonlinear dynamics using sensitivity analysis. In *28th International Joint Conference on Artificial Intelligence*, pages 5708–5714. AAAI Press, 2019.

[23] Andrew Clark. Control barrier functions for stochastic systems. *Automatica*, 130:109688, 2021.

[24] Edmund M Clarke and Paolo Zuliani. Statistical model checking for cyber-physical systems. In *International Symposium on Automated Technology for Verification and Analysis*, pages 1–12. Springer, 2011.

[25] Jeremy Coulson, John Lygeros, and Florian Dörfler. Distributionally robust chance constrained data-enabled predictive control. *arXiv:2006.01702*, 2020.

[26] Charles Dawson, Zengyi Qin, Sicun Gao, and Chuchu Fan. Safe nonlinear control using robust neural lyapunov-barrier functions. In *Conference on Robot Learning*, pages 1724–1735. PMLR, 2022.

[27] Verband der Automobilindustrie. Lane keeping assist systems. `https://www.vda.de/en/topics/safety-and-standards/lkas/lane-keeping-assist-systems.html`, 2020.

[28] Patricia Derler, Edward A Lee, and Alberto Sangiovanni Vincentelli. Modeling cyber–physical systems. *Proceedings of the IEEE*, 100(1):13–28, 2011.

[29] Peyman Mohajerin Esfahani, Tobias Sutter, and John Lygeros. Performance bounds for the scenario approach and an extension to a class of non-convex programs. *IEEE Transactions on Automatic Control*, 60(1):46–58, 2014.

[30] Georgios E Fainekos and George J Pappas. Robustness of temporal logic specifications. In *Formal Approaches to Software Testing and Runtime Verification*, pages 178–192. Springer, 2006.

[31] Samira S Farahani, Rupak Majumdar, Vinayak S Prabhu, and Sadegh Soudjani. Shrinking horizon model predictive control with signal temporal logic constraints under stochastic disturbances. *IEEE Transactions on Automatic Control*, 2018.

[32] Samira S. Farahani, Sadegh Soudjani, Rupak Majumdar, and Carlos Ocampo-Martinez. Robust model predictive control with signal temporal logic constraints for Barcelona wastewater system. *IFAC-PapersOnLine*, 50(1):6594–6600, 2017. 20th IFAC World Congress.

[33] Samira S Farahani, Sadegh Soudjani, Rupak Majumdar, and Carlos Ocampo-Martinez. Formal controller synthesis for wastewater systems with signal temporal logic constraints: The Barcelona case study. *Journal of Process Control*, 69:179–191, 2018.

[34] Angelos Georghiou, Angelos Tsoukalas, and Wolfram Wiesemann. Robust dual dynamic programming. *Operations Research*, 2019.

[35] Antoine Girard. Reachability of uncertain linear systems using zonotopes. In *International Workshop on Hybrid Systems: Computation and Control*, pages 291–305. Springer, 2005.

[36] Antoine Girard, Gregor Gössler, and Sebti Mouelhi. Safety controller synthesis for incrementally stable switched systems using multiscale symbolic models. *IEEE Transactions on Automatic Control, vol. 61, no. 6, pp. 1537–1549*, 2016.

[37] Michael Grant and Stephen Boyd. CVX: Matlab software for disciplined convex programming, version 2.1. `http://cvxr.com/cvx`, March 2014.

[38] Sofie Haesaert, Petter Nilsson, and Sadegh Soudjani. Formal multi-objective synthesis of continuous-state MDPs. In *2021 American Control Conference (ACC)*, pages 3428–3433. IEEE, 2021.

[39] Sofie Haesaert and Sadegh Soudjani. Robust dynamic programming for temporal logic control of stochastic systems. *IEEE Transactions on Automatic Control*, 66(6):2496–2511, 2020.

[40] Sofie Haesaert, Sadegh Soudjani, and Alessandro Abate. Temporal logic control of general Markov decision processes by approximate policy refinement. *IFAC-PapersOnLine*, 51(16):73–78, 2018.

[41] Sofie Haesaert, Paul MJ Van den Hof, and Alessandro Abate. Data-driven property verification of grey-box systems by Bayesian experiment design. In *2015 American Control Conference (ACC)*, pages 1800–1805. IEEE, 2015.

[42] Sofie Haesaert, Paul MJ Van den Hof, and Alessandro Abate. Automated experiment design for data-efficient verification of parametric Markov decision processes. In *International Conference on Quantitative Evaluation of Systems*, pages 259–274. Springer, 2017.

[43] Sofie Haesaert, Paul MJ Van den Hof, and Alessandro Abate. Data-driven and model-based verification via Bayesian identification and reachability analysis. *Automatica*, 79:115–126, 2017.

[44] Ernst Moritz Hahn, Mateo Perez, Sven Schewe, Fabio Somenzi, Ashutosh Trivedi, and Dominik Wojtczak. Omega-regular objectives in model-free reinforcement learning. In *International conference on tools and algorithms for the construction and analysis of systems*, pages 395–412. Springer, 2019.

[45] Shuo Han, Ufuk Topcu, and George J Pappas. A sublinear algorithm for barrier-certificate-based data-driven model validation of dynamical systems. In *54th IEEE conference on decision and control (CDC)*, pages 2049–2054, 2015.

[46] Mohammadhosein Hasanbeig, Alessandro Abate, and Daniel Kroening. Logically-constrained neural fitted Q-iteration. In *Proceedings of the 18th International Conference on Autonomous Agents and MultiAgent Systems*, pages 2012–2014. International Foundation for Autonomous Agents and Multiagent Systems, 2019.

[47] Martin Herceg, Michal Kvasnica, Colin N Jones, and Manfred Morari. Multi-Parametric Toolbox 3.0. In *2013 European Control Conference (ECC)*, pages 502–510. IEEE, 2013.

[48] MA Hernández. Chebyshev's approximation algorithms and applications. *Computers & Mathematics with Applications*, 41(3-4):433–445, 2001.

[49] Pushpak Jagtap, George J Pappas, and Majid Zamani. Control barrier functions for unknown nonlinear systems using Gaussian processes. In *2020 59th IEEE Conference on Decision and Control (CDC)*, pages 3699–3704. IEEE, 2020.

[50] 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.

[51] Pushpak Jagtap, Sadegh Soudjani, and Majid Zamani. Formal synthesis of stochastic systems via control barrier certificates. *IEEE Transactions on Automatic Control*, pages 1–1, 2020.

[52] Svante Janson. Large deviations for sums of partly dependent random variables. *Random Structures & Algorithms*, 24(3):234–248, 2004.

[53] Takafumi Kanamori and Akiko Takeda. Worst-case violation of sampled convex programs for optimization with uncertainty. *Journal of Optimization Theory and Applications*, 152(1):171–197, 2012.

[54] Milad Kazemi, Rupak Majumdar, Mahmoud Salamati, Sadegh Soudjani, and Ben Wooding. Data-driven abstraction-based control synthesis. *arXiv preprint arXiv:2206.08069*, 2022.

[55] Milad Kazemi, Mateo Perez, Fabio Somenzi, Sadegh Soudjani, Ashutosh Trivedi, and Alvaro Velasquez. Translating omega-regular specifications to average objectives for model-free reinforcement learning. In *Proc. of the 21st International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2022),*, 2022.

[56] Milad Kazemi and Sadegh Soudjani. Formal policy synthesis for continuous-state systems via reinforcement learning. In *Integrated Formal Methods: 16th International Conference, IFM 2020, Lugano, Switzerland, November 16–20, 2020, Proceedings 16*, pages 3–21. Springer, 2020.

[57] Joris Kenanian, Ayca Balkan, Raphael M Jungers, and Paulo Tabuada. Data driven stability analysis of black-box switched linear systems. *Automatica*, 109:108533, 2019.

[58] Yonit Kesten, Amir Pnueli, and Lion Raviv. Algorithmic verification of linear temporal logic specifications. In *International Colloquium on Automata, Languages, and Programming*, pages 1–16. Springer, 1998.

[59] Harold J Kushner. Stochastic stability and control. Technical report, Brown Univ Providence RI, 1967.

[60] Morteza Lahijanian, Sean B Andersson, and Calin Belta. Formal verification and synthesis for discrete-time stochastic systems. *IEEE Transactions on Automatic Control*, 60(8):2031–2045, 2015.

[61] Abolfazl Lavaei, Mahmoud Khaled, Sadegh Soudjani, and Majid Zamani. AMYTISS: Parallelized automated controller synthesis for large-scale stochastic systems. In *Computer Aided Verification: 32nd International Conference, CAV 2020, Los Angeles, CA, USA, July 21–24, 2020, Proceedings, Part II 32*, pages 461–474. Springer, 2020.

[62] Abolfazl Lavaei, Mateo Perez, Milad Kazemi, Fabio Somenzi, Sadegh Soudjani, Ashutosh Trivedi, and Majid Zamani. Compositional reinforcement learning for discrete-time stochastic control systems. *arXiv preprint arXiv:2208.03485*, 2022.

[63] Abolfazl Lavaei, Fabio Somenzi, Sadegh Soudjani, Ashutosh Trivedi, and Majid Zamani. Formal controller synthesis for continuous-space MDPs via model-free reinforcement learning. in ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS), 2020.

[64] Siyuan Liu and Majid Zamani. Verification of approximate opacity via barrier certificates. *IEEE Control Systems Letters*, 5(4):1369–1374, 2021.

[65] Rupak Majumdar, Kaushik Mallik, Mateusz Rychlicki, Anne-Kathrin Schmuck, and Sadegh Soudjani. A flexible toolchain for symbolic rabin games under fair and stochastic uncertainties. In *International Conference on Computer Aided Verification*, pages 3–15. Springer, 2023.

[66] Rupak Majumdar, Kaushik Mallik, and Sadegh Soudjani. Symbolic controller synthesis for Büchi specifications on stochastic systems. In *Proceedings of the 23rd International Conference on Hybrid Systems: Computation and Control*, pages 1–11, 2020.

[67] Rupak Majumdar, Mahmoud Salamati, and Sadegh Soudjani. Neural abstraction-based controller synthesis and deployment. *arXiv preprint arXiv:2307.03783*, 2023.

[68] Oded Maler and Dejan Nickovic. Monitoring temporal properties of continuous signals. In *Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems*, pages 152–166. Springer, 2004.

[69] Vishnu Murali, Ashutosh Trivedi, and Majid Zamani. A scenario approach for synthesizing k-inductive barrier certificates. *IEEE Control Systems Letters*, 6:3247–3252, 2022.

[70] Luyao Niu, Hongchao Zhang, and Andrew Clark. Safety-critical control synthesis for unknown sampled-data systems via control barrier functions. In *2021 60th IEEE Conference on Decision and Control (CDC)*, pages 6806–6813. IEEE, 2021.

[71] Gareth D Padfield. *Helicopter flight dynamics*. Wiley Online Library, 2008.

[72] Sriram Pemmaraju and Steven Skiena. *Computational Discrete Mathematics: Combinatorics and Graph Theory with Mathematica®*. Cambridge university press, 2003.

[73] Swantje Plambeck, Görschwin Fey, and Schyga. Decision tree models of continuous systems. In *27th International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2022.

[74] Stephen Prajna and Ali Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *International Workshop on Hybrid Systems: Computation and Control*, pages 477–492. Springer, 2004.

[75] Stephen Prajna, Ali Jadbabaie, and George J Pappas. A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control*, 52(8):1415–1428, 2007.

[76] Vasumathi Raman, Alexandre Donzé, Dorsa Sadigh, Richard M Murray, and Sanjit A Seshia. Reactive synthesis from signal temporal logic specifications. In *Proceedings of the 18th International Conference on Hybrid Systems: Computation and Control*, pages 239–248. ACM, 2015.

[77] José A Ramos and P Lopes Dos Santos. Mathematical modeling, system identification, and controller design of a two tank system. In *46th IEEE CDC*, pages 2838–2843. IEEE, 2007.

[78] Hadi Ravanbakhsh and Sriram Sankaranarayanan. Learning control Lyapunov functions from counterexamples and demonstrations. *Autonomous Robots*, 43(2):275–307, 2019.

[79] Alexander Robey, Haimin Hu, Lars Lindemann, Hanwen Zhang, Dimos V Dimarogonas, Stephen Tu, and Nikolai Matni. Learning control barrier functions from expert demonstrations. *arXiv:2004.03315*, pages 3717–3724, 2020.

[80] Alexander Robey, Lars Lindemann, Stephen Tu, and Nikolai Matni. Learning robust hybrid control barrier functions for uncertain systems. *IFAC-PapersOnLine*, 54(5):1–6, 2021.

[81] Dorsa Sadigh and Ashish Kapoor. Safe control under uncertainty with probabilistic signal temporal logic. 2016.

[82] Sadra Sadraddini and Calin Belta. Formal guarantees in data-driven model identification and control synthesis. In *Proceedings of the 21st International Conference on Hybrid Systems: Computation and Control*, pages 147–156, 2018.

[83] Ali Salamati, Abolfazl Lavaei, Sadegh Soudjani, and Majid Zamani. Data-driven safety verification of stochastic systems. *7th IFAC Conference on Analysis and Design of Hybrid Systems*, 2021.

[84] Ali Salamati, Abolfazl Lavaei, Sadegh Soudjani, and Majid Zamani. Data-driven verification and synthesis of stochastic systems through barrier certificates. *Automatica, to appear*, 2023.

[85] Ali Salamati, Sadegh Soudjani, and Zamani. Data-driven verification under signal temporal logic constraints. in 21th IFAC World Congress, 2020.

[86] Ali Salamati, Sadegh Soudjani, and Majid Zamani. Data-driven verification under signal temporal logic constraints. *21st IFAC World Congress*, 2020.

[87] Ali Salamati, Sadegh Soudjani, and Majid Zamani. Data-driven verification of stochastic linear systems with signal temporal logic constraints. *Automatica*, 131:109781, 2021.

[88] Ali Salamati and Majid Zamani. Data-driven safety verification of stochastic systems via barrier certificates: A wait-and-judge approach. *The 4th Annual Learning for Dynamics and Control Conference*, 2022.

[89] Ali Salamati and Majid Zamani. Safety verification of stochastic systems: A repetitive scenario approach. *IEEE Control Systems Letters*, 7:448–453, 2022.

[90] Oliver Schön, Birgit van Huijgevoort, Sofie Haesaert, and Sadegh Soudjani. Bayesian approach to temporal logic control of uncertain systems. *arXiv preprint arXiv:2304.07428*, 2023.

[91] Koushik Sen, Mahesh Viswanathan, and Gul Agha. Statistical model checking of black-box probabilistic systems. In *International Conference on Computer Aided Verification*, pages 202–215. Springer, 2004.

[92] Koushik Sen, Mahesh Viswanathan, and Gul Agha. On statistical model checking of stochastic systems. In *International Conference on Computer Aided Verification*, pages 266–280. Springer, 2005.

[93] Fedor Shmarov, Sadegh Soudjani, Nicola Paoletti, Ezio Bartocci, Shan Lin, Scott A Smolka, and Paolo Zuliani. Automated synthesis of safe digital controllers for sampled-data stochastic nonlinear systems. *IEEE Access*, 8:180825–180843, 2020.

[94] Christoffer Sloth, George J Pappas, and Rafael Wisniewski. Compositional safety analysis using barrier certificates. In *Proceedings of the 15th ACM international conference on Hybrid Systems: Computation and Control*, pages 15–24, 2012.

[95] S Soudjani, C Gevaerts, and A Abate. Faust 2: Formal abstractions of uncountable-state stochastic processes. In *21st International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2015)*. Newcastle University, 2015.

[96] Sadegh Soudjani and Alessandro Abate. Higher-order approximations for verification of stochastic hybrid systems. In *Automated Technology for Verification and Analysis: 10th International Symposium, ATVA 2012, Thiruvananthapuram, India, October 3-6, 2012. Proceedings 10*, pages 416–434. Springer, 2012.

[97] Sadegh 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.

[98] Sadegh Soudjani, Alessandro Abate, and Rupak Majumdar. Dynamic Bayesian networks as formal abstractions of structured stochastic processes. In *26th International Conference on Concurrency Theory*, pages 169–183. Schloss Dagstuhl, 2015.

[99] Sadegh Soudjani and Rupak Majumdar. Concentration of measure for chance-constrained optimization. *IFAC-PapersOnLine*, 51(16):277–282, 2018.

[100] Sadegh Soudjani, Rupak Majumdar, and Tigran Nagapetyan. Multilevel Monte Carlo method for statistical model checking of hybrid systems. In *Quantitative Evaluation of Systems*, pages 351–367, Cham, 2017. Springer International Publishing.

[101] Mária Svoreňová, Jan Křetínský, Martin Chmelík, Krishnendu Chatterjee, Ivana Černá, and Calin Belta. Temporal logic control for stochastic linear systems using abstraction refinement of probabilistic games. *Nonlinear Analysis: Hybrid Systems*, 23:230–253, 2017.

[102] Abdalla Swikir and Majid Zamani. Compositional synthesis of symbolic models for networks of switched systems. *IEEE Control Syst. Lett.*, 3(4):1056–1061, 2019.

[103] Paulo Tabuada. *Verification and Control of Hybrid Systems: A Symbolic Approach*. Springer, 2009.

[104] Paulo Tabuada and Lucas Fraile. Data-driven stabilization of SISO feedback linearizable systems. *arXiv preprint arXiv:2003.14240*, 2020.

[105] Birgit Van Huijgevoort, Oliver Schön, Sadegh Soudjani, and Sofie Haesaert. Syscore: Synthesis via stochastic coupling relations. In *Proceedings of the 26th ACM International Conference on Hybrid Systems: Computation and Control*, pages 1–11, 2023.

[106] Li Wang, Aaron D Ames, and Magnus Egerstedt. Safety barrier certificates for collisions-free multirobot systems. *IEEE Transactions on Robotics*, 33(3):661–674, 2017.

[107] Zheming Wang and Raphaël M Jungers. Data-driven computation of invariant sets of discrete time-invariant black-box systems. *arXiv:1907.12075*, 2019.

[108] Viraj Brian Wijesuriya and Alessandro Abate. Bayes-adaptive planning for data-efficient verification of uncertain Markov decision processes. In *International Conference on Quantitative Evaluation of Systems*, pages 91–108. Springer, 2019.

[109] GR Wood and BP Zhang. Estimation of the lipschitz constant of a function. *Journal of Global Optimization*, 8(1):91–103, 1996.

[110] Zhengfeng Yang, Min Wu, and Wang Lin. An efficient framework for barrier certificate generation of uncertain nonlinear hybrid systems. *Nonlinear Analysis: Hybrid Systems*, 36:100837, 2020.

[111] Ye Yao, Kun Yang, Mengwei Huang, and Liangzhu Wang. A state-space model for dynamic response of indoor air temperature and humidity. *Building and Environment*, 64:26–37, 2013.

[112] Håkan LS Younes, Marta Kwiatkowska, Gethin Norman, and David Parker. Numerical vs. statistical probabilistic model checking. *International Journal on Software Tools for Technology Transfer*, 8(3):216–228, 2006.

[113] Majid Zamani and Murat Arcak. Compositional abstraction for networks of control systems: A dissipativity approach. *IEEE Trans. Control Network Syst.*, 5(3):1003–1015, 2018.

[114] Majid Zamani, Peyman Mohajerin Esfahani, Rupak Majumdar, Alessandro Abate, and John Lygeros. Symbolic control of stochastic systems via approximately bisimilar finite abstractions. *IEEE Transactions on Automatic Control*, 59(12):3135–3150, 2014.

[115] Majid Zamani, Ilya Tkachev, and Alessandro Abate. Towards scalable synthesis of stochastic control systems. *Discrete Event Dynamic Systems*, 27(2):341–369, 2017.

[116] Lijun Zhang, Zhikun She, Stefan Ratschan, Holger Hermanns, and Ernst Moritz Hahn. Safety verification for probabilistic hybrid systems. In *International Conference on Computer Aided Verification*, pages 196–211. Springer, 2010.

List of Symbols

$\mathbb{N} := \{1, 2, 3, \ldots\}$	positive integers
$\mathbb{N}_0 := \{0, 1, 2, \ldots\}$	non-negative integers
$\mathbb{R}$	real numbers
$\mathbb{R}_0^+$	non-negative real numbers
$\mathbb{R}^+$	positive real numbers
$\mathbb{1}_{\mathscr{A}} : X \to \{0, 1\}$	the indicator function of a set $\mathscr{A} \subseteq X$
$\mathbf{1}_m$	a column vector of ones in $\mathbb{R}^{m \times 1}$
$\lVert x \rVert$	Euclidean norm of any $x \in \mathbb{R}^n$
$\lVert A \rVert = \sup_{x \neq 0} \lVert Ax \rVert / \lVert x \rVert$	induced norm of any matrix $A \in \mathbb{R}^{m \times n}$
$\lvert x \rvert$	absolute value of a real number x
$f^{-1} : Y \to X$	inverse of a function $f : X \to Y$
$\mathcal{S} \models_{\mathcal{H}} \Psi$	satisfaction of a property Ψ within horizon $\mathcal{H}$ by a system $\mathcal{S}$
Ω	sample space of random variables
$\mathfrak{B}(X)$	Borel σ-algebras on a set X
$(X, \mathfrak{B}(X))$	measurable space on X
$\mathbb{P}$	probability measure
$\mathrm{Var}(z) := \mathbb{E}(z^2) - (\mathbb{E}(z))^2$	variance of random variable z
$\mathbb{E}$	expectation operator
$\mathcal{S}$ and S	stochastic system
$\exp(\cdot)$	natural exponential function
$\mathrm{erf}^{-1}(\cdot)$	error inverse function
$[a, b]$	closed interval for any $a, b \in \mathbb{R}, a \leq b$
τ_s	sample time of discretization
$\frac{\partial f}{\partial x}$	partial derivative of of the function f with respect to x
$f^n(x)$	the n^{th} derivative of the function f
$\mathrm{M}(\theta)$	parameterized model of a system S

List of Abbreviations

dt-SS	discrete-time Stochastic System
dt-SCS	discrete-time Stochastic Control System
i.i.d.	independent identically distributed
RCP	Robust Convex Program
RP	Robust Program
SCP	Scenario Convex Program
CCP	Chance Constraint Program
RSP	Repetitive Scenario Program
BC	Barrier Certificate
SS	Stochastic System
CPS	Cyber-Physical System
ML	Machine Learning
STL	Signal Temporal Logic
LTL	Linear Temporal Logic
LTI	Linear Time Invariant
MCM	Monte Carlo Method
PWA	Piece-wise Affine
WJR	Wait, Judge, and Repeat

Curriculum Vitae

I am an electrical engineering and machine learning specialist. My PhD focuses on machine learning, model-based, and data-driven methods for ensuring the safety and performance of cyber- physical systems, including autonomous systems. I received my bachelor's degree in electronics and my master's degree in control engineering from Shiraz University and K.N. Toosi University of Technology, respectively. My particular area of expertise is in industrial systems and engineering project management, in which I have over seven years working experience.

During my studies, I have worked on various projects, developing practical and theoretical solutions for industrial systems, including a data-driven framework guaranteeing the safety of cyber-physical systems.

Prior to this, my career includes experience conducting engineering tests to determine the parameters of governor, turbine and excitation systems, and constructing the overall model in over 30 power plants. I also have experience leading teams of engineering scientists and technicians and dealing with regulatory authorities. I have also designed and built an advanced battery management system for the national energy institute (NRI) with application to electric vehicles, working as the project manager and lead engineer.

My scholarly pursuits are intricately woven into the convergence of Control Theory, Computer Science, Artificial Intelligence, and Data Science, underscoring my ardent dedication to exploring their interconnected realms.

List of Publications

Journal Papers

- **A. Salamati**, A. Lavaie, S. Soudjani, and M. Zamani, “Data-Driven Verification and Synthesis of Stochastic Systems Through Barrier Certificates”, Automatica, 2023.
- **A. Salamati** and M. Zamani, “Safety Verification of Stochastic Systems: A Repetitive Scenario Approach”, IEEE Control Systems Letters, 2022.
- N. Noroozi, **A. Salamati**, and M. Zamani, “Data-driven Safety Verification of Discrete-time Networks: A Compositional Approach”, IEEE Control Systems Letters, vol. 6, pp. 2210–2215, December 2022.
- **A. Salamati**, S. Soudjani, and M. Zamani, “Data-driven verification of stochastic linear systems with signal temporal logic constraints”, Automatica , vol. 131, September 2021.

Conference Papers

- **A. Salamati** and M. Zamani, “Data-Driven Safety Verification of Stochastic Systems”, 9th Conference on Intelligent Cars on Digital Roads, Saint-Rafael, France, 2023.
- **A. Salamati** and M. Zamani, “Safety Verification of Stochastic Systems: A Repetitive Scenario Approach”, 61st IEEE Conference on Decision and Control (CDC), Cancun, Mexico, 2022.
- **A. Salamati** and M. Zamani, “Data-Driven Safety Verification of Stochastic Systems via Barrier Certificates: A Wait-and-Judge Approach”, 4th Conference on Learning for Dynamics and Control (L4DC), Stanford University, Palo Alto, USA, 2022.
- **A. Salamati**, A. Lavaee, S. Soudjani, and M. Zamani, “Data-driven Safety Verification of Stochastic Systems via Barrier Certificates”, 7th IFAC Conference on Analysis and Design of Hybrid Systems, July 2021. (**Best Repeatability Prize**)
- **A. Salamati**, S. Soudjani, and M. Zamani, “Data-Driven Verification under Signal Temporal Logic Constraints”, 21st IFAC World Congress, Berlin, Germany, July 2020.

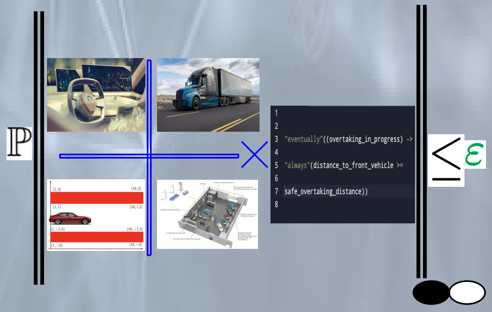
چکیده فارسی

امروزه باتوسعه روزافزون سیستم های سایبر-فیزیک ، حفظ ایمنی و عملکرد دقیق در آن ها از اهمیت بسیاری برخوردار است. اتوموبیل خودرانی را تصور کنید که فاقد سیستم های ایمنی در حین رانندگی می باشد. ناگفته پیداست چه سوانح تلخ جانی و مالی در انتظار سرنشینان آن و محیط اطراف خواهد بود. روش های مبتنی بر مدل بسیاری برای تامین ایمنی و عملکرد سیستم های سایبر-فیزیک توسعه یافته اند؛ لکن مدل صحیح و دقیق از یک سیستم پیچیده سخت افزاری نرم افزاری به طور معمول دست نیافتنی است. از این رو در این پایان نامه ، روش های به روزی در حوزه ماشین لرنینگ و داده محور برای حل معضل عدم دسترسی به مدل دقیق سیستم توسعه داده شده است.

ابتدا فرض می کنیم یک مدل پارامتری نیمه معین از سیستم تصادفی مورد نظر در دسترس است. همچنین مشخصه رفتاری دلخواه توسط لاجیک سیگنال-زمانی تعریف می شود. در مرحله اول به کمک استدلال بیزی و باتوجه به داده های ورودی-خروجی سیستم ، دانش اولیه از پارامترهای مدل به روز می شود. در مرحله بعد به کمک روشهای فرمال فضای پارامتری که لاجیک سیگنال زمانی به ازای آن صادق باشد، محاسبه می شود. با ترکیب این اطلاعات یک معیار احتمالاتی از میزان برآورده شدن مشخصه رفتاری دلخواه ارائه می شود.

درادامه پایان نامه این بار فرض می کنیم هیچ اطلاعاتی از سیستم تصادفی مورد نظر نداریم ، بلکه تنها امکان دسترسی به داده های ورودی-خروجی آن وجود دارد. ابتدا یک مساله ایمنی در ادبیات موضوع را به صورت یک مساله بهینه سازی مقاوم صورت بندی می کنیم. ازآن جا که در مرتبه اول این مساله می بایست به ازای تمام نقاط فضای حالت شود، و دوم این که مدل سیستم ناشناخته است ، حل مساله دشوار است. از این رو این مساله را برای تعداد محدودی از نقاط فضای حالت حل می کنیم. سپس یک تئوری برای ارتباط پاسخ این مساله بهینه سازی جدید با ایمنی سیستم تصادفی اصلی توسعه داده شده است.

از آن جا که روش بالا نیازمند تعداد زیادی داده مخصوصا برای سیستم های با بعد بالاتر می باشد ، درادامه پایان نامه متدهایی را برای کاهش تعدادداده های مورد نیاز و حل کارآمد تر مساله ایمنی سیستم های تصادفی ناشناخته توسعه داده ایم.



```
"eventually"((overtaking_in_progress) ->

"always"(distance_to_front_vehicle >=

safe_overtaking_distance))
```

Machine Learning and Data-Driven Techniques for Verification and Synthesis of Cyber-Physical Systems