Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 58-11 (2024) 63–68

Multiplicative Barrier Certificates for Probabilistic Safety of Markov Jump Systems

Behrad Samari *, **Matteo Della Rossa** **, **Abolfazl Lavaei** *, **Sadegh Soudjani** ***, **Raphael Jungers** ****

* *School of Computing, Newcastle University, United Kingdom*
** *University of Udine, Italy*
*** *Max Planck Institute for Software Systems, Germany*
**** *ICTEAM Institute, UCLouvain, Belgium*

Abstract: This work offers a formal framework for providing safety certificates over discrete-time Markov jump systems (MJSs). Our proposed scheme centers around a new concept of *multiplicative barrier certificates* (MBCs), enabling us to establish a probabilistic lower bound for the safety property in *infinite* time horizons within this class of models. In particular, while a summative barrier certificate, as commonly proposed in the relevant literature, may not be available to ensure the safety of MJS models, we introduce an alternative approach in a multiplicative form, as opposed to the conventional "decreasing in mean" formulation. We demonstrate that in scenarios where a summative barrier does not exist, there is potential for the existence of a multiplicative counterpart. We also provide a systematic methodology grounded on the counterexample-guided inductive synthesis (CEGIS) scheme to systematically construct the proposed multiplicative certificates. We showcase the efficacy of our approach through its application in an air traffic management system.

Keywords: Multiplicative barrier certificates, Markov jump systems, safety specifications, formal methods

1. INTRODUCTION

Motivation and State of the Art. Markov Jump Systems (MJSs), a specialized category of parameter-switching systems, provide a model for a class of multi-modal stochastic systems comprising two core components: system *modes* and system *states*. The (usually finite) set of *modes* represents the possible configurations of the system, and the dynamic transition between them is modeled by countable Markov chains or processes. The system *states* lie in a vector space, and the corresponding evolution is described by a differential or difference equation. In other words, MJSs can be seen as a subclass of stochastic systems where underlying parameters undergo random changes at discrete time intervals, guided by a Markov process. In practical applications, MJSs find relevance in capturing stochastic abrupt variations in system structure and coefficients, which could originate from events like system failures, repairs, external disturbances, or operational shifts (Shi and Li, 2015). For a theoretic introduction to this framework, we refer to the works by Mariton (1988); Fang et al. (1995); Fang and Loparo (2002).

When working with stochastic systems in general, and MJSs specifically, one often needs to tackle *safety* and *reachability* problems in a probabilistic sense. Safety analysis of a given system aims to determine whether its trajectories can stay within a specific safe set. Reachability analysis, on the other hand, checks whether system trajectories can reach a target set starting from the initial set. In a stochastic setting, the goal is to establish the minimum probability that the system remains within the safe set (likewise for stochastic reachability). For a general introduction to these concepts, we refer to the work by Prajna et al. (2007).

Despite being challenging problems, both from a theoretic and computational point of view, safety and reachability analysis for stochastic systems has been the topic of intense research in the past decades (Lavaei et al., 2022). One promising strategy to tackle this issue involves employing *discretization-free* methods centered around *barrier certificates*. The barrier approach was initially introduced for verifying (stochastic) hybrid systems by Prajna and Jadbabaie (2004) and Prajna et al. (2007). Over the past decade, it has garnered considerable attention in formal verification and controller synthesis for various classes of stochastic systems, see (Zhang et al., 2010; Yang et al., 2020; Ahmadi et al., 2019; Santoyo et al., 2019; Clark, 2019; Lavaei and Frazzoli, 2024; Nejati et al., 2024). While current findings regarding the formal analysis of stochastic systems, including MJS models, through barrier certificates are extensive, regrettably, all the literature's results advocate for a summative barrier approach of different modes of MJS (*e.g.,* (Lavaei and Frazzoli, 2022; Nejati et al., 2022)), which might not exist in many scenarios.

Original Contribution. The primary contribution of this work lies in introducing, for the first time, the concept of *multiplicative barrier certificates* for the probabilistic safety verification of Markov jump systems. Specifically,

10.1016/j.ifacol.2024.07.426

despite the absence of a commonly proposed summative barrier certificate in the relevant literature to guarantee the safety of MJS models, we introduce an alternative approach in a *multiplicative* form, as opposed to the conventional "decreasing in mean" formulation. This approach is motivated by stability analysis of Markov jump *linear* systems, in which almost-sure stability (equivalently, the existence of multiple *norms* decreasing in a multiplicative sense) provides a less restrictive stability condition with respect to stability in mean (equivalently, the existence of multiple norms decreasing in mean), see for example the work by Fang et al. (1995); Costa et al. (2005); Della Rossa and Jungers (2022). Additionally, we provide a systematic methodology based on the counterexample-guided inductive synthesis (CEGIS) scheme to construct the proposed multiplicative certificates. Proofs of all statements are omitted due to lack of space.

2. PROBLEM DESCRIPTION

2.1 Notation

Sets of real numbers, positive real numbers, and non-negative real numbers are denoted by $\mathbb{R}$, $\mathbb{R}_{>0}$, and $\mathbb{R}_{\geq 0}$, respectively. The set of non-negative integers is represented by $\mathbb{N} := \{0, 1, 2, \dots\}$, while $\mathbb{N}_+ = \{1, 2, \dots\}$ denotes the set of positive integers. We denote an empty set with $\emptyset$. Given $M \in \mathbb{N}_+$, we define $I_M := \{1, \dots, M\}$, while the set Σ_M denotes the *one-sided Bernoulli space* defined by $\Sigma_M := \{\sigma = (\sigma_0, \sigma_1, \sigma_2, \dots) \mid \forall k \in \mathbb{N},\ \sigma_k \in I_M\}$.

2.2 Markov Jump Systems

In this section, we present a formal description of Markov jump systems, serving as the underlying dynamics in our work.

Definition 1. Consider $M \in \mathbb{N}_+$, a closed set $X \subseteq \mathbb{R}^n$, and a function $f : X \times I_M \to X$ such that $f(\cdot, i)$ is continuous, for all $i \in I_M$. We consider the system

$$x(k+1) = f(x(k), \sigma(k)), \quad k \in \mathbb{N}, \tag{1}$$

where the switching signal $\sigma \in \Sigma_M$ is assumed to be the realizations of a time-homogeneous Markov chain whose transition probabilities are given by

$$p_{ij} = \mathbb{P}\{\sigma(k+1) = j \mid \sigma(k) = i\}, \quad \forall i, j \in I_M.$$

We denote by $P \in \mathbb{R}^{M \times M}$ the matrix whose (i, j) entry is equal to p_{ij}. Let $z = (z_1, \dots, z_M)^\top$ such that $z_j \in \mathbb{R}_{\geq 0}$. Then, the initial probability distribution of $\sigma(0)$ is given by $\pi = (p_1, \dots, p_M)^\top \in \Xi_M := \{z \in \mathbb{R}^M_{\geq 0} \mid \sum_{j=1}^M z_j = 1\}$. With $\mu_{P,\pi}$, we denote the probability measure induced by P and π on the space of switching sequences Σ_M. Given $x_0 \in X$ and $\sigma \in \Sigma_M$, we denote by $\Phi(k, x_0, \sigma)$ the *solution* of (1), starting at $x(0) = x_0$ with respect to the signal σ, evaluated at time $k \in \mathbb{N}$.

The primary aim in this work is to analyze the stochastic behavior of system (1) to establish probabilistic certificates over the safety of the system. It is worth noting that the class of models defined in (1) has found applications in various domains, such as air traffic management systems (Zhou et al., 2011) and power systems incorporating stochastic loads (Ugrinovskii and Pota, 2005). To provide a clearer understanding of MJS in (1), the subsequent subsection offers a motivating example, which will also serve as one of the case studies in our work.

2.3 Motivating Example: Air Traffic Management

To illustrate the concepts in this work, we consider the air traffic flow management subject to weather-related uncertainties. This scenario involves various operational modes and stochastic variations in the number of aircraft arriving in each interval, as described in (Zhou et al., 2011). Consider an MJS with the following dynamics:

$$\begin{cases} \mathsf{e}(k) = \mathsf{a}(q(k))\mathsf{b}(k-1) + \mathsf{c}(q(k)), \\ \mathsf{b}(k) = \mathsf{b}(k-1) + \Upsilon(k) - \mathsf{e}(k), \\ \mathsf{B}(k) = \mathsf{b}(k-1) - \mathsf{e}(k), \end{cases} \tag{2}$$

where $\mathsf{e}(k)$ is the crossing flow, $\mathsf{b}(k)$ is the buffer length, and $\mathsf{B}(k)$ is the backlog, *i.e.,* the number of aircraft being delayed at time step k. Moreover, $q(k) \in \mathbb{R}^{M \times 1}$, with M being the number of operational modes, has only one entry as 1, representing the state of the weather at time step k modeled by a Markov chain with the transition probability matrix $P \in \mathbb{R}^{M \times M}$, and $\mathsf{a}(q(k))$ and $\mathsf{c}(q(k))$ represent the values of parameters a and c, associated with the state of the Markov chain $q(k)$, respectively. In the MJS (2), when the Markov chain is in the adverse weather condition, the parameters are set as $\mathsf{a} = 0.04$ and $\mathsf{c} = 4.22$. Conversely, in the favorable weather, the values shift to $\mathsf{a} = 0.98$ and $\mathsf{c} = 0.09$. The variable $\Upsilon(k)$ represents the number of aircraft arriving during each time interval of $\Delta t = 20$ minutes. This quantity follows a Poisson distribution with a rate parameter λ (indicating the inflow rate), where $\lambda \Delta t = 4.9$.

2.4 Probabilistic Safety Property

In this subsection, we initially present the formal definition of the probabilistic safety property within the scope of this work. Subsequently, we define the problem we aim to address.

Definition 2. (Probabilistic safety). Let us consider $M \in \mathbb{N}_+$, a closed set $X \subseteq \mathbb{R}^n$, a function $f : X \times I_M \to X$, and a Markov chain (P, π). Given sets $X_0, X_u \subseteq X$, as initial and unsafe sets, and a horizon $K \in \mathbb{N}$, we say that the MJS is K-safe with a probability $\rho \in [0, 1)$ if all trajectories of MJS starting from any initial conditions $x \in X_0$ never reach the unsafe rejoin X_u with a probability ρ, *i.e,*

$$\mu_{P,\pi}\left(\{\sigma \in \Sigma_M \mid \Phi(k, x, \sigma) \in X_s \text{ for all } 0 \leq k \leq K\}\right) \geq \rho, \tag{3}$$

for all $x \in X_0$, where $X_s = X \backslash X_u$ is the safe set. If the bound ρ and the safety property remain independent of the initial probability π, we denote that the property holds *uniformly* across the set Ξ_M of initial probabilities.

Characterization and computation of the safety probability on MJSs are studied in the more general setting of partially-degenerate systems (Soudjani and Abate, 2012). Specifically, this requires computing value functions $\mathbb{U}_k : X \times I_M \to [0, 1]$, with $\mathbb{U}_0(x, \sigma) = \mathbf{1}_{X_s}(x)$ being the indicator function of the safe set and for $k \in \{0, 1, 2, \dots, K\}$,

$$\mathbb{U}_{k+1}(x, \sigma) = \mathbf{1}_{X_s}(x) \sum_{\sigma'=1}^{M} p_{\sigma\sigma'} \mathbb{U}_k(f(x, \sigma), \sigma'),\ \forall x \in X, \sigma \in I_M.$$

Even for the case of affine dynamics and polytopic safe sets, these value functions become piecewise constant

with polytopic regions, but the number of regions grows exponentially with the time horizon K. This motivates us to use the concept of barrier certificates that does not suffer from such exponential computational complexities.

We now formally define the problem that we aim to solve in this work.

Problem 1. Consider the Markov jump system, described in (1), and the probabilistic safety property outlined in Definition 2. Develop a formal framework based on *multiplicative barrier certificates*, as opposed to the conventional summative ones proposed in the literature, aiming to compute the probabilistic lower bound ρ in (3) as the safety certificate of the MJS within *infinite* time horizons, *e.g.,* $0 \leq k < \infty$.

To address Problem 1, we introduce our new concept of multiplicative barrier certificates in the next section.

3. MULTIPLICATIVE BARRIER CERTIFICATES FOR MJS

Here, we introduce the new notion of multiplicative barrier certificates to establish a probabilistic safety certificate for MJS in (1). To achieve this, we initiate by recalling the conventional summative barrier certificates, as commonly suggested in the literature, such as the one by Lavaei and Frazzoli (2022).

Definition 3. (Summative Barrier Certificates). Consider the Markov jump system in (1) with a function $f : X \times I_M \to X$ such that $f(\cdot, i)$ is continuous for all $i \in I_M$. Let $X_0, X_u \subseteq X$ be the initial and unsafe sets of the system. A set of functions $V_1, \ldots, V_M : X \to \mathbb{R}_{\geq 0}$ is a *summative* barrier certificate (SBC) if there exist $0 \leq \varepsilon < C$, and $c \in \mathbb{R}_{\geq 0}$, such that

$$X_0 \subseteq L_{V_i}(\varepsilon), \qquad \forall i \in I_M, \tag{4a}$$
$$L_{V_i}(C) \cap X_u = \emptyset, \qquad \forall i \in I_M, \tag{4b}$$
$$\sum_{j \in I_M} p_{ij} V_j(f(x,j)) \leq V_i(x) + c, \quad \forall i \in I_M, \forall x \in X, \tag{4c}$$

where $L_{V_i}(\varepsilon) := \{x \in X \mid V_i(x) \leq \varepsilon\}$, is the *$\varepsilon$-sublevel set* of V (likewise for $L_{V_i}(C)$).

The required conditions in (4) are independent of the initial probability π. Consequently, they offer safety certificates that remain uniform regardless of the initial probabilities, as formalized in the subsequent result (Lavaei and Frazzoli, 2022; Kushner, 1967).

Proposition 1. Consider the Markov jump system described in (1), with $V_1, \ldots, V_M : X \to \mathbb{R}_{\geq 0}$ serving as their *summative* barrier certificates, as in Definition 3. Then for any initial probability $\pi \in \Xi_M$, any initial state $x_0 \in X_0$, and any $k \in [0, K]$, the MJS is K-safe in the sense of Definition 2 with the following guaranteed lower-bound probability ρ:

$$\mu_{P,\pi}\left(\{\sigma \in \Sigma_M \mid \Phi(k, x, \sigma) \in X_s \text{ for all } 0 \leq k \leq K\}\right) \geq \rho = 1 - \frac{\varepsilon + Kc}{C}. \tag{5}$$

Given that we treat Markov jump systems with general nonlinear sub-dynamics, it is typical for the solution's behavior to be convoluted locally, posing challenges in designing functions that satisfy (4c) globally, *i.e.,* for all $x \in X$. In the subsequent corollary, we demonstrate a relaxation of this condition.

Corollary 1. Under the hypothesis of Definition 3, suppose there exists a closed set $\hat{X}_0 \subseteq X_0$ that is *surely mapped* into X_0, *i.e.*, it holds that

$$f(x,i) \in X_0, \ \ \forall x \in \hat{X}_0, \ \forall i \in I_M. \tag{6}$$

Then if condition (4c) is satisfied for all $x \in X \setminus \hat{X}_0$ (and not necessarily globally on X), Proposition 1 continues to yield the same outcomes, while preserving the probability bound in (5).

Inspired by the revelation that summative barrier certificates may not be available in various scenarios (as will be presented in Subsection 5.1), we now introduce our innovative *multiplicative* barrier certificates. This formulation draws inspiration from the classical Lyapunov conditions for the *almost-sure stability* of Markov jump systems, as exemplified in the work by Della Rossa and Jungers (2022) and references therein. In the following, we demonstrate that this form could be more suitable in specific contexts, particularly when the summative barrier is unavailable.

Definition 4. (Multiplicative Barrier Certificates). Consider the Markov jump system in (1) with a function $f : X \times I_M \to X$ such that $f(\cdot, i)$ is continuous for all $i \in I_M$. Let $X_0, X_u \subseteq X$ be the initial and unsafe sets of the system. set of functions $W_1, \ldots, W_M : X \to \mathbb{R}_{\geq 0}$ is a *multiplicative* barrier certificate (MBC) if there exist $0 \leq \bar{\varepsilon} < \bar{C}$, and a $\bar{\gamma} \in (0, 1)$ such that

$$X_0 \subseteq L_{W_i}(\bar{\varepsilon}), \qquad \forall i \in I_M, \tag{7a}$$
$$L_{W_i}(\bar{C}) \cap X_u = \emptyset, \qquad \forall i \in I_M, \tag{7b}$$
$$\prod_{j \in I_M} W_j(f(x,j))^{p_{ij}} \leq \bar{\gamma} W_i(x), \qquad \forall i \in I_M, \forall x \in X. \tag{7c}$$

Remark 1. Note that despite the bilinearity among unknown parameters of multiplicative barrier certificates $W_1, \ldots, W_M$ in condition (7c), we provide a systematic approach in Section 4 based on the CEGIS framework, which inherently handles this bilinearity without encountering any difficulties.

We now present the key result of our work, revealing that the new multiplicative barrier certificates offer a quantified probabilistic lower bound on the safety of the MJS within *infinite* time horizons.

Theorem 2. Consider the Markov jump system described in (1), with $W_1, \ldots, W_M : X \to \mathbb{R}_{\geq 0}$ serving as its *multiplicative* barrier certificates, as in Definition 4. Suppose there exists a closed set $\hat{X}_0 \subseteq X_0$ such that:

(1) $\{x \in X \mid \exists i \in I_M \text{ s.t. } W_i(x) = 0\} \subset \text{int}(\hat{X}_0)$,
(2) property (6) holds,

with $\text{int}(\hat{X}_0)$ being the interior of the set $\hat{X}_0$. Then for any initial probability $\pi \in \Xi_M$, any initial state $x_0 \in X_0$, and any $k \in [0, \infty)$, the MJS is K-safe within *infinite time horizons* with the guaranteed lower-bound probability ρ as in (5) with

$$c := \max\{0, \log(\bar{\gamma})\} = 0,$$
$$\varepsilon := \log(\bar{\varepsilon}) + \log(\alpha),$$
$$C := \log(\bar{C}) + \log(\alpha),$$

where $\alpha := \max_{i \in I} \{\sup_{x \in X \setminus \hat{X}_0} \frac{1}{W_i(x)}\}$.

Remark 2. It is worth noting that condition (7c) can be somewhat relaxed by allowing the constant $\bar{\gamma}$ to be greater than one. However, this relaxation comes at the expense of transitioning from the infinite-horizon guarantee to a finite time one as in (5) with $c = \log(\bar{\gamma})$.

Remark 3. One needs to first compute $\bar{\varepsilon}$ and $\bar{C}$ according to (7a),(7b), and then compute ε and C according to Theorem 2. The guaranteed probability ρ will be improved if the distance between $\bar{\varepsilon}$ and $\bar{C}$ (accordingly, ε and C) increases.

4. COMPUTATION OF MBC

In this section, we employ an approach on the basis of the counterexample-guided inductive synthesis (CEGIS) framework to construct MBCs fulfilling conditions (7a)-(7c). This approach leverages existing Satisfiability Modulo Theories (SMT) solvers, including Z3 (De Moura and Bjørner, 2008), dReal (Gao et al., 2013), and OptiMathSAT (Sebastiani and Trentin, 2015) and utilizes satisfiability (feasibility) solvers to construct MBCs.

We aim to express the conditions of Definition 4 as a satisfiability problem. This formulation enables the search for parametric MBCs through the CEGIS approach, as formalized in the following proposition.

Proposition 2. Under the assumption that the MJS has a compact state set $X \subseteq \mathbb{R}^n$, suppose there exist functions $W_i(x), \forall i \in I_M$, and constants $\bar{\gamma} \in (0,1)$, $0 \leq \bar{\varepsilon} < \bar{C}$, such that the following expression holds true for all $i \in I_M$:

$$\psi(b) := \bigwedge_{x\in X} (W_i(x) \geq 0) \bigwedge_{x\in X_0} (W_i(x) \leq \bar{\varepsilon}) \bigwedge_{x\in X_u} (W_i(x) \geq \bar{C}) \bigwedge_{x\in X} \Big(\prod_{j\in I_M} W_j(f(x,j))^{p_{ij}} \leq \bar{\gamma} W_i(x) \Big). \tag{8}$$

Then, $W_i(x)$ satisfies conditions (7a)-(7c) in Definition 4.

In the following, we provide a brief explanation of the CEGIS steps employed for the computation of functions $W_i(x)$ for all $i \in I_M$:

(1) Specify parameterized MBCs as $W_i(b,x) = \sum_{j=1}^{r} b_j \, w_j(x)$, wherein $w_j(x)$ are (possibly nonlinear) basis functions and $b_j \in \mathbb{R}$ are unknown coefficients for $j \in \{1, 2, \ldots, r\}$.
(2) A finite set of samples $\bar{X} \in X$, a constant $\bar{\gamma} \in (0,1)$, and $0 \leq \bar{\varepsilon} \leq \bar{C}$ should be selected.
(3) Construct potential MBCs $W_i(b,x), \forall i \in I_M$, by computing unknown coefficients b_i such that the following expression holds true:

$$\bigwedge_{x\in \bar{X}} (W_i(x) \geq 0) \bigwedge_{x\in \bar{X}\cap X_0} (W_i(x) \leq \bar{\varepsilon}) \bigwedge_{x\in \bar{X}\cap X_u} (W_i(x) \geq \bar{C}) \bigwedge_{x\in \bar{X}} \Big(\prod_{j\in I_M} W_j(f(x,j))^{p_{ij}} \leq \bar{\gamma} W_i(x) \Big). \tag{9}$$

The previously mentioned expression leads us to a linear arithmetic formula incorporating Boolean combinations of linear inequality constraints in b_j. This can be effectively solved using SMT solvers or, alternatively, by utilizing nonlinear optimization toolboxes.
(4) Search for a counterexample $x_c \in X$ such that the candidate MBCs $W_i(b,x)$, obtained in the previous step, satisfy $\neg\psi(b)$ in (8), with $\neg$ being the negation, *i.e.*,

$$\bigvee_{x\in X} (W_i(x) < 0) \bigvee_{x\in X_0} (W_i(x) > \bar{\varepsilon}) \bigvee_{x\in X_u} (W_i(x) < \bar{C}) \bigvee_{x\in X} \Big(\prod_{j\in I_M} W_j(f(x,j))^{p_{ij}} > \bar{\gamma} W_i(x) \Big). \tag{10}$$

If $\neg\psi(b)$ has no feasible solution, the obtained candidate solution serves as valid MBCs for all $x \in X$, concluding the algorithm. However, if $\neg\psi(b)$ is feasible for some $x = x_c \in X$, then the counterexample x_c should be included in the finite set, $X := X \cup \{x_c\}$, and Steps 3,4 should be repeated.

5. CASE STUDIES

In this section, to provide a comparison between multiplicative and summative barrier certificates, we initially demonstrate that, even in the constrained linear case, there may be a lack of available summative barrier certificates to offer safety guarantees for Markov jump systems. Simultaneously, we showcase the ability to construct multiplicative barrier certificates for the same example within our framework. Subsequently, we apply our findings to the Air Traffic Management in (2) as the second case study.

5.1 MJS with MBCs but without SBCs

Consider the MJS $f(x,i) := A_i x$, with two modes $i \in \{1,2\}$ and the following matrices:

$$A_1 = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & 0 \\ 0 & a \end{bmatrix},$$

with $a > 2$. Let the transition matrix of the considered Markov chain be as $P = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$. We consider $X = \mathbb{R}^2_{\geq 0}$, *i.e.*, the positive cone, which is surely forward invariant ($f(X,i) \subseteq X$, for all $i \in I_M$) since the matrices have non-negative coefficients. Consider $X_0 = \mathbb{B}(0,\varepsilon)$ and $X_s = \mathbb{B}(0,C)$ for some $0 \leq \varepsilon < C$, where $\mathbb{B}(0,\mathrm{r})$ represents the closed ball of radius r, for some arbitrary norm on $\mathbb{R}^2_{\geq 0}$.

We now prove that the system has no homogeneous *polynomial summative* barrier certificates in the sense of Definition 3, when considering $X \subseteq \mathbb{R}^2_{\geq 0}$ as a compact set and $c = 0$. Indeed, suppose by contradiction that $p_1, p_2 \in \mathbb{R}_h[x]$, polynomial homogeneous of degree $h \in \mathbb{N}_+$, positive in X, provide SBCs according to Definition 3 (with $c = 0$). Then, according to (4c), for any $x = [x_1, x_2]^\top \in X$, we have

$$\frac{1}{2}p_1(f(x,1)) + \frac{1}{2}p_2(f(x,2)) = \frac{a^h p_1([x_1,0]^\top) + a^h p_2([0,x_2]^\top)}{2} \leq p_1([x_1,0]^\top).$$

For instance, selecting $x = [x_1, 0]^\top \in X$ with $x_1 \neq 0$, this implies

$$\frac{a^h}{2} p_1([x_1,0]^\top) \leq p_1([x_1,0]^\top), \quad \forall x_1 \in \mathbb{R}_{\geq 0},$$

which leads to a contradiction since $a > 2$ and $h \in \mathbb{N}_+$ implies $a^h/2 > 1$.

This indicates that there are no *summative* barrier certificates for this example that satisfy conditions (4a)-(4c)

with $c = 0$. We now proceed with exploring *multiplicative* barrier certificates as proposed in Definition 4. Let us consider $a = 2.01$, $X = [0, 100]^2$, $X_u = [95, 100]^2$, and $X_0 = \mathbb{B}(0, 1)$. By employing the CEGIS framework introduced in Section 4, *multiplicative* barrier certificates of degree one are computed as the following:

$$W_1(x) = x_1 + 4.45x_2,$$
$$W_2(x) = 4.45x_1 + x_2.$$

Moreover, we obtain $\bar{\varepsilon} = 4.56$, $\bar{C} = 518.17$, $\bar{\gamma} = 0.47$, and $\alpha = 2.01$. Therefore, we have

$$c = \max\{0, \log(0.47)\} = 0,$$
$$\varepsilon = \log(4.56) + \log(2.01) = 0.96,$$
$$C = \log(518.17) + \log(2.01) = 3.01.$$

Thus, according to (5), the MJS is K-safe in the sense of Definition 2 within an *infinite* time horizon (as $c = 0$) with the guaranteed probability $\rho = 68\%$. It is worth highlighting that although this quantified probability might not be as high as desired, a noteworthy point to take into account is that there are no summative barrier certificates within the same template of MBCs to provide a probabilistic guarantee for this example. This implementation was performed using the Z3 SMT solver in Python on a MacBook Pro (Apple M2 Max), completing in about 5 seconds.

Figure 1 schematically illustrates the fulfillment of condition (7c).

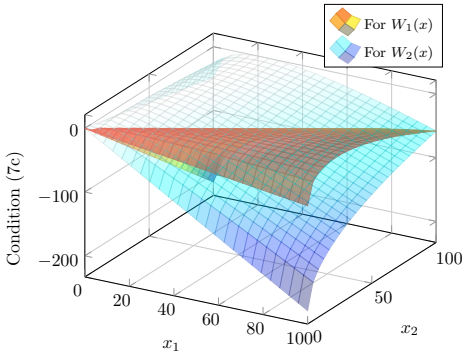


Fig. 1. Satisfaction of condition (7c): $(W_1(f(x,1)))^{0.5}(W_2(f(x,2)))^{0.5} - \bar{\gamma}W_i(x)$ is non-positive for all $i \in \{1, 2\}$ and $x \in X$. The surface for $W_1(x)$ is depicted in hot color, while the surface in cold color is corresponding to $W_2(x)$.

5.2 Air Traffic Management

As the second case study of the work, consider the MJS in (2) with two modes $i \in \{1, 2\}$, where the first mode corresponds to the adverse weather condition, whereas the second mode is associated with the favorable weather condition. By defining $x = [\mathsf{b}, \mathsf{B}]^\top$, after some algebraic manipulation, we can rewrite (2) as $f(x, i) := A_i x + B_i$ with the following matrices:

$$A_1 = \begin{bmatrix} 0.96 & 0 \\ 0.96 & 0 \end{bmatrix}, \quad B_1 = \begin{bmatrix} 4.9 - 0.09 \\ -0.09 \end{bmatrix},$$
$$A_2 = \begin{bmatrix} 0.02 & 0 \\ 0.02 & 0 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 4.9 - 4.22 \\ -4.22 \end{bmatrix}.$$

For the sake of simplicity, we substitute the variable $\Upsilon(k)$ in (2) with its expected value. Furthermore, let

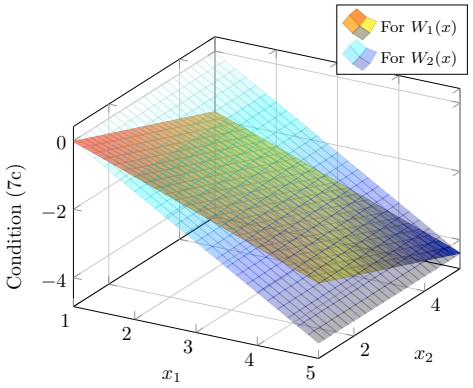


Fig. 2. Fulfillment of condition (7c) is ensured by the expression $(W_1(f(x,1)))^{0.5}(W_2(f(x,2)))^{0.5} - \bar{\gamma}W_i(x)$ being non-positive for all $i \in \{1, 2\}$ and $x \in X$.

the transition matrix of the considered Markov chain be given as $P = \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$. We also consider $X = [1, 5]^2$, $X_u = [4.95, 5]^2$, and $X_0 = \mathbb{B}(1.01, 0.01)$. By employing the CEGIS framework, detailed in Section 4, *multiplicative* barrier certificates are obtained as

$$W_1(x) = x_1 + 0.5x_2 - 1,$$
$$W_2(x) = 1.5x_1 + 0.0039x_2 - 1.$$

Furthermore, we compute $\bar{\varepsilon} = 0.5352$, $\bar{C} = 6.4238$, $\bar{\gamma} = 0.875$, and $\alpha = 2$. Hence, we have

$$c = \max\{0, \log(0.875)\} = 0,$$
$$\varepsilon = \log(0.5352) + \log(2) = 0.0295,$$
$$C = \log(6.4238) + \log(2) = 1.1088.$$

Consequently, in accordance with (5), the MJS is K-safe in the sense of Definition 2 within an *infinite* time horizon with the guaranteed probability $\rho = 97\%$. This implementation was performed using the Z3 SMT solver in Python on a MacBook Pro (Apple M2 Max), completing in about 18 seconds.

We now aim in constructing *summative* barrier certificates for this example, with the same template, to potentially provide a probabilistic safety certificate independent of the time horizon. Using the same template, SBCs are computed as

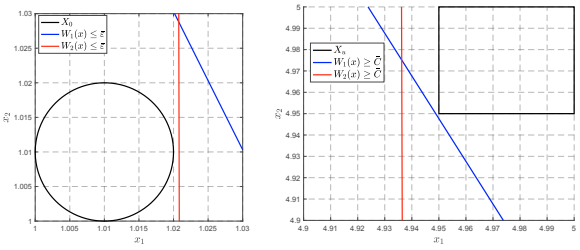
$$V_1(x) = x_1 + 1.041x_2 + 2.5943,$$
$$V_2(x) = 1.2201x_1 + 0.8209x_2 + 2.5939.$$

Moreover, we compute $\varepsilon = 4.67$, $C = 12.697$, and $c = 0$. This results in the guaranteed probability $\rho = 63\%$, which is notably lower than the one computed with *multiplicative* barrier certificates. It is essential to note that, using this template, this is the highest probability one can achieve based on SBCs.

Figure 2 provides a schematic illustration of the satisfaction of condition (7c), while the satisfaction of conditions (7a) and (7b) is presented in Figure 3.

6. CONCLUSIONS

In this work, we introduced a formal framework aimed at offering safety certificates for discrete-time Markov jump systems. Our approach was based on the concept of *multiplicative barrier certificates* (MBCs), which enables the



(a) Satisfaction of condition (7a)

(b) Satisfaction of condition (7b)

Fig. 3. As it can be seen, both conditions (7a) and (7b) are satisfied. The initial and unsafe sets X_0, X_u are depicted with a circle and a square, respectively.

establishment of a probabilistic lower bound for safety properties within this specific class of models. Our work highlights the significance of MBCs, especially in scenarios where traditional summative barriers are not applicable, demonstrating the potential for the existence of MBCs as a viable alternative. We also presented a systematic methodology based on the counterexample-guided inductive synthesis (CEGIS) scheme for the systematic construction of the proposed multiplicative certificates. We applied our results to two case studies, including an air traffic management system. Exploring avenues to enhance *scalability* for *large-scale* MJSs could be a potential future direction.

REFERENCES

Ahmadi, M., Singletary, A., Burdick, J.W., and Ames, A.D. (2019). Safe policy synthesis in multi-agent POMDPs via discrete-time barrier functions. In *Proceedings of the 58th Conference on Decision and Control (CDC)*, 4797–4803.

Clark, A. (2019). Control barrier functions for complete and incomplete information stochastic systems. In *Proceedings of the American Control Conference (ACC)*, 2928–2935.

Costa, O.L.V., Fragoso, M.D., and Marques, R.P. (2005). *Discrete-time Markov jump linear systems*. Probability and Its Applications. Springer-Verlag.

De Moura, L. and Bjørner, N. (2008). Z3: An efficient SMT solver. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, 337–340. Springer.

Della Rossa, M. and Jungers, R. (2022). Almost sure stability of stochastic switched systems: Graph lifts-based approach. In *Proceedings of the 61st Conference on Decision and Control (CDC)*, 1021–1026.

Fang, Y., Loparo, K.A., and Feng, X. (1995). Stability of discrete time jump linear systems. *Journal of Mathematical Systems, Estimation and Control*, 5(3), 275–321.

Fang, Y. and Loparo, K. (2002). Stochastic stability of jump linear systems. *IEEE Transactions on Automatic Control*, 47(7), 1204–1208.

Gao, S., Kong, S., and Clarke, E.M. (2013). dReal: An SMT solver for nonlinear theories over the reals. In *Automated Deduction–CADE-24, Proceedings '24*, 208–214. Springer.

Kushner, H. (1967). *Stochastic stability and control*. Mathematics in Science and Engineering. Academic Press.

Lavaei, A. and Frazzoli, E. (2022). Compositional controller synthesis for interconnected stochastic systems with Markovian switching. In *Proceedings of American Control Conference (ACC)*, 4838–4843.

Lavaei, A. and Frazzoli, E. (2024). Scalable synthesis of safety barrier certificates for networks of stochastic switched systems. *IEEE Transactions on Automatic Control*.

Lavaei, A., Soudjani, S., Abate, A., and Zamani, M. (2022). Automated verification and synthesis of stochastic hybrid systems: A survey. *Automatica*, 146.

Mariton, M. (1988). Almost sure and moments stability of jump linear systems. *Systems & Control Letters*, 11(5), 393–397.

Nejati, A., Nayak, S.P., and Schmuck, A.K. (2024). Context-triggered games for reactive synthesis over stochastic systems via control barrier certificates. In *Proceedings of the 27th ACM International Conference on Hybrid Systems: Computation and Control (HSCC)*.

Nejati, A., Soudjani, S., and Zamani, M. (2022). Compositional construction of control barrier functions for continuous-time stochastic hybrid systems. *Automatica*, 145.

Prajna, S. and Jadbabaie, A. (2004). Safety verification of hybrid systems using barrier certificates. In *Proceedings of the International Workshop on Hybrid Systems: Computation and Control (HSCC)*, 477–492.

Prajna, S., Jadbabaie, A., and Pappas, G. (2007). A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control*, 52(8), 1415–1428.

Santoyo, C., Dutreix, M., and Coogan, S. (2019). Verification and control for finite-time safety of stochastic systems via barrier functions. In *Proceedings of the IEEE Conference on Control Technology and Applications*, 712–717.

Sebastiani, R. and Trentin, P. (2015). Optimathsat: A tool for optimization modulo theories. In *International Conference on Computer Aided Verification*, 447–454. Springer.

Shi, P. and Li, F. (2015). A survey on Markovian jump systems: modeling and design. *International Journal of Control, Automation and Systems*, 13, 1–16.

Soudjani, S. and Abate, A. (2012). Probabilistic invariance of mixed deterministic-stochastic dynamical systems. In *Proceedings of the 15th ACM International Conference on Hybrid Systems: Computation and Control (HSCC)*, 207–216.

Ugrinovskii, V. and Pota, H.R. (2005). Decentralized control of power systems via robust control of uncertain Markov jump parameter systems. *International Journal of Control*, 78(9), 662–677.

Yang, Z., Wu, M., and Lin, W. (2020). An efficient framework for barrier certificate generation of uncertain nonlinear hybrid systems. *NAHS*, 36.

Zhang, L.and She, Z., Ratschan, S., Hermanns, H., and Hahn, E.M. (2010). Safety verification for probabilistic hybrid systems. In *CAV*, 196–211.

Zhou, Y., Wan, Y., Roy, S., Taylor, C., and Wanke, C. (2011). A stochastic modeling and analysis approach to strategic traffic flow management under weather uncertainty. In *AIAA Guidance, Navigation, and Control Conference*, 6514.