Formal Verification of Stochastic Max-Plus-Linear Systems

Sadegh Esmaeil Zadeh Soudjani, Dieky Adzkiya, and Alessandro Abate

***Abstract*—This work investigates the computation of finite abstractions of Stochastic Max-Plus-Linear (SMPL) systems and their formal verification against general bounded-time linear temporal specifications. SMPL systems are probabilistic extensions of discrete-event MPL systems, which are widely employed for modeling engineering systems dealing with practical timing and synchronization issues. Departing from the standard existing approaches for the analysis of SMPL systems, we newly propose to construct formal, finite abstractions of a given SMPL system: the SMPL system is first re-formulated as a discrete-time Markov process, then abstracted as a finite-state Markov Chain (MC). The derivation of precise guarantees on the level of the introduced formal approximation allows us to probabilistically model check the obtained MC against bounded-time linear temporal specifications (which are of rather general applicability), and to reliably export the obtained results over the original SMPL system. The approach is practically implemented on a dedicated software and is elucidated and run over numerical examples.**

***Index Terms*—Max-plus-linear systems, max-plus algebra, discrete-time stochastic processes, continuous-state processes, probabilistic model checking, linear-time logic, finite abstractions.**

I. Background and Goals

MAX-PLUS-LINEAR (MPL) systems are a class of discrete-event systems [1], [2] with a continuous state space characterizing the timing of the underlying sequential discrete events. MPL systems are used to describe the timing synchronization between interleaved processes, under the assumption that timing events are dependent linearly (within the max-plus algebra) on previous event occurrences. MPL systems are widely employed in the analysis and scheduling of infrastructure networks, such as communication and railway systems [3], or production and manufacturing lines [4], [5].

Stochastic Max-Plus-Linear (SMPL) systems [6], [7], [8] are MPL systems where the time interval between successive event occurrences (in the examples above, the transportation, processing, or production times) are now characterized by random quantities. In practical applications SMPL systems are evidently more realistic than simpler MPL ones: for instance in a model for a railway network, train running times depend on imperceptible changes in driver behavior, on hardly predictable weather conditions, and on volatile passenger numbers at stations: as such they can arguably be more suitably modeled by random variables than fixed deterministic delays.

We are interested in analyzing general dynamical properties of SMPL systems. Only a few approaches have been developed in the literature, and focus on the study of the steady-state behavior of SMPL systems, for example employing Lyapunov exponents and asymptotic growth rates [9], [10], [11], [12], [13], [14]. The Lyapunov exponent of an SMPL system is analogous to the max-plus eigenvalue for an autonomous MPL system [11, Sec. 7.3]. The series expansion formula of a Lyapunov exponent has been discussed in [12], [13]. The asymptotic behavior of sequences of states of SMPL systems is analyzed in [14]. The computation of Lyapunov exponent of SMPL systems under some assumptions has been studied in [9], and later extended to approximate computations under other technical assumptions in [10, p. 251]. The application of model predictive control and system identification to SMPL systems is studied in [15], [16]. An alternative approach to model uncertainties in MPL systems using intervals is discussed in [17], [18], [19].

As we mentioned in the previous paragraph, the existing works on SMPL systems focus on the study of steady-state behaviors: as such, existing approaches cannot distinguish time-dependent dynamical properties of trajectories outside their steady state. This motivates us to develop a new approach for studying *general dynamical properties* of SMPL systems via formal verification. The formal verification approach is based on developing finite-state abstractions and, whilst quite different in the nature of the used techniques and of the models of interest, can be related to the approach discussed in [20] for (deterministic) MPL systems. As discussed shortly, here general dynamical properties are expressed as formulae in a temporal logic, and verification is attained via (probabilistic) model checking. Furthermore this work can also be seen as broad extension of [3, Ch. 9], where the authors discuss the sensitivity of deterministic MPL systems w.r.t. a periodic timetable against disturbances: this contribution focuses on verifying general behaviors of SMPL systems w.r.t. a periodic timetable.

Verification techniques and tools for deterministic, discrete-time, finite-state systems have been widely investigated and developed in the past decades [21], often by means of model checking [22]. The application of formal methods to stochastic models is typically limited to discrete-state structures, either in continuous or in discrete time [22], [23]. Continuous-space models on the other hand require the use of finite abstractions, as it is classically done for example with finite bisimulations of timed automata [24]. With focus on stochastic models with continuous state space, as is the case for SMPL systems, numerical schemes based on Markov Chain (MC) approxi-

S. Esmaeil Zadeh Soudjani and A. Abate are with the Department of Computer Science, University of Oxford, Oxford OX1 2JD, U.K. e-mail: {Sadegh.Soudjani,Alessandro.Abate}@cs.ox.ac.uk.

D. Adzkiya is with the Department of Mathematics, Institut Teknologi Sepuluh Nopember, Surabaya 60111, Indonesia e-mail: dieky@matematika.its.ac.id.

The first two authors have equally contributed to this work.

This work has been supported by the European Commission Marie Curie grant MANTRAS 249295, IAPP project AMBI 324432, and by the John Fell OUP Research Fund.

mations of stochastic systems have been introduced in [25], [26], and applied to the approximate study of probabilistic reachability or invariance in [27], [28], however these finite abstractions do not come with explicit error bounds and as such their use cannot lead to certified guarantees. On the contrary in [29], [30], a technique with formal guarantees has been introduced to provide formal abstractions of discrete-time, continuous-space Markov models, with the objective of investigating their probabilistic invariance [29] by employing probabilistic model checking algorithms over a finite-state MC [30]. In view of scalability and of generality, the approach has been improved in [31], [32] and applied to Probabilistic Computation Tree Logic (PCTL) properties. Furthermore the abstraction approach proposed in [33] allows constructing a single abstraction to be then used for verifying any bounded linear temporal specification. Interestingly, these procedures have been shown [34] to introduce an approximate probabilistic bisimulation of the concrete model [35], which reinforces the quantitative relationship between concrete and abstract models.

***Contributions**:* The aim of this work is to formally verify SMPL systems w.r.t. a periodic timetable via probabilistic model checking, and in particular to characterize and to compute the satisfiability of Bounded Linear Temporal Logic (BLTL) formulae [36]. More precisely, for any allowable initial event time, we determine the probability that the time difference between the occurrence of events and a deterministic periodic timetable satisfies a given BLTL formula (cf. Section II-C). BLTL formulae are a class of Linear Temporal Logic (LTL) formulae where time horizon of the specifications is finite. LTL formulae have been widely used to characterize dynamical properties of numerous models, such as discrete-time linear systems [37], stochastic systems [38], [39], and Markov decision processes [40]. A number of interesting dynamical properties can be expressed as BLTL formulae, e.g. finite-time invariance, finite-time reachability, finite-time reach-avoid, or properties expressed as finite strings over automata.

The approach works as follows. We first interpret a given SMPL system as a discrete-time Markov process, as first suggested by [7], [8]. Then we adapt the techniques in [30], [32], [33] to the structure of the SMPL system, in order to generate a finite abstraction in the form of a finite-state MC, together with guarantees on the level of approximation introduced in the process. The formal approximation is guaranteed to hold over any BLTL formula [33]. The BLTL property over the obtained MC can then be analyzed via probabilistic model checking [22] and computed via existing software [41], [42]. The result obtained from the model checking software is then combined with the approximation guarantees, in order to obtain the probability that the concrete (original) SMPL system satisfies the given property. Throughout the manuscript we discuss the structural assumptions and computational requirements underpinning our results, and examine relaxations and algorithmic improvements aimed towards generalization and scalability.

In order to further elucidate the approach, we discuss the computation of finite-horizon probabilistic invariance, here encoded as a simple BLTL formula, of an SMPL system: more precisely, for any given occurrence time for the initial event, we determine the probability that the time associated with the occurrence of N consecutive events remains close to a given deterministic N-step timetable.

Finally, we conclude by discussing an alternative technique based on the following approach: first, we approximate the original density functions by piecewise polynomial density functions; in the second step, the value function associated with the approximated density functions is computed explicitly using a computer algebra program. We compare the performance of this technique and the abstraction approach: our experiments suggest that the abstraction approach at the core of this work is more scalable, thus reinforcing its potential for applications.

***Structure of this article**:* The article is structured as follows. Initially, Section II-A introduces the SMPL formalism, whereas Section II-C presents the problem of probabilistic model checking of SMPL systems against BLTL specifications. Section III discusses the formal abstraction of an SMPL system as a Markov chain. Section IV describes the quantification of the abstraction error and presents numerical examples, focused on the probabilistic invariance problem. An alternative formal approach for the computation of the solution of the probabilistic invariance problem is discussed in Section V, which is based on the approximation of the density functions with piecewise polynomials. Finally, Section VI concludes this work with future research directions.

***Related work by the authors**:* This manuscript represents an extension and a completion of the results in [43]: there finite abstraction techniques are constructed exclusively towards the solution of the probabilistic invariance problem. This work generalizes [43] and develops abstractions of SMPL systems for model checking against general BLTL specifications. We further elaborate on extensions geared towards computability, and in particular provide a formulation of the abstraction error that is dimension-dependent, and, as such, parallelizable. Moreover, we discuss an alternative formal approach for computation of the solution of the probabilistic invariance problem based on approximation of the density functions with piecewise-polynomial ones.

II. Models and Problem Statement

We introduce the basics of max-plus algebra and of autonomous SMPL systems, and discuss probabilistic model checking of SMPL systems against BLTL specifications, a goal that will be further elaborated throughout the article.

A. Modeling: Stochastic Max-Plus-Linear Systems

The notations $\mathbb{N}$ and $\mathbb{N}_n$ represent the whole positive integers $\{1, 2, \ldots\}$ and the first n positive integers $\{1, 2, \ldots, n\}$, respectively. We use bold letters to denote vectors and indexed letters for the elements of the vector, for instance $\mathbf{x} = [x_1, \ldots, x_n]^T$. Furthermore we define $\mathbb{R}_\varepsilon$ and ε respectively as $\mathbb{R} \cup \{\varepsilon\}$ and $-\infty$. For $\alpha, \beta \in \mathbb{R}_\varepsilon$, introduce the two operations

$$\alpha \oplus \beta = \max\{\alpha, \beta\} \qquad \text{and} \qquad \alpha \otimes \beta = \alpha + \beta,$$

where the element ε is considered to be absorbing w.r.t. $\otimes$ [11, Definition 3.4], namely $\alpha \otimes \varepsilon = \varepsilon$ for all $\alpha \in \mathbb{R}_\varepsilon$. The rules for the order of evaluation of the max-algebraic operators correspond to those in the conventional algebra: max-algebraic multiplication $\otimes$ has a higher precedence than max-algebraic addition $\oplus$ [11, Sec. 3.1].

The basic max-algebraic operations are extended to matrices as follows. If $A, B \in \mathbb{R}_\varepsilon^{m\times n}$; $C \in \mathbb{R}_\varepsilon^{m\times p}$; $D \in \mathbb{R}_\varepsilon^{p\times n}$; and $\alpha \in \mathbb{R}_\varepsilon$, then

$$[\alpha \otimes A]_{ij} = \alpha \otimes A_{ij} = \alpha + A_{ij},$$
$$[A \oplus B]_{ij} = A_{ij} \oplus B_{ij} = \max\{A_{ij}, B_{ij}\},$$
$$[C \otimes D]_{ij} = \bigoplus_{k=1}^{p} C_{ik} \otimes D_{kj} = \max_{k\in\{1,\dots,p\}} \{C_{ik} + D_{kj}\},$$

for each $i \in \mathbb{N}_m$ and $j \in \mathbb{N}_n$. Notice the analogy between $\oplus$, $\otimes$ and respectively $+$, $\times$ for matrix and vector operations in the conventional algebra. In this paper the usual multiplication $\times$ is usually omitted, whereas the max-algebraic multiplication $\otimes$ is always written explicitly. Given $m \in \mathbb{N}$, the m-th max-algebraic power of $A \in \mathbb{R}_\varepsilon^{n\times n}$ is denoted by $A^{\otimes m}$ and corresponds to $A \otimes \cdots \otimes A$ (m times). Notice that max-algebraic power has higher precedence than $\otimes$ and $\oplus$; $A^{\otimes 0}$ is an n-dimensional max-plus identity matrix, i.e. the diagonal and non-diagonal elements are 0 and ε, respectively. In this paper, the following notation is adopted for reasons of convenience. A vector with each component being equal to 0 (resp., $-\infty$) is also denoted by 0 (resp., ε).

An autonomous SMPL system is defined as:

$$\mathbf{x}(k+1) = A(k) \otimes \mathbf{x}(k), \tag{1}$$

where $\mathbf{x}(k) = [x_1(k), \dots, x_n(k)]^T \in \mathbb{R}^n$; each entry of the state matrix $A(k)$ either equals the constant ε, or is an independent and identically distributed random variable w.r.t. $k \in \mathbb{N}$, taking values on the real line; and further $A_{ij}(\cdot)$ are independent for all $i, j \in \mathbb{N}_n$. The random sequence $\{A_{ij}(\cdot)\}$ is then characterized by a given density function $t_{ij}(\cdot)$ and corresponding distribution function $T_{ij}(\cdot)$ (cf. Theorem 1 below). In (1) the independent variable k denotes an increasing deterministic occurrence index, whereas the state variable $\mathbf{x}(k)$ defines the (continuous) time of the k-th occurrence of the discrete events. The state component $x_i(k)$ denotes the time of the k-th occurrence of the i-th event. In this work, the occurrence time of all events is a real number because the state space is $\mathbb{R}^n$ (rather than $\mathbb{R}_\varepsilon^n$): in order to guarantee $\mathbf{x}(k) \in \mathbb{R}^n$ for all k, the random matrix A has to be regular (or row-finite) [3, Sec. 1.2], namely A contains at least one element different from ε in each row. Since this article is based exclusively on autonomous (that is, not non-deterministic) SMPL systems, the adjective will be dropped for simplicity.

In contrast with SMPL systems, deterministic MPL systems are defined according to (1) where the state matrix $A(k)$ is given and event-invariant (independent of k). Under a natural irreducibility condition [11, Definition 2.13] on matrix A, the deterministic MPL system admits periodic regimes, namely there exists a finite sequence of (max-plus) linearly-independent vectors $\{\mathbf{x}^1, \mathbf{x}^2, \dots, \mathbf{x}^\mu\}$ such that $\mathbf{x}^{k+1} = A \otimes \mathbf{x}^k$, $k \in \mathbb{N}_{\mu-1}$, and there is a constant d that satisfies $A \otimes \mathbf{x}^\mu = d \otimes \mathbf{x}^1$. The parameter d and corresponding vectors for the periodic regime $\mathbf{x}^1, \mathbf{x}^2, \dots, \mathbf{x}^\mu$ represent the max-plus eigenvalue and its associated eigenvectors of matrix $A^{\otimes\mu}$, respectively [6, Sec. 2.5.3]. Such periodic regimes are essential ingredients in the analysis and design of timetables for real applications [44] modeled as MPL systems.

Example 1: Consider the following SMPL system representing a simple railway network between two connected stations. The state variables $x_i(k)$ for $i \in \mathbb{N}_2$ denote the time of the k-th departure at station i:

$$\mathbf{x}(k+1) = A(k) \otimes \mathbf{x}(k),$$
$$= \begin{bmatrix} 2 + e_{11}(k) & 5 + e_{12}(k) \\ 3 + e_{21}(k) & 3 + e_{22}(k) \end{bmatrix} \otimes \mathbf{x}(k),$$

or equivalently,

$$x_1(k+1) = \max\{2 + e_{11}(k) + x_1(k), 5 + e_{12}(k) + x_2(k)\},$$
$$x_2(k+1) = \max\{3 + e_{21}(k) + x_1(k), 3 + e_{22}(k) + x_2(k)\},$$

where we have assumed that $e_{11}(\cdot) \sim Exp(2)$, $e_{12}(\cdot) \sim Exp(4/5)$, $e_{21}(\cdot) \sim Exp(4/3)$, and $e_{22}(\cdot) \sim Exp(4/3)$, and $Exp(\lambda)$ represents the exponential distribution with rate λ. Notice that $A_{ij}(\cdot)$ denotes the traveling time from station j to station i and amounts to a deterministic constant plus a delay modeled by the random variable $e_{ij}(\cdot)$. A few sample trajectories of the SMPL system, initialized at $\mathbf{x}(0) = [1, 0]^T$, are displayed in Fig. 1 (left). Note that when all random delays are assumed to be equal to zero, the resulting deterministic system

$$\mathbf{s}(k+1) = A_d \otimes \mathbf{s}(k),\ A_d = \begin{bmatrix} 2 & 5 \\ 3 & 3 \end{bmatrix},\ \mathbf{s}(0) = \mathbf{x}(0), \tag{2}$$

admits the unique solution $\mathbf{s}(k) = \mathbf{s}(0) + dk = [1 + 4k, 4k]^T$, where $d = 4$ is the max-plus eigenvalue of matrix A_d, and $\mathbf{s}(0) = [1, 0]^T$ is a corresponding eigenvector of the deterministic MPL system. Then the initial condition $\{\mathbf{s}(0)\}$ is associated with a periodic regime with period $\mu = 1$, and the associated periodic trajectory can be used as a timetable (cf. Section II-B) for the train departures. Note that in this particular example the increasing sequence $\{\mathbf{s}(k)\}$ provides a lower bound on the SMPL trajectories $\mathbf{x}(k)$, due to the positive supports of the density functions for the delays $e_{ij}(\cdot)$, as visible in Fig. 1 (left). □

B. Properties of Interest

Let us consider events that are scheduled to occur periodically, that is assume there is a *periodic timetable* where each event is repeated at regular intervals characterized by the cycle time $d \in \mathbb{R}$. For instance a periodic railway timetable defines the scheduled arrival and departure times within a basic period of length d for each periodic train line at all served stations. As discussed in Section I, stochastic delays due to transportation times and train interactions are an unavoidable characteristic of real-world railway networks: it is therefore meaningful to study and analyze properties of a railway timetable w.r.t. daily transportation time variations. For instance, stability and recoverability properties of a timetable associated to an SMPL system representing a railway network are studied in [44]. In

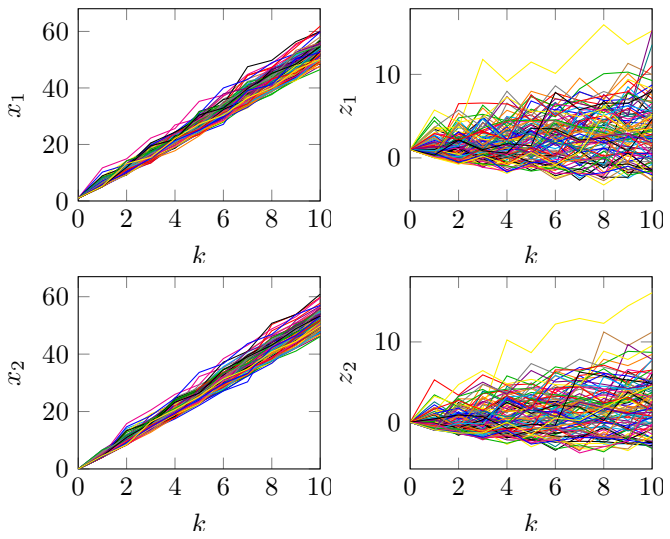

Fig. 1. The left and right plots represent 100 sample trajectories of the SMPL system in Examples 1 and 2 for 10 discrete steps (horizontal axis), respectively. Notice the different scales for the vertical axes.

this work, we consider probabilistic model checking of the SMPL system in (1) against a specification w.r.t. a periodic timetable. More specifically, for each possible time of initial occurrence of all the events ($x_i(0), i \in \mathbb{N}_n$), we are interested in determining the probability that the difference of the time of k-th occurrence of all events ($\mathbf{x}(k)$) and the corresponding time of the periodic timetable satisfies a given BLTL formula, for $k \in \mathbb{N}_N \cup \{0\}$. For instance, we may want to determine the probability that the time of the occurrence of all events is at least 5 time units ahead of the corresponding events in the periodic timetable, as well as at most 5 time units behind it: this example deals with an invariance property, where the (bounded) invariant set is defined as the desired time of occurrence of all events w.r.t. the periodic timetable.

Let us formally define a periodic timetable: $\mathbf{s}(\cdot)$ is called a periodic timetable with cycle time $d > 0$ and (arbitrary) initial time $\mathbf{s}(0) = \mathbf{s}_0 \in \mathbb{R}^n$, if the successive scheduled event times are given by the deterministic MPL system $\mathbf{s}(k+1) = d \otimes \mathbf{s}(k)$. In our analysis the periodic timetable can be freely selected: for instance, it can be an arbitrary function of the periodic regimes of the SMPL system in the absence of stochastic delays (cf. (2) in Example 1, where a periodic trajectory is generated from a fixed initial condition in the eigenspace of the model). The mean behavior of the SMPL system, which is proved in general to be eventually periodic [44], may also be selected as the given timetable.

Since we are interested in delays of event occurrences w.r.t. the given timetable, we introduce new variables $\mathbf{z}(\cdot)$ defined as the difference between the states of the original SMPL system in (1) and those of the periodic timetable $\mathbf{s}(\cdot)$, i.e. $\mathbf{z}(k) = \mathbf{x}(k) - \mathbf{s}(k)$, and $\mathbf{z}(k) = [z_1(k), \dots, z_n(k)]^T \in \mathbb{R}^n$ for $k \in \mathbb{N} \cup \{0\}$. The dynamics of $\mathbf{z}(\cdot)$ are given by

$$z_i(k+1) = \max\{A_{i1}(k) - d + x_1(k) - s_i(k), \dots \\ \dots, A_{in}(k) - d + x_n(k) - s_i(k)\},$$

for $i \in \mathbb{N}_n$. From the dynamics of $\mathbf{s}(k)$, we obtain $s_i(k) - s_j(k) = s_i(0) - s_j(0)$ for all $i, j \in \mathbb{N}_n$ and $k \in \mathbb{N} \cup \{0\}$. Then we substitute $s_i(k) = s_i(0) - s_j(0) + s_j(k)$ to the j-th term of the equation for $z_i(k+1)$, and further substitute $x_i(k) - s_i(k)$ by $z_i(k)$ to obtain

$$z_i(k+1) = \max\{A_{i1}(k) + s_1(0) - s_i(0) - d + z_1(k), \dots \\ \dots, A_{in}(k) + s_n(0) - s_i(0) - d + z_n(k)\}.$$

In matrix notation, the dynamics of the newly introduced SMPL system are then given by

$$\mathbf{z}(k+1) = [A(k) + D] \otimes \mathbf{z}(k), \tag{3}$$

where $D = [d_{ij}]_{i,j} \in \mathbb{R}^{n \times n}$ (i.e. d_{ij} is the entry of matrix D at row i and column j), $d_{ij} = s_j(0) - s_i(0) - d$. Notice that $A_{ij}(k) \otimes d_{ij}$ are independent for all $k \in \mathbb{N} \cup \{0\}$ and $i, j \in \mathbb{N}_n$. The density (resp., distribution) function of $A_{ij}(k) \otimes d_{ij}$ corresponds to the density (resp., distribution) function of $A_{ij}(k)$ shifted forward of d_{ij} units. In (3) the deterministic index k again denotes an increasing occurrence index, whereas the state variable $\mathbf{z}(k)$ defines the delay w.r.t. the schedule of the k-th occurrence of all events: in particular the state component $z_i(k)$ denotes the delay w.r.t. the schedule of k-th occurrence of the i-th event. Notice that if the delay is negative then the event occurs ahead of the schedule, whereas if the delay is positive then the event occurs behind the schedule.

As confirmed by Example 1, the trajectories of the SMPL system (1) are lower bounded by a monotonically increasing sequence under some weak conditions on the density functions $t_{ij}(\cdot)$[1]. This condition results in a potentially very large state space for the state variable $\mathbf{x}(\cdot)$. In contrast, the timing of events w.r.t. to the timetable, encompassed by $\mathbf{z}(\cdot)$, belongs to a substantially smaller set $\mathcal{Z}$: this is beneficial since it will reduce the computational complexity of our abstraction, as detailed later.

Example 2: Consider the SMPL system in Example 1. Sample trajectories of the new SMPL system associated with $\mathbf{s}(0) = [0, 0]^T$ and $d = 5$ are depicted in Fig. 1 (right). □

The next theorem shows that, much like the original model in (1), the new SMPL system can be described as a discrete-time homogeneous Markov process.[2] A Markov process is a stochastic process where the probability distribution of the next state depends only on the current state.

Theorem 1: The SMPL system in (3) is fully characterized by the following conditional density function

$$t_z(\bar{\mathbf{z}}|\mathbf{z}) = \prod_{i=1}^{n} t_i(\bar{z}_i|\mathbf{z}) \quad \text{where}$$

$$t_i(\bar{z}_i|\mathbf{z}) = \sum_{j=1}^{n} \left[t_{ij}(\bar{z}_i - d_{ij} - z_j) \prod_{\substack{k=1 \\ k \neq j}}^{n} T_{ik}(\bar{z}_i - d_{ik} - z_k) \right]$$

for $i \in \mathbb{N}_n$. □

The proof of Theorem 1 appears in Appendix A.

[1]More precisely, it can be shown that if $A_{ij}(k) \geq \underline{a}_{ij} > 0$, such that $\underline{A} = [\underline{a}_{ij}]_{i,j}$ is irreducible, then there exists a subsequence of $\mathbf{x}(k)$ that is bounded element-wise from below by a monotonically increasing sequence.

[2]Note that this result can be generalized to multi-periodic timetables, namely timetables characterized by $\mathbf{s}(k+1) = \mathbf{d} \otimes \mathbf{s}(k)$, where $\mathbf{d} \in \mathbb{R}^{n \times n}$ is a diagonal matrix, whereas in periodic timetables the cycle time is a scalar. However the associated Markov process becomes inhomogeneous, which greatly increases the computational complexity of the discussed procedures.

C. Problem Statement: Probabilistic Model Checking of SMPL Systems Against BLTL Formulae

We present some basic definitions to formalize the probabilistic model checking problem on the SMPL system in (3). We introduce a set of finitely many atomic propositions AP and a labeling function $L : \mathcal{Z} \to 2^{AP}$. Notation 2^{AP} denotes the power set of AP. Atomic propositions intuitively express simple facts about the states of the system, or can be thought of as properties associated to the states (e.g., "initial," "safe," or "target" states). The labeling function L relates a set $L(\mathbf{z}) \in 2^{AP}$ of atomic propositions to any state $\mathbf{z} \in \mathcal{Z}$. The set $L(\mathbf{z})$ represents the atomic propositions that are satisfied by state $\mathbf{z}$.

BLTL is a fragment of LTL, made up of formulae where the time horizon of the specifications is bounded [33, Sec. 2.4]. This class of formulae has been recently employed in statistical model checking of stochastic systems [39]. Recall that an LTL formula consists of atomic propositions, of Boolean connectors, and of two temporal modalities: $\bigcirc$ (pronounced "next") and U (pronounced "until"). BLTL formulae are instead obtained with only the temporal modality $\bigcirc$. More formally, the syntax of BLTL over the set of atomic propositions AP is given by the following grammar:

$$\varphi \quad ::= \quad a \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \bigcirc\varphi,$$

where $a \in AP$. The semantics of BLTL formulae are inherited from those of LTL formulae [45, Sec. 5.1.2].

We define the probabilistic model-checking problem over a BLTL specification as follows. Given the SMPL system in (3), a set of atomic propositions AP, a labeling function L, an initial state $\mathbf{z}(0) \in \mathcal{Z}$, and a BLTL formula φ, find the probability that the trajectory starting from state $\mathbf{z}(0)$ satisfies φ:

$$\Pr\{\mathbf{z}(0) \vDash \varphi\}. \tag{4}$$

BLTL formulae can express well-known bounded-time verification problems, such as probabilistic reachability, reach-avoid, and invariance (safety) [36, p. 220]. In order to make the discussion as clear as possible, we provide the details of the construction of a BLTL formula associated with the simplest problem of invariance. The finite-horizon probabilistic invariance problem amounts to evaluating the probability that a finite execution associated with the initial condition $\mathbf{z}(0)$ remains inside a given invariant set $\mathcal{A}$ during the finite event horizon N, as follows:

$$P_{\mathbf{z}_0}(\mathcal{A}) = \Pr\{\mathbf{z}(k) \in \mathcal{A} \text{ for all } k \in \mathbb{N}_N \cup \{0\} | \mathbf{z}(0) = \mathbf{z}_0\}, \tag{5}$$

where $\mathcal{A}$ is assumed to be Borel measurable (that is, constructed from open sets via operations of countable union, countable intersection, and relative complement). Define the set of atomic propositions $AP = \{a\}$ and the labeling function as $L(\mathbf{z}) = \{a\}$ if $\mathbf{z} \in \mathcal{A}$ and $L(\mathbf{z}) = \emptyset$ if $\mathbf{z} \notin \mathcal{A}$. Consider a BLTL formula given by

$$\square^{\leq N} a = a \wedge \bigcirc a \wedge \bigcirc\bigcirc a \wedge \cdots \wedge \underbrace{\bigcirc\bigcirc\cdots\bigcirc}_{N \text{times}} a.$$

Then the probabilistic invariance can be characterized as the following probability: $\Pr\{\mathbf{z}(0) \vDash \square^{\leq N} a\}$. This quantity, or more generally the expression in (4), is numerically computed over finite-space models such as Markov chains, via known existing software PRISM [41]. An explicit characterization of probabilistic invariance is provided in Proposition 2 and can indeed be computed in PRISM. On the other hand, the characterization over models of interest in this work requires the approach discussed next, and will leverage the software FAUST^2 [46], to be discussed below.

input: SMPL system (3) and labeling function $L : \mathcal{Z} \to 2^{AP}$
output: A finite-state MC $(\mathcal{P}, T_p)$

1: Select a finite partition of the state space $\mathcal{Z}$ of cardinality m, as $\mathcal{Z} = \cup_{i=1}^{m} \mathcal{Z}_i$, such that all states in a partition set satisfy the same set of atomic propositions
2: For each $\mathcal{Z}_i$, select a single representative point $\mathbf{z}_i \in \mathcal{Z}_i$
3: Define $\mathcal{P} = \{\phi_i, i \in \mathbb{N}_m\}$ as the finite state space of the MC
4: Compute the transition probability matrix T_p as

$$T_p(\phi_i, \phi_j) = \int_{\Xi(\phi_j)} t_z(\bar{\mathbf{z}}|\mathbf{z}_i) d\bar{\mathbf{z}}, \quad \text{for all } i, j \in \mathbb{N}_m.$$

5: Define the induced labeling function $L_p : \mathcal{P} \to 2^{AP}$ for the MC as $L_p(\phi_i) = L(\mathbf{z}_i)$ for all $i \in \mathbb{N}_m$

Fig. 2. Algorithm 2. Generation of a finite-state MC from an SMPL system and a labeling function L.

III. Abstractions by Finite-State Markov Chains

We resort to the abstraction procedure presented in [30, Sec. 3.1], properly extended to the models under study. The procedure generates a finite-state MC $(\mathcal{P}, T_p)$ from a given SMPL system (3), a set of finitely many atomic propositions AP, and a labeling function $L : \mathcal{Z} \to 2^{AP}$. We employ the obtained MC to approximately model check the SMPL system against a given BLTL specification defined over the atomic propositions AP.

Let $\mathcal{P} = \{\phi_1, \ldots, \phi_m\}$ be a set of finitely many discrete states, and $T_p : \mathcal{P} \times \mathcal{P} \to [0, 1]$ a related transition probability matrix, such that $T_p(\phi_i, \phi_j)$ characterizes the probability of transitioning from state ϕ_i to state ϕ_j and thus induces a conditional discrete probability distribution over the finite space $\mathcal{P}$. Given a labeling function L, the algorithm in Fig. 2 provides a procedure to abstract an SMPL system by a finite-state MC.[3] The set $\mathcal{P} = \{\phi_1, \ldots, \phi_m\}$ denotes the discrete state space of cardinality m. In Algorithm 2, $\Xi : \mathcal{P} \to 2^{\mathcal{Z}}$ represents the concretization function, i.e. a set-valued map that associates to any discrete state (point) $\phi_i \in \mathcal{P}$ the corresponding continuous partition set $\mathcal{Z}_i \subset \mathcal{Z}$.

Remark 1: The bottleneck of Algorithm 2 lies in the computation of transition probability matrix T_p (step 4), due to the integration of kernel t_z. The required number of integrations is m^2, where m represents the cardinality of the set of discrete states. This integration can be circumvented if the distribution functions $T_{ij}(\cdot)$ for all $i, j \in \mathbb{N}_n$ have explicit analytical form (e.g. an exponential distribution).

[3]For simplicity, when referring to an algorithm we will use the term "Algorithm 2" rather than "the Algorithm in Fig. 2."

The abstraction procedure in Algorithm 2 preserves the underlying labels, and has been shown to introduce an approximate probabilistic bisimulation of the concrete model [35], [34]. This means that Algorithm 2 can be applied to abstract an SMPL system as a finite-state MC, regardless of the particular BLTL specification. As discussed below, the quantification of the abstraction error in Section IV requires that the state space $\mathcal{Z}$ is bounded. □

Considering the obtained finite-state, discrete-time MC $(\mathcal{P}, T_p)$ and the induced labeling function L_p, the BLTL model checking problem amounts to evaluating the probability that an execution associated with the initial condition $\phi(0) \in \mathcal{P}$ satisfies a given BLTL specification φ expressed over the labels induced by function L_p. This can be stated as the following probability:

$$\Pr\{\phi(0) \vDash \varphi\}. \tag{6}$$

In general, the solution can be obtained by leveraging probabilistic model checking software [41], [42]. In the special case of a BLTL specification representing finite-horizon invariance, the solution can also be characterized using dynamic programming, as shown in Section IV-B. The next section discusses the error associated to the general abstraction procedure, and presents numerical examples focused on the simple finite-horizon invariance problem.

IV. Quantification of the Abstraction Error

This section starts by precisely defining the error related to the abstraction procedure, which is due to the approximation of a continuous concrete model by a finite discrete one. A bound on the abstraction error in [32] is applied to the BLTL model checking problem under some structural assumptions, namely in the case of Lipschitz-continuous density functions, or alternatively of piecewise Lipschitz-continuous density functions.

The abstraction error is defined as the maximum difference between the outcomes obtained by (4) and (6) for any pair of initial conditions $\mathbf{z}(0) \in \mathcal{Z}$ and $\xi(\mathbf{z}(0)) \in \mathcal{P}$, where the abstraction function $\xi : \mathcal{Z} \to \mathcal{P}$ associates to any point $\mathbf{z} \in \mathcal{Z}$ on the SMPL state space, the corresponding discrete state $\xi(\mathbf{z}) \in \mathcal{P}$. Since an exact computation of this error is not possible in general, we resort to determining an upper bound of the abstraction error, which is denoted as E. More formally, we are interested in quantifying E that satisfies

$$|\Pr\{\mathbf{z}(0) \vDash \varphi\} - \Pr\{\xi(\mathbf{z}(0)) \vDash \varphi\}| \leq E, \tag{7}$$

for all $\mathbf{z}(0) \in \mathcal{Z}$ and any BLTL formula φ. Notice that the quantification of this error allows making sense of the results obtained from model checking the MC ($\Pr\{\xi(\mathbf{z}(0)) \vDash \varphi\}$) for the verification of the SMPL system ($\Pr\{\mathbf{z}(0) \vDash \varphi\}$).

We raise the following assumption on the SMPL system in (1) and in (3). Recall that the density function of $A_{ij}(k) \otimes d_{ij}$ in (3) corresponds to the density function of $A_{ij}(k)$ in (1) shifted d_{ij} units forward.

Assumption 1: The density functions $t_{ij}(\cdot)$ for $i, j \in \mathbb{N}_n$ are bounded:

$$t_{ij}(z) \leq M_{ij} \quad \text{for all } z \in \mathbb{R}. \qquad \square$$

Assumption 1 implies that the distribution functions $T_{ij}(\cdot)$ for $i, j \in \mathbb{N}_n$ are Lipschitz-continuous. Recall that the (global) Lipschitz constant of a one-dimensional function can be computed as the maximum of the absolute value of the first derivative of the function. Thus

$$|T_{ij}(z) - T_{ij}(z')| \leq M_{ij}|z - z'| \quad \text{for all } z, z' \in \mathbb{R}.$$

For the computation of the bound on the abstraction error, we use the following result based on [32], which has inspired most of this work.

Proposition 1 ([32, pp. 933-934]): Suppose Assumption 1 holds and the density function $t_z(\bar{\mathbf{z}}|\mathbf{z})$ satisfies the condition

$$\int_{\mathcal{Z}} |t_z(\bar{\mathbf{z}}|\mathbf{z}) - t_z(\bar{\mathbf{z}}|\mathbf{z}')| d\bar{\mathbf{z}} \leq H\|\mathbf{z} - \mathbf{z}'\| \quad \text{for all } \mathbf{z}, \mathbf{z}' \in \mathcal{Z},$$

then an upper bound on the abstraction error in (7) is $E = NH\delta$, where N is the horizon of the specification φ and $\delta = \max\{\|\mathbf{z} - \mathbf{z}'\| \text{ s.t. } z, z' \in \mathcal{Z}_i \text{ and } i \in \mathbb{N}_m\}$ is the diameter. □

The horizon of the BLTL specification is easily computed on the syntax of the formula [33, Sec. 2.4]. Proposition 1 shows that the upper bound on the abstraction error depends on the partition diameter (cf. step 1 of Algorithm 2). Recall that the cardinality of the partition in step 1 of Algorithm 2 is finite. Thus in order to guarantee that δ is finite, the state space has to be bounded. This restriction requires us to truncate the state space into a bounded set while maintaining the whole dynamics of the system. In order to do so, assume the density function of the initial state and that of entries of state matrix A have bounded support[4]. This assumption enables us to compute bounds on the support of finite trajectories of the SMPL system in (3), which in turn can be used to construct a bounded state space [18]. On the other hand, for some BLTL specifications it is not required to partition the whole state space: for instance, in the case of invariance only the boundedness of the invariant set is required for the abstraction procedure.

In the remainder of this section, we first determine the constant H for Lipschitz-continuous density functions, then generalize the result to piecewise Lipschitz-continuous density functions. We reformulate the upper bound on the abstraction error as a summation of dimension-dependent terms. Finally we provide a simple application to the study of the probabilistic invariance problem.

A. Lipschitz-Continuous Density Functions

Assumption 2: The density functions $t_{ij}(\cdot)$ for $i, j \in \mathbb{N}_n$ are Lipschitz-continuous, namely there exist finite and positive constants h_{ij}, such that

$$|t_{ij}(z) - t_{ij}(z')| \leq h_{ij}|z - z'| \quad \text{for all } z, z' \in \mathbb{R}. \qquad \square$$

Assumption 2 requires the density functions $t_{ij}(\cdot)$ to be continuous and to have bounded one-sided derivatives.

Under Assumptions 1 and 2, the conditional density function $t_z(\bar{\mathbf{z}}|\mathbf{z})$ is Lipschitz-continuous. This opens up the application

[4]If instead $t_{ij}(\cdot)$ has an unbounded support, we must truncate it to a bounded one. This introduces another error on top of the abstraction error presented in this section, see [47] for more details.

of the results in [30], [32] for the approximate solution of the probabilistic invariance problem. Notice that the Lipschitz constant of $t_z(\bar{\mathbf{z}}|\mathbf{z})$ may be large, which implies a rather conservative upper bound on the abstraction error. To improve this bound, we can instead directly use Proposition 1 presented before – an option also discussed in [32]. In particular we present three technical lemmas that are essential for the computation of the constant H with proofs appearing in Appendix A. After the derivation of the improved bound, the obtained results are applied to a numerical example.

Lemma 1: Any one-dimensional continuous distribution function $T(\cdot)$ satisfies the inequality

$$\int_{\mathbb{R}} |T(\bar{z}-z)-T(\bar{z}-z')|d\bar{z} \leq |z-z'| \quad \text{for all } z, z' \in \mathbb{R}. \ \square$$

Lemma 2: Suppose the random vector $\bar{\mathbf{z}}$ can be organized as $\bar{\mathbf{z}} = [\bar{\mathbf{z}}_1^T, \bar{\mathbf{z}}_2^T]^T$, so that its conditional density function is the multiplication of the conditional density functions of $\bar{\mathbf{z}}_1, \bar{\mathbf{z}}_2$ as:

$$f(\bar{\mathbf{z}}|\mathbf{z}) = f_1(\bar{\mathbf{z}}_1|\mathbf{z}) f_2(\bar{\mathbf{z}}_2|\mathbf{z}).$$

Then it holds that

$$\int_{\mathcal{Z}} |f(\bar{\mathbf{z}}|\mathbf{z}) - f(\bar{\mathbf{z}}|\mathbf{z}')|d\bar{\mathbf{z}} \leq \sum_{i=1}^{2} \int_{\Pi_i(\mathcal{Z})} |f_i(\bar{\mathbf{z}}_i|\mathbf{z}) - f_i(\bar{\mathbf{z}}_i|\mathbf{z}')|d\bar{\mathbf{z}}_i,$$

with $\Pi_i(\cdot)$ the projection operator on the i-th axis. $\square$

Lemma 3: Suppose the vector $\mathbf{z}$ can be organized as $\mathbf{z} = [\mathbf{z}_1^T, \mathbf{z}_2^T]^T$, and that the density function of the conditional random variable $(\bar{z}|\mathbf{z})$ is of the form

$$f(\bar{z}|\mathbf{z}) = f_1(\bar{z}, \mathbf{z}_1) f_2(\bar{z}, \mathbf{z}_2),$$

where $f_1(\bar{z}, \mathbf{z}_1), f_2(\bar{z}, \mathbf{z}_2)$ are bounded non-negative functions with $M_1 = \sup f_1(\bar{z}, \mathbf{z}_1)$ and $M_2 = \sup f_2(\bar{z}, \mathbf{z}_2)$. Then for a given set $\mathcal{C} \in \mathcal{B}(\mathbb{R})$:

$$\begin{aligned}\int_{\mathcal{C}} |f(\bar{z}|\mathbf{z}_1, \mathbf{z}_2) - f(\bar{z}|\mathbf{z}_1', \mathbf{z}_2')|d\bar{z} \\ \leq M_2 \int_{\mathcal{C}} |f_1(\bar{z}, \mathbf{z}_1) - f_1(\bar{z}, \mathbf{z}_1')|d\bar{z} \\ + M_1 \int_{\mathcal{C}} |f_2(\bar{z}, \mathbf{z}_2) - f_2(\bar{z}, \mathbf{z}_2')|d\bar{z}. \quad \square\end{aligned}$$

Theorem 2: Under Assumptions 1 and 2, the constant H in Proposition 1 is

$$H = \sum_{i,j=1}^{n} H_{ij} + (n-1)M_{ij},$$

where $H_{ij} = \mathcal{L}_i h_{ij}$, and where the constant $\mathcal{L}_i = \mathcal{L}(\Pi_i(\mathcal{Z}))$ is the Lebesgue measure of the projection of the bounded state space onto the i-th axis. $\square$

In the next section we clarify the derivation of the quantities above over the computation of the probabilistic invariance as in (5). The case study utilizes a beta distribution to characterize delays. The motivation for employing a beta distribution is that its density function has a bounded support. Thus by scaling and shifting the density function, we can construct a distribution taking positive real values within an interval. This is reasonable, since this distribution is used to model processing or transportation times, and as such it can only take positive values. Another reason for using a beta distribution is that it can approximate the normal distribution with arbitrary accuracy.

Definition 1 (Beta Distribution): The general formula for the density function of the beta distribution is

$$t(x; \alpha, \beta, a, b) = \frac{(x-a)^{\alpha-1}(b-x)^{\beta-1}}{B(\alpha,\beta)(b-a)^{\alpha+\beta-1}} \qquad \text{if } a \leq x \leq b,$$

and 0 otherwise, where $\alpha, \beta > 0$ are the shape parameters; the interval $[a, b]$ is the support of the density function; and $B(\cdot,\cdot)$ is the beta function. A random variable X characterized by this distribution is denoted by $X \sim Beta(\alpha, \beta, a, b)$. $\square$

The case where $a = 0$ and $b = 1$ is called the standard beta distribution. Notice that the density function of the beta distribution is unbounded if any of the shape parameters belongs to the interval $(1, 2)$. Let us remark that if the shape parameters are positive integers, the beta distribution has a piecewise polynomial density function, which has been used in the literature for the identification of SMPL systems [16, Sec. 4.3].

B. Application to the Probabilistic Invariance Problem

In this section we characterize explicitly the probabilistic invariance problem (5) using dynamic programming. We discuss the construction of a finite-state MC from the original SMPL system (3), and describe a computable solution over the finite-state MC via dynamic programming. The next proposition provides a theoretical framework to study the finite-horizon probabilistic invariance problem in (5).

Proposition 2 ([29, Lemma 1]): Consider value functions $V_k : \mathcal{Z} \to [0, 1]$, for $k \in \mathbb{N}_N \cup \{0\}$, computed through the following backward recursion:

$$V_k(\mathbf{z}) = \mathbb{1}_{\mathcal{A}}(\mathbf{z}) \int_{\mathcal{A}} V_{k+1}(\bar{\mathbf{z}}) t_z(\bar{\mathbf{z}}|\mathbf{z}) d\bar{\mathbf{z}} \quad \text{for all } \mathbf{z} \in \mathcal{Z},$$

and initialized with $V_N(\mathbf{z}) = \mathbb{1}_{\mathcal{A}}(\mathbf{z})$ for all $\mathbf{z} \in \mathcal{Z}$. Then $\Pr\{\mathbf{z}(0) \vDash \square^{\leq N} a\} = V_0(\mathbf{z}(0))$. $\square$

The notation $\mathbb{1}_{\mathcal{A}} : \mathcal{Z} \to \{0, 1\}$ denotes the indicator function of the invariant set $\mathcal{A} \subseteq \mathcal{Z}$, i.e. $\mathbb{1}_{\mathcal{A}}(\mathbf{z}) = 1$ if $\mathbf{z} \in \mathcal{A}$ and $\mathbb{1}_{\mathcal{A}}(\mathbf{z}) = 0$ if $\mathbf{z} \notin \mathcal{A}$. For any $k \in \mathbb{N}_N \cup \{0\}$, notice that $V_k(\mathbf{z})$ represents the probability that an execution of the SMPL system (3) remains within the invariant set $\mathcal{A}$ over the residual event horizon $\{k, \ldots, N\}$, starting from $\mathbf{z}$ at event step k. This result characterizes the finite-horizon probabilistic invariance problem as a dynamic programming problem.

In order to compute approximate solution of the invariance problem (5), Algorithm 2 can be employed to abstract the SMPL system in (3). We select a partition that is proposition-preserving: in other words, the selected partition for the state space $\mathcal{Z}$ is the union of partition for the invariant set $\mathcal{A}$ and that for the complement of the invariant set $\mathcal{Z}\backslash\mathcal{A}$ (as shown in [30], [32], $\mathcal{Z}\backslash\mathcal{A}$ can be simply regarded as another partition set).

Considering the obtained finite-state, discrete-time MC $(\mathcal{P}, T_p)$ with the initial condition $\phi(0)$ and the induced labeling function L_p, the probabilistic invariance problem amounts to evaluating the following probability: $\Pr\{\phi(0) \vDash \square^{\leq N} a\}$.

We define the invariant set $\mathcal{A}_p$ as the set of discrete states that satisfy the atomic proposition a, i.e. $\mathcal{A}_p = \{\phi \in \mathcal{P} \mid L_p(\phi) = \{a\}\}$. The solution of the finite-horizon probabilistic invariance problem over the MC abstraction can be determined via a discrete version of Proposition 2, as follows.

Proposition 3: Consider value functions $V_k^p : \mathcal{P} \to [0,1]$, for $k \in \mathbb{N}_N \cup \{0\}$, computed through the following backward recursion:

$$V_k^p(\phi) = \mathbb{1}_{\mathcal{A}_p}(\phi) \sum_{\bar{\phi} \in \mathcal{P}} V_{k+1}^p(\bar{\phi}) T_p(\phi, \bar{\phi}) \quad \text{for all } \phi \in \mathcal{P},$$

initialized with $V_N^p(\phi) = \mathbb{1}_{\mathcal{A}_p}(\phi)$ for all $\phi \in \mathcal{P}$. Then $\Pr\{\phi(0) \vDash \Box^{\leq N} a\} = V_0^p(\phi(0))$. □

For any $k \in \mathbb{N}_N \cup \{0\}$, notice that $V_k^p(\phi)$ represents the probability that an execution of the finite-state MC remains within the discrete invariant set $\mathcal{A}_p$ over the residual event horizon $\{k, \dots, N\}$, starting from ϕ at event step k. The quantities in Proposition 3 can be easily computed via linear algebra operations.

Example 3: We apply the results in Theorem 2 to the two-dimensional system (3), where $A_{ij}(\cdot) \sim Beta(2, 2, 0, b_{ij})$, $i, j \in \mathbb{N}_2$, $b_{11} = 4$, $b_{12} = 10$, $b_{21} = 6 = b_{22}$. Skipping the details of the direct calculations, the supremum and the Lipschitz constant of the density functions are respectively

$$\begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix} = \begin{bmatrix} 3/8 & 3/20 \\ 1/4 & 1/4 \end{bmatrix}, \begin{bmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{bmatrix} = \begin{bmatrix} 3/8 & 3/50 \\ 1/6 & 1/6 \end{bmatrix}.$$

Considering a periodic timetable with $\mathbf{s}(0) = [0,0]^T$ and $d = 4$, selecting invariant set $\mathcal{A} = [-5,5]^2$, and event horizon $N = 5$, according to Theorem 2 and Proposition 1 we obtain an abstraction error $E = 43.5\delta$. In order to obtain an abstraction error bounded by $E = 0.1$, we would need to discretize set $\mathcal{A}$ uniformly with 6152 bins per each dimension (step 1 of Algorithm 2). The representative points have been selected at the center of the squares obtained by uniform discretization (step 2). The obtained finite-state MC has $m = 6152^2 + 1$ discrete states (step 3), where the additional state [30], [32] is considered as the representative point of the partition set $\mathcal{Z} \backslash \mathcal{A}$. The solution of the invariance problem obtained over the abstract model (cf. Proposition 3) is depicted in Fig. 3 (left panel). It is computed via the software tool FAUST^2 [46], which is implemented in MATLAB and available for download. □

C. Piecewise Lipschitz-Continuous Density Functions

The structural assumptions raised in Section IV-A limit the general applicability of the work. For the sake of generality, we extend the previous results to models aligned with the following requirement.

Assumption 3: The density functions $t_{ij}(\cdot)$ for $i, j \in \mathbb{N}_n$ are piecewise Lipschitz-continuous, namely there exist partitions $\mathbb{R} = \cup_{k=1}^{m_{ij}} D_{ij}^k$ and corresponding finite and positive constants h_{ij}^k, such that

$$|t_{ij}^k(z) - t_{ij}^k(z')| \leq h_{ij}^k |z - z'| \text{ for all } k \in \mathbb{N}_{m_{ij}}; z, z' \in D_{ij}^k,$$
$$t_{ij}(z) = \sum_{k=1}^{m_{ij}} t_{ij}^k(z) \mathbb{1}_{D_{ij}^k}(z) \text{ for all } z \in \mathbb{R}. \quad \square$$

This alternative assumption relaxes Assumption 2, allowing discontinuities in the density functions $t_{ij}(\cdot)$: this makes the results applicable to a wider class of SMPL systems.

The notation k used in Assumption 3 does not denote a power, nor the occurrence index in (1), it is the index of a set in the partition of cardinality $\sum_{i,j} m_{ij}$. Notice that if Assumption 3 holds and the density functions are Lipschitz-continuous, then Assumption 2 is automatically satisfied with $h_{ij} = \max_k h_{ij}^k$. In other words, with Assumption 3 we allow relaxing Assumption 2 to hold only within arbitrary sets partitioning the state space of the SMPL system. For instance, as expected for the probabilistic invariance problem we may limit the assumption to hold within the invariant set.

Under Assumptions 1 and 3, we now present a result extending Theorem 2 for the computation of the constant H.

Theorem 3: Under Assumptions 1 and 3, the constant H in Proposition 1 is

$$H = \sum_{i,j=1}^{n} H_{ij} + (n-1) M_{ij},$$

where $H_{ij} = \mathcal{L}_i \max_k h_{ij}^k + \sum_k |J_{ij}^k|$ and $\mathcal{L}_i = \mathcal{L}(\Pi_i(\mathcal{Z}))$. The notation $J_{ij}^k = \lim_{z \downarrow c_{ij}^k} t_{ij}(z) - \lim_{z \uparrow c_{ij}^k} t_{ij}(z)$ denotes the jump distance of the density function $t_{ij}(\cdot)$ at the k-th discontinuity point c_{ij}^k. □

The proof is similar to that of Theorem 2, the only difference being in the computation of constant H_{ij} for the inequality

$$\int_{\Pi_i(\mathcal{Z})} |t_{ij}(\bar{z}_i - d_{ij} - z_j) - t_{ij}(\bar{z}_i - d_{ij} - z_j')| d\bar{z}_i \leq H_{ij} |z_j - z_j'|, \quad (8)$$

for all $z_j, z_j' \in \Pi_j(\mathcal{Z})$, which utilizes a decomposition of t_{ij} into a continuous part and a piecewise constant function. The complete proof is presented in Appendix A. We display the results with a numerical example.

Example 4: Consider the density function of the exponential distribution with rate 1, i.e. $t(z) = e^{-z}$ if $z \geq 0$ and 0 otherwise (cf. Fig. 4 in the left). Notice that the density function is piecewise Lipschitz-continuous (cf. Assumption 3). Furthermore the density function presents one discontinuity point $c^1 = 0$ with associated jump distance equal to $J^1 = 1$. One can show that the density function can be decomposed into a piecewise constant function $g^d(z) = \theta(z)$ and a continuous function $g^c(z) = 0\mathbb{1}_{z<0} + (e^{-z} - 1)\mathbb{1}_{z \geq 0}$, as depicted in Fig. 4 (middle and right plots). □

In some cases, it is possible to obtain a smaller value for H_{ij} by substituting the density function directly into the inequality in (8). Furthermore H_{ij} may be independent of the size of the state space. For instance, if the delay is modeled by an exponential distribution as in Example 1, then $A_{ij}(\cdot)$ for all $i, j \in \mathbb{N}_n$ follows a shifted exponential distribution, i.e. $A_{ij}(\cdot) \sim SExp(\lambda_{ij}, \varsigma_{ij})$. In this case, $H_{ij} = \lambda_{ij} + \lambda_{ij}^2 \mathcal{L}_i$, as per Theorem 3. However if we compute directly the left-hand side of (8), we get the quantity $H_{ij} = 2\lambda_{ij}$, which is independent of the shape of the state space. This fact is proven in general in Theorem 4, for the class of distribution functions introduced next.

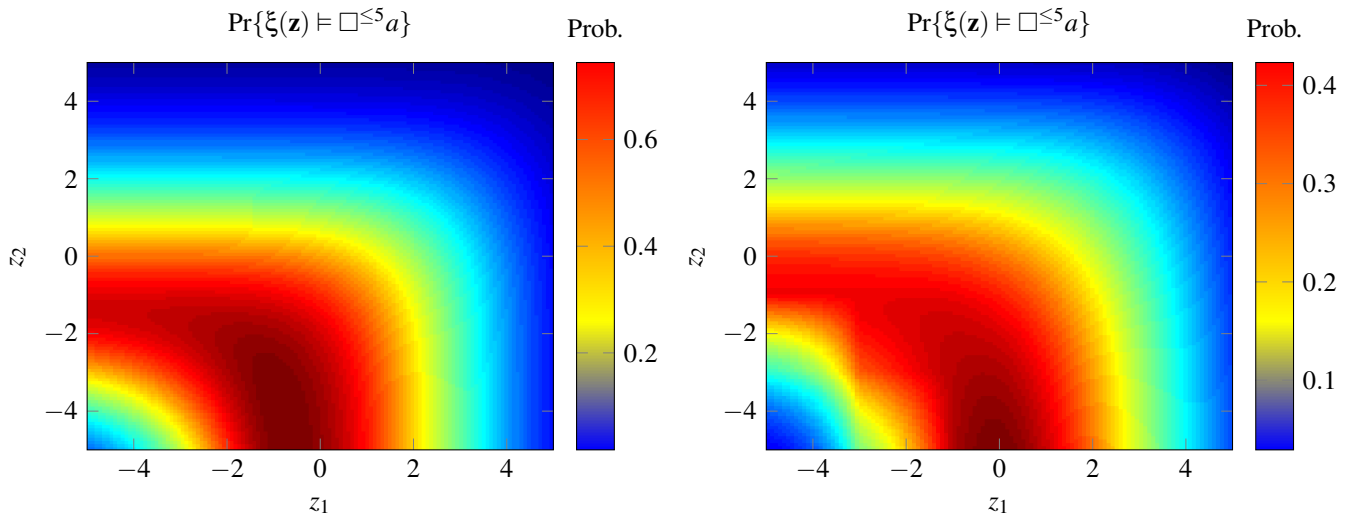

Fig. 3. The left and right plots show solution of the finite-horizon probabilistic invariance problem for two-dimensional SMPL systems with beta (Example 3) and exponential (Example 5) distributions, respectively. The plots have been obtained by computing the problem over finite abstractions obtained by uniform discretization of the set of interest and selection of central representative points. Notice that the abstraction function $\xi : \mathcal{Z} \to \mathcal{P}$ associates to any point $\mathbf{z} \in \mathcal{Z}$ on the SMPL state space, the corresponding discrete state $\xi(\mathbf{z}) \in \mathcal{P}$ (cf. Section III).

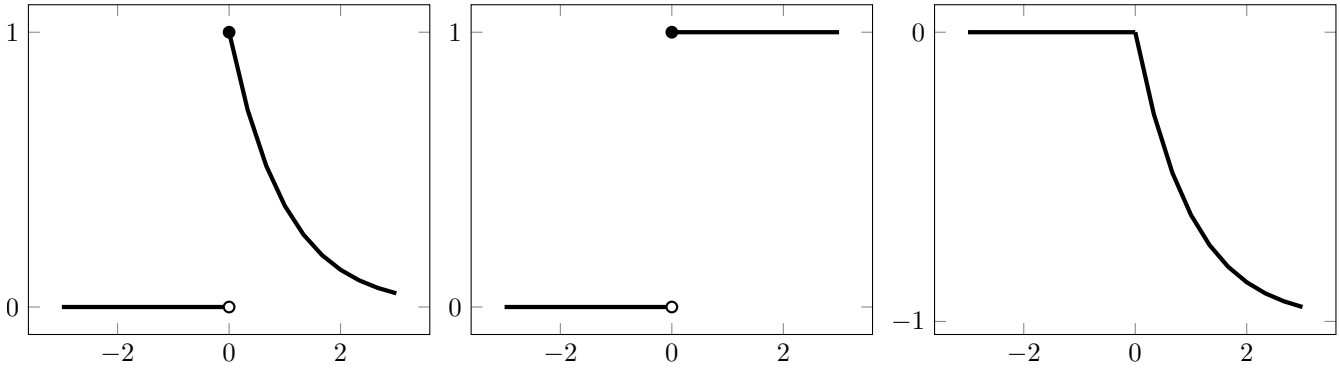

Fig. 4. The density function of the exponential distribution with rate 1 (left plot) is the sum of two functions: the unit step function $\theta(\cdot)$ on the middle plot and a continuous part on the right plot.

Definition 2 (Shifted Exponential Distribution): The density function of an exponential distribution shifted by ς is

$$t(x; \lambda, \varsigma) = \lambda \exp\{-\lambda(x - \varsigma)\}\theta(x - \varsigma),$$

where $\theta(\cdot)$ represents the unit step function. A random variable X characterized by this distribution is denoted by $X \sim SExp(\lambda, \varsigma)$. □

Theorem 4: Any random sequence $A_{ij}(\cdot) \sim SExp(\lambda_{ij}, \varsigma_{ij})$ satisfies inequality (8) with $H_{ij} = 2\lambda_{ij}$. □

Given the previous result, the bound related to the abstraction error over SMPL systems with $A_{ij}(\cdot) \sim SExp(\lambda_{ij}, \varsigma_{ij})$ can be improved and explicitly shown as follows. The maximum value of the density function $t_{ij}(\cdot)$ equals λ_{ij}, i.e. $M_{ij} = \lambda_{ij}$ for all $i, j \in \mathbb{N}_n$ (cf. Assumption 1). By Theorem 3 and Proposition 1, the bound of the abstraction error is then

$$E = N\delta(n + 1) \sum_{i,j=1}^{n} \lambda_{ij}.$$

Let us go back to Example 3 and adapt according to Definition 2 and Theorem 4.

Example 5: Consider the two-dimensional SMPL system (1), where $A_{ij}(\cdot) \sim SExp(\lambda_{ij}, \varsigma_{ij})$ and

$$\begin{bmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{bmatrix} = \begin{bmatrix} 1/2 & 1/3 \\ 1 & 1/3 \end{bmatrix}, \quad \begin{bmatrix} \varsigma_{11} & \varsigma_{12} \\ \varsigma_{21} & \varsigma_{22} \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix}.$$

Considering a periodic timetable with $\mathbf{s}(0) = [0, 0]^T$ and $d = 4$, selecting invariant set $\mathcal{A} = [-5, 5]^2$, and event horizon $N = 5$, we get $E = 32.5\delta$. In order to obtain a desired error $E = 0.1$, we need to use 4597 bins per dimension on a uniform discretization of the set $\mathcal{A}$. The solution of the invariance problem over the abstract model is presented in Fig. 3 (right panel).

Let us now empirically validate the obtained outcomes, to emphasize that we obtain safe guarantees on the performance of the approximation algorithm. We have computed 1000 sample trajectories, with an initial condition that has been uniformly generated from the level set corresponding to a satisfaction probability equal to 0.3, namely within the set $\{\mathbf{z} \mid \Pr\{\xi(\mathbf{z}) \vDash \Box^{\leq 5} a\} \geq 0.3\}$. Practically, this means we have sampled the initial condition on points corresponding to colors warmer than the "orange level" in Fig. 3 (right). Given

the error bound $E = 0.1$, we would expect that the trajectories are invariant with a likelihood greater than 0.2. Among the cohort, we have found that 348 trajectories stay inside the invariant set for the given 5 steps, which is aligned with the guarantee we have derived.

Furthermore we have compared the approximate solution against the following empirical approach: for each representative point, we generate 1000 sample trajectories starting from it and compute ratio of the number of trajectories that stay in the invariant set for 5 steps to the total number of trajectories (1000). The maximum absolute difference between the approximate solution and the empirical approach for all representative points is 0.0673, which aligns with the error bound of 0.1.

Finally, extending these two empirical studies to the SMPL system in Example 3 leads to results that are quite analogous to the ones just discussed. □

D. Dimension-Dependent Error Formulation

With the goal of improving the computational efficiency of the approach, in this section we formulate a bound on the abstraction error as a summation of dimension-dependent terms. This allows for a "parallelization" of the computation of the quantities leading to the error term. Consider the partition $\mathcal{Z} = \cup_{j=1}^{m} \mathcal{Z}_j$. For each $r \in \mathbb{N}_n$, we define diameter of the partition along the r-th dimension as

$$\delta_r = \max\{|z_r - z'_r| \text{ s.t. } z_r, z'_r \in \Pi_r(\mathcal{Z}_j) \text{ and } j \in \mathbb{N}_m\}.$$

Theorem 5: The bound on abstraction error can be written as $E = N \sum_{r=1}^{n} H(r)\delta_r$, where

$$H(r) = \sum_{i,j=1}^{n} M_{ij} + \sum_{i=1}^{n} (H_{ir} - M_{ir}), \tag{9}$$

the constants H_{ir} are defined according to (8), M_{ij} represents the maximum value of density function $t_{ij}(\cdot)$, and N is the horizon of the BLTL specification. □

Theorem 5 suggests that we can refine the partition along single dimensions, namely that for each $r \in \mathbb{N}_n$ the value of δ_r is determined based on N, $H(r)$ and E. In order to obtain a partition of $\mathcal{Z}$ with minimum cardinality, we distribute the abstraction error equally along all dimensions, i.e. $NH(r)\delta_r = E/n$ for each $r \in \mathbb{N}_n$.

Remark 2: The quantity $H(r)$ can be further reduced to the following

$$H(r) = \sum_{i,j=1}^{n} \min\{M_{ir}, M_{ij}\} + \sum_{i=1}^{n} (H_{ir} - M_{ir}). \qquad \square$$

Example 6: Consider the matrix M containing all the maximum values of the density functions

$$M = [M_{ij}]_{i,j} = \begin{bmatrix} 1 & 3 & 2 \\ 5 & 6 & 8 \\ 7 & 4 & 3 \end{bmatrix}.$$

Let us compare the first term of $H(r)$ according to Theorem 5 and Remark 2. In Theorem 5, the constant contribution of these maximum values is $\|M\|_1 = \sum_{i,j} |M_{ij}| = 39$ whereas in Remark 2 it is reduced to $32, 34, 33$, for r equals $1, 2, 3$, respectively. The reduction will be more relevant as the difference of the maximal values $M_{(\cdot)}$ are larger. □

V. Explicit Verification via Symbolic Computations

In this section, we discuss an alternative approach to solve the finite-horizon probabilistic invariance problem. The alternative approach assumes that the density functions are or may be approximated as piecewise polynomial density functions, which allows for explicit integrations reducing to updates of the coefficients of the polynomial parts. This approach is also formal in the sense that we are able to determine the error of the procedure, which is due to the approximation of the density functions.

Consider that the density functions $t_{ij}(\cdot)$ are approximated by piecewise polynomial density functions $\tilde{t}_{ij}(\cdot)$ for all $i, j \in \mathbb{N}_n$. The approximation error of $\tilde{t}_{ij}(\cdot)$ is denoted by ϵ_{ij}, which is defined as

$$\int_{\mathbb{R}} |t_{ij}(x) - \tilde{t}_{ij}(x)| dx \leq \epsilon_{ij} \quad \text{for all } i, j \in \mathbb{N}_n.$$

We define an SMPL system derived from (3) where the density functions are the piecewise polynomial approximation, as follows:

$$\mathbf{z}(k+1) = \left[\tilde{A}(k) + D\right] \otimes \mathbf{z}(k). \tag{10}$$

Each entry of $\tilde{A}(k)$ is independent and identically distributed w.r.t. $k \in \mathbb{N}$; and $\tilde{A}_{ij}(\cdot)$ are independent for all $i, j \in \mathbb{N}_n$. The random sequence $\{\tilde{A}_{ij}(\cdot)\}$ is then characterized by the density function $\tilde{t}_{ij}(\cdot)$ and corresponding distribution function $\tilde{T}_{ij}(\cdot)$ for $i, j \in \mathbb{N}_n$. The conditional density function is denoted by $\tilde{t}_z(\bar{\mathbf{z}}|\mathbf{z})$. The expression of $\tilde{t}_z(\bar{\mathbf{z}}|\mathbf{z})$ is similar with that of Theorem 1.

The finite-horizon probabilistic invariance problem over the introduced SMPL system (10) can be formulated as follows:

$$\tilde{P}_{\mathbf{z}_0}(\mathcal{A}) = \Pr\{\mathbf{z}(k) \in \mathcal{A} \text{ for all } k \in \mathbb{N}_N \cup \{0\} | \mathbf{z}(0) = \mathbf{z}_0\}.$$

As for Proposition 2, the quantity of interest can be characterized by backward recursions over functions $\tilde{V}_k : \mathbb{R}^n \to [0, 1], k \in \mathbb{N}_N \cup \{0\}$, as follows. Initially we define $\tilde{V}_N(\mathbf{z}) = \mathbb{1}_{\mathcal{A}}(\mathbf{z})$, for all $\mathbf{z} \in \mathcal{Z}$. Then we compute $\tilde{V}_k$ for $k \in \mathbb{N}_{N-1} \cup \{0\}$ using the formula in Proposition 2. This leads to $\tilde{P}_{\mathbf{z}_0}(\mathcal{A}) = \tilde{V}_0(\mathbf{z}_0)$. Since $\tilde{t}_z(\bar{\mathbf{z}}|\mathbf{z})$ is a piecewise polynomial function, $\tilde{V}_k$ can be computed via simple integrations using a computer algebra program. In other words here $\tilde{V}_k$ are thus obtained "symbolically", rather than numerically as before. It is of interest to provide a quantitative comparison between the outcome obtained in this way, and the solution resulting from Proposition 2: in other words, we are interested in deriving bounds on the relative error. Next, we define the error related to the alternative approach, which is due to the approximation of density functions with piecewise polynomial density functions. Then a bound of the error is formulated w.r.t. the finite-horizon probabilistic invariance problem.

Since an exact computation of this error is not possible in general, we resort to determining an upper bound of the error,

which is denoted by $\tilde{E}$. More formally, we are interested in quantifying $\tilde{E}$ satisfying

$$|P_{\mathbf{z}_0}(\mathcal{A}) - \tilde{P}_{\mathbf{z}_0}(\mathcal{A})| \leq \tilde{E} \quad \text{for all } \mathbf{z}_0 \in \mathcal{A}. \tag{11}$$

Theorem 6: Suppose for each $i, j \in \mathbb{N}_n$ the density function $t_{ij}(\cdot)$ is replaced by $\tilde{t}_{ij}(\cdot)$ such that

$$\int_{\mathbb{R}} |t_{ij}(z) - \tilde{t}_{ij}(z)| dz \leq \epsilon_{ij}.$$

Then an upper bound on the error in (11) is $\tilde{E} = Nn\mathcal{K}$, where N is the event horizon, n is the dimension of the system and $\mathcal{K} = \sum_{i,j=1}^{n} \epsilon_{ij}$. □

Let us now focus on computational experiments.

Example 7: We have implemented this alternative symbolic approach, and the related approximation procedure, on a shifted exponential distribution in Mathematica. The procedure is presented in Appendix B. We have further tested the implementation of the alternative approach on Example 5, and run experiments on a 12-core Intel Xeon 3.47 GHz PC with 24 GB of memory. In this case, we choose $\tilde{E} = 0.1$, $N = 5$ and $n = 2$. From Theorem 6, we obtain $\mathcal{K} = 0.01$. We define ϵ_{ij} to be the same for $i, j \in \mathbb{N}_2$. This implies $\epsilon_{ij} = \mathcal{K}/4 = 0.0025$ for $i, j \in \mathbb{N}_2$. In the approximation procedure (cf. Algorithm 5), we choose $p = 1$. The outcome for the new, symbolic approach has clearly exhibited increased computational challenges, running short of memory already during the computation of $\tilde{V}_3$: a-posteriori, the reason has been found to reside on the number of regions in $\tilde{V}_k$, which grows exponentially as k decreases (cf. Proposition 2). □

Example 8: We have tested the implementation of the alternative approach on Example 3, where the density function is already a piecewise polynomial function. The outcomes are quite similar with the previous experiment: running short of memory during the first computations of $\tilde{V}$. □

In conclusion, while enticing because of its explicit nature and for the derived related formal error bounds, the alternative symbolic approach holds promise but requires further research towards practical scalability. As of now it does not appear to be as practically deployable as the core technique discussed earlier in this manuscript.

VI. Conclusions and Future Work

This work has developed new model checking procedures for Stochastic Max-Plus-Linear (SMPL) systems against BLTL specifications, based on finite abstractions. We have assumed that each random variable characterizing the SMPL system has a fixed support, which implies that the topology of the SMPL system is fixed over time: we are interested to relax this assumption in order to obtain results that are robust against topological changes. Computationally, we are interested in improving the abstraction by integrating it with the software tool FAUST^2 [46].

Appendix

A. Proof of Statements

Proof of Theorem 1: The independence property of $A_{ij}(\cdot) \otimes d_{ij}$, for all $i, j \in \mathbb{N}_n$, leads to the multiplicative expression of $t_z(\bar{\mathbf{z}}|\mathbf{z})$. In order to show the expression of the components $t_i(\bar{z}_i|\mathbf{z})$, first we compute the i-th conditional distribution function $T_i(\bar{z}_i|\mathbf{z})$, then we compute the i-th conditional density function $t_i(\bar{z}_i|\mathbf{z})$ by taking the derivative of $T_i(\bar{z}_i|\mathbf{z})$ w.r.t. $\bar{z}_i$:

$$\begin{aligned}
&T_i(\bar{z}_i|\mathbf{z}) \\
&= \Pr\{\max\{A_{i1} + d_{i1} + z_1, \ldots, A_{in} + d_{in} + z_n\} \leq \bar{z}_i|\mathbf{z}\} \\
&= \Pr\{A_{i1} + d_{i1} + z_1 \leq \bar{z}_i, \ldots, A_{in} + d_{in} + z_n \leq \bar{z}_i|\mathbf{z}\} \\
&= \prod_{j=1}^{n} \Pr\{A_{ij} \leq \bar{z}_i - d_{ij} - z_j|\mathbf{z}\} = \prod_{j=1}^{n} T_{ij}(\bar{z}_i - d_{ij} - z_j|\mathbf{z}).
\end{aligned}$$

By simple manipulation, the derivative of $T_i(\bar{z}_i|\mathbf{z})$ w.r.t. $\bar{z}_i$ coincides with the expression of $t_i(\bar{z}_i|\mathbf{z})$. □

Proof of Lemma 1: We prove the inequality for the case $z' > z$. For the other case, the proof is similar. Consider any arbitrary $a, b \in \mathbb{R}$. Since the distribution function is non-decreasing we can write

$$\begin{aligned}
&\int_a^b |T(\bar{z} - z) - T(\bar{z} - z')| d\bar{z} \\
&= \int_a^b T(\bar{z} - z) d\bar{z} - \int_a^b T(\bar{z} - z') d\bar{z} = g(z) - g(z'),
\end{aligned}$$

where $g(z) = \int_a^b T(\bar{z} - z) d\bar{z} = \int_{a-z}^{b-z} T(u) du$. By the fundamental theorem of calculus, we obtain

$$|g'(z)| = |T(a - z) - T(b - z)| \leq 1.$$

Finally based on the mean value theorem, we can write $|g(z) - g(z')| \leq |z - z'|$. Since the inequality holds for any interval $[a, b]$, we conclude that it also holds over $\mathbb{R}$. □

Proof of Lemma 2: In the following derivation, we use the triangle inequality and the following property of density functions: they are positive functions and their integral is bounded by one. We obtain

$$\begin{aligned}
&\int_{\mathcal{Z}} |f(\bar{\mathbf{z}}|\mathbf{z}) - f(\bar{\mathbf{z}}|\mathbf{z}')| d\bar{\mathbf{z}} \\
&= \int_{\mathcal{Z}} |f_1(\bar{\mathbf{z}}_1|\mathbf{z}) f_2(\bar{\mathbf{z}}_2|\mathbf{z}) - f_1(\bar{\mathbf{z}}_1|\mathbf{z}') f_2(\bar{\mathbf{z}}_2|\mathbf{z}')| d\bar{\mathbf{z}} \\
&\leq \int_{\mathcal{Z}} |f_1(\bar{\mathbf{z}}_1|\mathbf{z}) - f_1(\bar{\mathbf{z}}_1|\mathbf{z}')| f_2(\bar{\mathbf{z}}_2|\mathbf{z}) d\bar{\mathbf{z}} \\
&\quad + \int_{\mathcal{Z}} |f_2(\bar{\mathbf{z}}_2|\mathbf{z}) - f_2(\bar{\mathbf{z}}_2|\mathbf{z}')| f_1(\bar{\mathbf{z}}_1|\mathbf{z}') d\bar{\mathbf{z}} \\
&\leq \int_{\Pi_1(\mathcal{Z})} |f_1(\bar{\mathbf{z}}_1|\mathbf{z}) - f_1(\bar{\mathbf{z}}_1|\mathbf{z}')| d\bar{\mathbf{z}}_1 \int_{\Pi_2(\mathcal{Z})} f_2(\bar{\mathbf{z}}_2|\mathbf{z}) d\bar{\mathbf{z}}_2 \\
&\quad + \int_{\Pi_2(\mathcal{Z})} |f_2(\bar{\mathbf{z}}_2|\mathbf{z}) - f_2(\bar{\mathbf{z}}_2|\mathbf{z}')| d\bar{\mathbf{z}}_2 \int_{\Pi_1(\mathcal{Z})} f_1(\bar{\mathbf{z}}_1|\mathbf{z}') d\bar{\mathbf{z}}_1 \\
&\leq \int_{\Pi_1(\mathcal{Z})} |f_1(\bar{\mathbf{z}}_1|\mathbf{z}) - f_1(\bar{\mathbf{z}}_1|\mathbf{z}')| d\bar{\mathbf{z}}_1 \\
&\quad + \int_{\Pi_2(\mathcal{Z})} |f_2(\bar{\mathbf{z}}_2|\mathbf{z}) - f_2(\bar{\mathbf{z}}_2|\mathbf{z}')| d\bar{\mathbf{z}}_2
\end{aligned}$$

□

Proof of Lemma 3: By using the triangle inequality, we

obtain the following chain of inequalities

$$\begin{aligned}
&\int_{\mathcal{C}} |f(\bar{z}|\mathbf{z}_1,\mathbf{z}_2) - f(\bar{z}|\mathbf{z}_1',\mathbf{z}_2')|d\bar{z} \\
&= \int_{\mathcal{C}} |f_1(\bar{z},\mathbf{z}_1)f_2(\bar{z},\mathbf{z}_2) - f_1(\bar{z},\mathbf{z}_1')f_2(\bar{z},\mathbf{z}_2')|d\bar{z} \\
&\le \int_{\mathcal{C}} |f_1(\bar{z},\mathbf{z}_1) - f_1(\bar{z},\mathbf{z}_1')|f_2(\bar{z},\mathbf{z}_2)d\bar{z} \\
&\quad + \int_{\mathcal{C}} |f_2(\bar{z},\mathbf{z}_2) - f_2(\bar{z},\mathbf{z}_2')|f_1(\bar{z},\mathbf{z}_1')d\bar{z} \\
&\le M_2 \int_{\mathcal{C}} |f_1(\bar{z},\mathbf{z}_1) - f_1(\bar{z},\mathbf{z}_1')|d\bar{z} \\
&\quad + M_1 \int_{\mathcal{C}} |f_2(\bar{z},\mathbf{z}_2) - f_2(\bar{z},\mathbf{z}_2')|d\bar{z}. \qquad \square
\end{aligned}$$

Proof of Theorem 2: Using Lemma 2 on the multiplicative structure of the conditional density function we have:

$$\int_{\mathcal{Z}} |t_z(\bar{\mathbf{z}}|\mathbf{z}) - t_z(\bar{\mathbf{z}}|\mathbf{z}')|d\bar{\mathbf{z}} \le \sum_{i=1}^{n} \int_{\Pi_i(\mathcal{Z})} |t_i(\bar{z}_i|\mathbf{z}) - t_i(\bar{z}_i|\mathbf{z}')|d\bar{z}_i,$$

and employing the triangle inequality for the additive structure of $t_i(\bar{z}_i|\mathbf{z})$ and utilizing Lemma 3 and Assumption 1, we obtain:

$$\begin{aligned}
&\le \sum_{i,j=1}^{n} \int_{\Pi_i(\mathcal{Z})} |t_{ij}(\bar{z}_i - d_{ij} - z_j) - t_{ij}(\bar{z}_i - d_{ij} - z_j')|d\bar{z}_i \\
&\quad + \sum_{i,j=1}^{n} \sum_{\substack{k=1 \\ k\neq j}}^{n} M_{ij} \int_{\Pi_i(\mathcal{Z})} |T_{ik}(\bar{z}_i - d_{ik} - z_k) \\
&\qquad\qquad -T_{ik}(\bar{z}_i - d_{ik} - z_k')|d\bar{z}_i. \qquad (12)
\end{aligned}$$

Finally, by Assumption 2 and Lemma 1 we obtain

$$\begin{aligned}
&\le \sum_{i,j=1}^{n} h_{ij}\mathcal{L}(\Pi_i(\mathcal{Z}))|z_j - z_j'| + \sum_{i,j=1}^{n} \sum_{\substack{k=1 \\ k\neq j}}^{n} M_{ij}|z_k - z_k'| \\
&\le \left(\sum_{i,j=1}^{n} H_{ij} + (n-1)M_{ij} \right) \|\mathbf{z} - \mathbf{z}'\| = H\|\mathbf{z} - \mathbf{z}'\|. \quad \square
\end{aligned}$$

Proof of Theorem 3: We show that the constant H_{ij} in (8) exists for piecewise Lipschitz-continuous density functions and compute it based on Assumption 3. Introduce the two functions $g_{ij}^d(z) = \sum_{k=1}^{m_{ij}-1} \mathcal{J}_{ij}^k \theta(z - c_{ij}^k)$ and $g_{ij}^c(z) = t_{ij}(z) - g_{ij}^d(z)$, where $\mathcal{J}_{ij}^k = \sum_{q=1}^{k} J_{ij}^q$, $\theta(\cdot)$ denotes the unit step function, and $\{c_{ij}^k \mid k \in \mathbb{N}_{m_{ij}-1}\}$ are the discontinuity points of the density function $t_{ij}(\cdot)$. Then the density function is decomposed into $t_{ij}(z) = g_{ij}^c(z) + g_{ij}^d(z)$, where g_{ij}^c is its continuous part and g_{ij}^d is a piecewise constant function encompassing its jumps (cf. Fig. 4). It is clear that

$$\begin{aligned}
&\int_{\Pi_i(\mathcal{Z})} |g_{ij}^d(\bar{z} - d_{ij} - z) - g_{ij}^d(\bar{z} - d_{ij} - z')|d\bar{z} \\
&\qquad\qquad \le \sum_{k=1}^{m-1} |\mathcal{J}_{ij}^k||z - z'|, \\
&\int_{\Pi_i(\mathcal{Z})} |g_{ij}^c(\bar{z} - d_{ij} - z) - g_{ij}^c(\bar{z} - d_{ij} - z')|d\bar{z} \\
&\qquad\qquad \le \mathcal{L}_i \max_k h_{ij}^k |z - z'|.
\end{aligned}$$

Adding both sides using the triangle inequality leads to the desired value for H_{ij}. $\square$

Proof of Theorem 4: We will show that the following inequality holds:

$$\begin{aligned}
&\int_{\Pi_i(\mathcal{A})} |t_{ij}(\bar{z}_i - d_{ij} - z_j; \lambda_{ij}, \varsigma_{ij}) - t_{ij}(\bar{z}_i - d_{ij} - z_j'; \lambda_{ij}, \varsigma_{ij})|d\bar{z}_i \\
&\quad \le 2\lambda_{ij}|z_j - z_j'|, \text{ for all } z_j, z_j' \in \Pi_j(\mathcal{Z}).
\end{aligned}$$

Without loss of generality, since the integrand and the expression on the right-hand side are symmetric w.r.t. z_j and z_j', let us assume that $z_j \le z_j'$. It follows that the integrand is a piecewise continuous function of $\bar{z}_i, z_j, z_j'$:

$$\begin{cases}
\lambda_{ij} \exp\{-\lambda_{ij}(\bar{z}_i - d_{ij} - z_j' - \varsigma_{ij})\} \\
\quad -\lambda_{ij} \exp\{-\lambda_{ij}(\bar{z}_i - d_{ij} - z_j - \varsigma_{ij})\}, \\
\qquad\qquad\qquad\qquad \text{if } \bar{z}_i \ge z_j' + d_{ij} + \varsigma_{ij}, \\
\lambda_{ij} \exp\{-\lambda_{ij}(\bar{z}_i - d_{ij} - z_j - \varsigma_{ij})\}, \\
\qquad\qquad\qquad \text{if } z_j + d_{ij} + \varsigma_{ij} \le \bar{z}_i \le z_j' + d_{ij} + \varsigma_{ij}, \\
0, \qquad\qquad\qquad\qquad \text{if } \bar{z}_i \le z_j + d_{ij} + \varsigma_{ij}.
\end{cases}$$

Thus the overall bounds can be computed based on the bounds of the first two sub-functions. We will prove that the first two sub-functions are bounded by $\lambda_{ij}|z_j - z_j'|$. Let us focus on the first sub-function:

$$\begin{aligned}
&\lambda_{ij} \int_{z_j' + d_{ij} + \varsigma_{ij}}^{+\infty} \big(\exp\{-\lambda_{ij}(\bar{z}_i - d_{ij} - z_j' - \varsigma_{ij})\} \\
&\quad - \exp\{-\lambda_{ij}(\bar{z}_i - d_{ij} - z_j - \varsigma_{ij})\}\big)\, d\bar{z}_i \\
&= \lambda_{ij}(\exp\{\lambda_{ij} z_j'\} - \exp\{\lambda_{ij} z_j\}) \\
&\quad \int_{z_j' + d_{ij} + \varsigma_{ij}}^{+\infty} \exp\{-\lambda_{ij}(\bar{z}_i - d_{ij} - \varsigma_{ij})\} d\bar{z}_i \\
&= (\exp\{\lambda_{ij} z_j'\} - \exp\{\lambda_{ij} z_j\})\ \exp\{-\lambda_{ij} z_j'\} \\
&= 1 - \exp\{-\lambda_{ij}(z_j' - z_j)\} \\
&\le \lambda_{ij}|z_j - z_j'|.
\end{aligned}$$

The last inequality holds because $\lambda_{ij}(z_j' - z_j) \ge 0$ and $1 - \exp\{-z\} \le z$ for all $z \ge 0$. Then we continue to the second sub-function:

$$\begin{aligned}
&\lambda_{ij} \int_{z_j + d_{ij} + \varsigma_{ij}}^{z_j' + d_{ij} + \varsigma_{ij}} \exp\{-\lambda_{ij}(\bar{z}_i - d_{ij} - z_j - \varsigma_{ij})\} d\bar{z}_i \\
&= -\exp\{-\lambda_{ij}(z_j' - z_j)\} + 1 \\
&\le \lambda_{ij}|z_j - z_j'|. \qquad \square
\end{aligned}$$

Proof of Theorem 5: The proof follows the same line of proofs of Theorems 2 and 3. We utilize the inequality (8) and Lemma 1 in the right-hand side of (12) to get

$$\int_{\mathcal{Z}} |t_z(\bar{\mathbf{z}}|\mathbf{z}) - t_z(\bar{\mathbf{z}}|\mathbf{z}')|d\bar{\mathbf{z}} \le \sum_{i,j=1}^{n} H_{ij}\delta_j + \sum_{i,j=1}^{n} \sum_{\substack{k=1 \\ k\neq j}}^{n} M_{ij}\delta_k,$$

which is equal to $\sum_{r=1}^{n} H(r)\delta_r$ with $H(r)$ defined in (9). Finally, Proposition 1 guarantees the abstraction error of $E = N\sum_{r=1}^{n} H(r)\delta_r$. $\square$

Proof of Theorem 6: We consider $T_{ij}(\cdot)$ and $\tilde{T}_{ij}(\cdot)$ the associated distribution functions:

$$|T_{ij}(z)-\tilde{T}_{ij}(z)| = \left|\int_{-\infty}^{z} t_{ij}(u)du - \int_{-\infty}^{z}\tilde{t}_{ij}(u)du\right| \leq \int_{-\infty}^{z}|t_{ij}(u)-\tilde{t}_{ij}(u)|du \leq \epsilon_{ij}.$$

Using this inequality we obtain

$$\begin{aligned}
&\int_{\mathcal{Z}}|t_z(\bar{\mathbf{z}}|\mathbf{z})-\tilde{t}_z(\bar{\mathbf{z}}|\mathbf{z})|d\bar{\mathbf{z}} \leq \sum_{i=1}^{n}\int_{\Pi_i(\mathcal{Z})}|t_i(\bar{z}_i|\mathbf{z})-\tilde{t}_i(\bar{z}_i|\mathbf{z})|d\bar{z}_i\\
&\leq \sum_{i,j=1}^{n}\int_{\Pi_i(\mathcal{Z})}|t_{ij}(\bar{z}_i+d-z_j)-\tilde{t}_{ij}(\bar{z}_i+d-z_j)|d\bar{z}_i\\
&\quad+\sum_{i,j=1}^{n}\sum_{\substack{k=1\\k\neq j}}^{n}\sup_{\bar{z}_i,z_k}|T_{ik}(\bar{z}_i+d-z_k)-\tilde{T}_{ik}(\bar{z}_i+d-z_k)|\\
&\leq \sum_{i,j=1}^{n}\epsilon_{ij}+\sum_{i,j=1}^{n}\sum_{\substack{k=1\\k\neq j}}^{n}\epsilon_{ik} = n\sum_{i,j=1}^{n}\epsilon_{ij}.
\end{aligned}$$

The upper bound on the error $\tilde{E}$ is obtained by applying the result in [33, Lemma 1] to the preceding inequality. □

B. Approximation of Exponential Functions by Piecewise Polynomial Functions

We now develop a procedure to compute an approximation of exponential functions with arbitrary accuracy. The approximation is characterized by a piecewise polynomial function.

Here we consider the negative exponential function $f : [0,+\infty) \to [0,1]$, $x \mapsto e^{-x}$ and provide a piecewise polynomial approximation $\tilde{f} : [0,+\infty) \to \mathbb{R}$ such that

$$\int_0^{+\infty}|f(x)-\tilde{f}(x)|dx \leq \epsilon,$$

for any given threshold $\epsilon > 0$. Having this piecewise polynomial approximation of the negative exponential function and using shifted scaled variables, we can approximate any shifted exponential distribution by a piecewise polynomial one for a given threshold.

For this purpose we select the shifted Legendre polynomials as the basis function with the following explicit representation

$$P_n(x) = (-1)^n\sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{k}(-x)^k,$$

which are orthogonal in the interval $[0,1]$, i.e.

$$\int_0^1 P_m(x)P_n(x)dx = \frac{1}{2n+1}\delta_{mn},$$

where δ_{mn} is the Kronecker delta, which equals 1 if $m=n$ and 0 otherwise. Note that since we do not have any weighting function inside the integral, we need to select the basis functions to be orthogonal with weight 1. To the best of our knowledge, Legendre polynomials are the only available option.

Define the new basis functions $\psi_{ij}(x)$ and construct $\tilde{f}(x)$ according to

$$\psi_{ij}(x) = P_j\left(\frac{x-i\ell}{\ell}\right)\mathbb{1}_{[i\ell,(i+1)\ell)}(x),$$
$$\tilde{f}(x) = \sum_{i=0}^{p-1}\sum_{j=0}^{q_i}c_{ij}\psi_{ij}(x),$$

where $\mathbb{1}_{[i\ell,(i+1)\ell)}(\cdot)$ is the indicator function of the interval $[i\ell,(i+1)\ell)$, the number of intervals for the function $\tilde{f}(\cdot)$ is denoted by p, the maximum degree of basis polynomials in the i-th interval is denoted by q_i, and the length of intervals $\ell > 0$ will be specified later. Note that these basis functions are still orthogonal over $\mathbb{R}$ and the coefficients can be computed as

$$c_{ij} = e^{-i\ell}\underbrace{(2j+1)\int_0^1 e^{-\ell u}P_j(u)du}_{\alpha_j}.$$

In the above equation, observe that α_j does not depend on i. This observation makes it possible to take $q_0 = q_1 = \ldots = q_{p-1} = q$ and simplify the function $\tilde{f}(\cdot)$ by the following

$$\tilde{f}_q(x) = \sum_{j=0}^{q}\alpha_j P_j(x),$$
$$\tilde{f}(x) = \sum_{i=0}^{p-1}e^{-i\ell}\tilde{f}_q\left(\frac{x-i\ell}{\ell}\right)\mathbb{1}_{[i\ell,(i+1)\ell)}(x).$$

Remark 3: The coefficients have a closed form

$$\begin{aligned}
\alpha_j = (2j+1)&\sum_{k=0}^{j}(-1)^{j+k}\binom{j}{k}\binom{j+k}{k}\frac{k!}{\ell^{k+1}}\\
&-(2j+1)e^{-\ell}\sum_{k=0}^{j}\sum_{r=0}^{k}(-1)^{j+k}\binom{j}{k}\binom{j+k}{k}\\
&\frac{k!}{(k-r)!}\frac{1}{\ell^{r+1}}.
\end{aligned}$$

□

Algorithm 5 presents the required steps to construct the approximation function. The advantage of this algorithm is that we compute the polynomial only for one interval and use it to generate the polynomials for all intervals. This property is due to the characteristics of the exponential function and in general does not hold for other functions.

Theorem 7: If $q \in \mathbb{N}$ is selected sufficiently large such that

$$\int_0^1|e^{-\ell x}-\tilde{f}_q(x)|dx \leq \epsilon_1, \tag{13}$$

then $\tilde{f}(x)$ approximates the exponential function $f(x) = e^{-x}$ which satisfies the inequality $\int_0^{+\infty}|f(x)-\tilde{f}(x)|dx \leq \epsilon$. □

Remark 4: The completeness of Legendre polynomials as basis functions implies that

$$\sum_{j=0}^{+\infty}\frac{\alpha_j^2}{2j+1} = \int_0^1 e^{-2\ell u}du = \frac{1-e^{-2\ell}}{2\ell}.$$

Moreover it guarantees that

$$\lim_{q\to\infty}\int_0^1|e^{-\ell x}-\tilde{f}_q(x)|dx = 0.$$

input: The approximation precision $0 < \epsilon < 1$ and the number of intervals $p \in \mathbb{N}$

output: $\tilde{f}(x) = \sum_{i=0}^{p-1} e^{-i\ell} \tilde{f}_q\left(\frac{x-i\ell}{\ell}\right) \mathbb{1}_{[i\ell,(i+1)\ell)}(x)$

1: Select the length of intervals $\ell = -\frac{1}{p}\ln\left(\frac{\epsilon}{2}\right) > 0$

2: Compute $\epsilon_1 = \dfrac{\epsilon}{2\ell}\dfrac{1-e^{-\ell}}{1-e^{-p\ell}}$

3: Define $\tilde{f}_q : [0,1] \to \mathbb{R}$ as the polynomial approximation of the function $e^{-\ell x}$ in the interval $[0,1]$:

$$\tilde{f}_q(x) = \sum_{j=0}^{q} \alpha_j P_j(x), \quad \alpha_j = (2j+1)\int_0^1 e^{-\ell u} P_j(u) du.$$

4: Select q sufficiently large such that

$$\int_0^1 |e^{-\ell x} - \tilde{f}_q(x)| dx \le \epsilon_1.$$

Fig. 5. Algorithm 5. Approximation of the function $f(x) = e^{-x}$ by a piecewise polynomial function $\tilde{f} : [0, +\infty) \to \mathbb{R}$.

Then there exists a q such that the inequality (13) is satisfied. The convergence to zero is not monotonic but we can find an upper bound for the quantity of q using Cauchy-Schwarz inequality:

$$\int_0^1 |e^{-\ell x} - \tilde{f}_q(x)| dx \le \left[\int_0^1 (e^{-\ell x} - \tilde{f}_q(x))^2 dx\right]^{1/2}$$
$$= \left[\frac{1-e^{-2\ell}}{2\ell} - \sum_{j=0}^{q} \frac{\alpha_j^2}{2j+1}\right]^{1/2}.$$

The right-hand side is now monotonically converges to zero which can be used to find an upper bound for the smallest value of q satisfying (13) (cf. step 4 of Algorithm 5). This upper bound must satisfy the inequality

$$\sum_{j=0}^{q} \frac{\alpha_j^2}{2j+1} \ge \frac{1-e^{-2\ell}}{2\ell} - \epsilon_1^2. \qquad \square$$

REFERENCES

[1] F. Baccelli, G. Cohen, and B. Gaujal, "Recursive equations and basic properties of timed Petri nets," *Discrete Event Dynamic Systems: Theory and Applications*, vol. 1, no. 4, pp. 415–439, Jun. 1992.

[2] H. P. Hillion and J. P. Proth, "Performance evaluation of job-shop systems using timed event graphs," *IEEE Trans. Autom. Control*, vol. 34, no. 1, pp. 3–9, Jan. 1989.

[3] B. Heidergott, G. J. Olsder, and J. W. van der Woude, *Max Plus at Work–Modeling and Analysis of Synchronized Systems: A Course on Max-Plus Algebra and Its Applications*. Princeton University Press, 2006.

[4] B. J. P. Roset, H. Nijmeijer, J. A. W. M. van Eekelen, E. Lefeber, and J. E. Rooda, "Event driven manufacturing systems as time domain control systems," in *Proc. 44th IEEE Conf. Decision and Control and European Control Conf. (CDC-ECC'05)*, Dec. 2005, pp. 446–451.

[5] J. A. W. M. van Eekelen, E. Lefeber, and J. E. Rooda, "Coupling event domain and time domain models of manufacturing systems," in *Proc. 45th IEEE Conf. Decision and Control (CDC'06)*, Dec. 2006, pp. 6068–6073.

[6] B. Heidergott, *Max-Plus Linear Stochastic Systems and Perturbation Analysis (The International Series on Discrete Event Dynamic Systems)*. Secaucus, NJ: Springer-Verlag New York, Inc., 2006.

[7] G. J. Olsder, J. A. C. Resing, R. E. De Vries, M. S. Keane, and G. Hooghiemstra, "Discrete event systems with stochastic processing times," *IEEE Trans. Autom. Control*, vol. 35, no. 3, pp. 299–302, Mar. 1990.

[8] J. A. C. Resing, R. E. de Vries, G. Hooghiemstra, M. S. Keane, and G. J. Olsder, "Asymptotic behavior of random discrete event systems," *Stochastic Processes and their Applications*, vol. 36, no. 2, pp. 195–216, Dec. 1990.

[9] J. W. van der Woude and B. Heidergott, "Asymptotic growth rate of stochastic max-plus systems that with a positive probability have a sunflower-like support," in *Proc. 8th Int. Workshop Discrete Event Systems (WODES'06)*, Jul. 2006, pp. 451–456.

[10] R. M. P. Goverde, B. Heidergott, and G. Merlet, "A coupling approach to estimating the Lyapunov exponent of stochastic max-plus linear systems," *European Journal of Operational Research*, vol. 210, no. 2, pp. 249–257, 2011.

[11] F. Baccelli, G. Cohen, G. J. Olsder, and J. P. Quadrat, *Synchronization and Linearity, An Algebra for Discrete Event Systems*. John Wiley and Sons, 1992.

[12] F. Baccelli and D. Hong, "Analytic expansions of max-plus Lyapunov exponents," *The Annals of Applied Probability*, vol. 10, no. 3, pp. 779–827, Aug. 2000.

[13] S. Gaubert and D. Hong, "Series expansions of Lyapunov exponents and forgetful monoids," INRIA, Tech. Rep. RR-3971, Jul. 2000.

[14] G. Merlet, "Cycle time of stochastic max-plus linear systems." *Electronic Journal of Probability*, vol. 13, no. 12, pp. 322–340, 2008.

[15] S. Farahani, T. J. J. van den Boom, H. van der Weide, and B. De Schutter, "An approximation approach for model predictive control of stochastic max-plus linear systems," in *Proc. 10th Int. Workshop Discrete Event Systems (WODES'10)*, Berlin, DE, Aug./Sep. 2010, pp. 386–391.

[16] S. Farahani, T. J. J. van den Boom, and B. De Schutter, "Exact and approximate approaches to the identification of stochastic max-plus-linear systems," *Discrete Event Dynamic Systems: Theory and Applications*, pp. 1–25, Apr. 2013.

[17] K. Cechlárová and R. A. Cuninghame-Green, "Interval systems of max-separable linear equations," *Linear Algebra and its Applications*, vol. 340, no. 1-3, pp. 215–224, 2002.

[18] K. Cechlárová, "Eigenvectors of interval matrices over maxplus algebra," *Discrete Applied Mathematics*, vol. 150, no. 1-3, pp. 2–15, 2005.

[19] H. Myšková, "Interval systems of max-separable linear equations," *Linear Algebra and its Applications*, vol. 403, no. 0, pp. 263–272, 2005.

[20] D. Adzkiya, B. De Schutter, and A. Abate, "Finite abstractions of max-plus-linear systems," *IEEE Trans. Autom. Control*, vol. 58, no. 12, pp. 3039–3053, Dec. 2013.

[21] R. P. Kurshan, *Computer-Aided Verification of Coordinating Processes: The Automata-Theoretic Approach*, ser. Princeton Series in Computer Science. Princeton University Press, 1994.

[22] C. Baier, J. P. Katoen, and H. Hermanns, "Approximate symbolic model checking of continous-time Markov chains," in *Proc. 10th Int. Conf. Concurrency Theory (CONCUR'99)*, ser. Lecture Notes in Computer Science, J. C. M. Baeten and S. Mauw, Eds. Springer, Heidelberg, 1999, vol. 1664, pp. 146–162.

[23] M. Kwiatkowska, G. Norman, R. Segala, and J. Sproston, "Verifying quantitative properties of continuous probabilistic timed automata," in *Proc. 11th Int. Conf. Concurrency Theory (CONCUR'00)*, ser. Lecture Notes in Computer Science, C. Palamidessi, Ed. Springer, Heidelberg, 2000, vol. 1877, pp. 123–137.

[24] R. Alur and D. L. Dill, "A theory of timed automata," *Theoretical Computer Science*, vol. 126, no. 2, pp. 183–235, 1994.

[25] H. J. Kushner and P. G. Dupuis, *Numerical Methods for Stochastic Control Problems in Continuous Time*. New York: Springer-Verlag, 2001.

[26] P. Chaput, V. Danos, P. Panangaden, and G. Plotkin, "Approximating Markov processes by averaging," *Journal of the ACM*, vol. 61, no. 1, pp. 5:1–5:45, Jan. 2014.

[27] K. Koutsoukos and D. Riley, "Computational methods for reachability analysis of stochastic hybrid systems," in *Hybrid Systems: Computation and Control (HSCC'06)*, ser. Lecture Notes in Computer Science, J. Hespanha and A. Tiwari, Eds. Springer, Heidelberg, 2006, vol. 3927, pp. 377–391.

[28] M. Prandini and J. Hu, "Stochastic reachability: Theory and numerical approximation," in *Stochastic hybrid systems*, ser. Automation and Control Engineering Series 24, C. G. Cassandras and J. Lygeros, Eds. Taylor & Francis Group/CRC Press, 2006, pp. 107–138.

[29] A. Abate, M. Prandini, J. Lygeros, and S. Sastry, "Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems," *Automatica*, vol. 44, no. 11, pp. 2724–2734, 2008.

[30] A. Abate, J. P. Katoen, J. Lygeros, and M. Prandini, "Approximate model checking of stochastic hybrid systems," *European Journal of Control*, vol. 16, no. 6, pp. 624–641, 2010.
[31] S. Esmaeil Zadeh Soudjani and A. Abate, "Adaptive gridding for abstraction and verification of stochastic hybrid systems," in *Proc. 8th Int. Conf. Quantitative Evaluation of Systems (QEST'11)*, Sep. 2011, pp. 59–69.
[32] ——, "Adaptive and sequential gridding procedures for the abstraction and verification of stochastic processes," *SIAM Journal on Applied Dynamical Systems*, vol. 12, no. 2, pp. 921–956, 2013.
[33] I. Tkachev and A. Abate, "Formula-free finite abstractions for linear temporal verification of stochastic hybrid systems," in *Hybrid Systems: Computation and Control (HSCC'13)*. ACM, 2013, pp. 283–292.
[34] A. Abate, "Approximation metrics based on probabilistic bisimulations for general state-space Markov processes: a survey," *Electronic Notes in Theoretical Computer Sciences*, pp. 3–25, 2014.
[35] J. Desharnais, A. Edalat, and P. Panangaden, "Bisimulation for labelled Markov processes," *Information and Computation*, vol. 179, no. 2, pp. 163 – 193, 2002.
[36] S. K. Jha, E. M. Clarke, C. J. Langmead, A. Legay, A. Platzer, and P. Zuliani, "A Bayesian approach to model checking biological systems," in *Computational Methods in Systems Biology*, ser. Lecture Notes in Computer Science, P. Degano and R. Gorrieri, Eds. Springer, Heidelberg, 2009, vol. 5688, pp. 218–234.
[37] M. Rungger, M. Mazo, Jr., and P. Tabuada, "Specification-guided controller synthesis for linear systems and safe linear-time temporal logic," in *Hybrid Systems: Computation and Control (HSCC'13)*, 2013, pp. 333–342.
[38] M. B. Horowitz, E. M. Wolff, and R. M. Murray, "A compositional approach to stochastic optimal control with co-safe temporal logic specifications," in *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS'14)*, Sep. 2014, pp. 1466–1473.
[39] P. Zuliani, A. Platzer, and E. M. Clarke, "Bayesian statistical model checking with application to stateflow/simulink verification," *Formal Methods in System Design*, vol. 43, no. 2, pp. 338–367, 2013.
[40] X. Ding, S. L. Smith, C. Belta, and D. Rus, "Optimal control of Markov decision processes with linear temporal logic constraints," *IEEE Trans. Autom. Control*, vol. 59, no. 5, pp. 1244–1257, May 2014.
[41] M. Kwiatkowska, G. Norman, and D. Parker, "PRISM 4.0: Verification of probabilistic real-time systems," in *Proc. 23rd Int. Conf. Computer Aided Verification (CAV'11)*, ser. Lecture Notes in Computer Science, G. Gopalakrishnan and S. Qadeer, Eds., vol. 6806. Springer, Heidelberg, 2011, pp. 585–591.
[42] J. P. Katoen, M. Khattri, and I. S. Zapreev, "A Markov reward model checker," in *Proc. 2nd Int. Conf. Quantitative Evaluation of Systems (QEST'05)*. Los Alamos, CA, USA: IEEE Computer Society, 2005, pp. 243–244.
[43] D. Adzkiya, S. Esmaeil Zadeh Soudjani, and A. Abate, "Finite abstractions of stochastic max-plus-linear systems," in *Proc. 11th Int. Conf. Quantitative Evaluation of Systems (QEST'14)*, ser. Lecture Notes in Computer Science, G. Norman and W. Sanders, Eds. Springer International Publishing, 2014, vol. 8657, pp. 74–89.
[44] R. M. P. Goverde, "Railway timetable stability analysis using max-plus system theory," *Transportation Research Part B: Methodological*, vol. 41, no. 2, pp. 179–201, 2007.
[45] C. Baier and J.-P. Katoen, *Principles of Model Checking*. The MIT Press, 2008.
[46] S. Esmaeil Zadeh Soudjani, C. Gevaerts, and A. Abate, "FAUST^2: Formal abstractions of uncountable-state stochastic processes," in *Tools and Algorithms for the Construction and Analysis of Systems (TACAS'15)*, ser. Lecture Notes in Computer Science, C. Baier and C. Tinelli, Eds. Springer, Heidelberg, 2015, vol. 9035, pp. 272–286.
[47] S. Esmaeil Zadeh Soudjani and A. Abate, "Precise approximations of the probability distribution of a Markov process in time: an application to probabilistic invariance," in *Tools and Algorithms for the Construction and Analysis of Systems (TACAS'14)*, ser. Lecture Notes in Computer Science, E. Ábrahám and K. Havelund, Eds. Springer, Heidelberg, 2014, vol. 8413, pp. 547–561.

Sadegh Esmaeil Zadeh Soudjani is a postdoctoral researcher in the Department of Computer Science at the University of Oxford (UK). He received the B.Sc. degrees in electrical engineering and pure mathematics, and the M.Sc. degree in control engineering from the University of Tehran, Tehran, Iran, in 2007 and 2009, respectively. He obtained a Ph.D. degree from the Delft Center for Systems and Control, Delft University of Technology, Delft, The Netherlands, in 2014. He was also a visiting scholar at Max Planck Institute for Software Systems, Kaiserslautern, Germany, in 2015.

His current research interests include analysis, verification, and controller synthesis of complex dynamical models – in particular of stochastic hybrid systems – and in their applications in cyber-physical systems, including smart grids, energy networks, and biological systems.

Dieky Adzkiya is a lecturer in the Department of Mathematics at Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia. He received the B.Sc. degree in September 2005 and the M.Sc. degree in October 2008, both in mathematics from Institut Teknologi Sepuluh Nopember. He received the Ph.D. degree in systems and control in October 2014 and after that he continued as a Postdoctoral Researcher until June 2015, both at the Delft Center for Systems and Control, Delft University of Technology, Delft, The Netherlands.

His research interests are in the analysis and verification of discrete-event systems and in their applications.

Alessandro Abate (S'02–M'08) is an Associate Professor in the Department of Computer Science at the University of Oxford (UK). He received a Laurea in Electrical Engineering in October 2002 from the University of Padova (IT), an MS in May 2004 and a PhD in December 2007, both in Electrical Engineering and Computer Sciences, at UC Berkeley (USA). He has been an International Fellow in the CS Lab at SRI International in Menlo Park (USA), and a PostDoctoral Researcher at Stanford University (USA), in the Department of Aeronautics and Astronautics. From June 2009 to mid 2013 he has been an Assistant Professor at the Delft Center for Systems and Control, TU Delft - Delft University of Technology (NL).

His research interests are in the verification and control of probabilistic and hybrid systems, and in their general application over a number of domains, particularly in systems biology and in energy.