Efficient Verification for Stochastic Mixed Monotone Systems

Maxence Dutreix and Samuel Coogan

***Abstract*— We present an efficient computational procedure to perform model checking on discrete-time, mixed monotone stochastic systems subject to an affine random disturbance. Specifically, we exploit the structure of such systems in order to efficiently compute a finite-state Interval-valued Markov Chain (IMC) that over-approximates the system's behavior. To that end, we first make the assumption that the disturbance is unimodal, symmetric, and independent on each coordinate of the domain. Next, given a rectangular partition of the state-space, we compute bounds on the probability of transition between all the states in the partition. The ease of computing the one-step reachable set of rectangular states under mixed monotone dynamics renders the computation of these transition bounds highly efficient. We furthermore investigate a method for over-approximating the IMC of mixed monotone systems when the disturbance is only approximately unimodal symmetric, and we discuss state-space refinement heuristics. Lastly, we present two verification case studies.**

I. Introduction

In recent years, much effort has been devoted to developing formal method techniques to check a wide array of systems against complex specifications [1], [2]. For cyber-physical systems, the state-space is often infinite, and a common approach to system verification is to abstract the dynamics into a finite set of states connected to one another by a finite number of transitions. These finite-state models enable to efficiently answer crucial questions about the dynamics of the original continuous system, such as *safety* or *reachability* [3], formulated in a variety of symbolic languages.

However, many formal methods techniques designed for deterministic or nondeterministic systems do not directly apply when stochastic components are present, and fewer works have been dedicated to the generalization of finite-state abstractions for stochastic systems. Among the approaches that have been developed, Markov chains with uncertain probabilities of transition have been studied in the context of Interval-Valued Markov Chains (IMC) in [4], [5]. These abstractions augment the properties of Markov chains by assigning a range of possible probabilities —as opposed to a single probability—for all state-to-state transitions. This approach motivates the development of novel machinery for performing *verification* and *synthesis* tasks on discrete-time stochastic systems [6], [7], [8]. In particular, [6] studied the problem of verifying a system against specifications given in *Probabilistic Computation Tree Logic* (PCTL) [9]. PCTL extends Computation Tree Logic (CTL) by introducing a probabilistic operator and permitting quantitative inquiries about the likelihood of paths over Markov chains [10]. The authors in [7] and [8] investigate the model checking problem for IMCs against PCTL specifications and ω-regular properties respectively.

Unfortunately, constructing interval-valued abstractions of stochastic systems is often a computationally expensive process, especially when the dynamics are nonlinear. Indeed, in the general case, calculating the exact lower and upper bounds of transitions between all discrete states involves numerical searches over the state space and evaluations of integrals, rendering this procedure highly time-inefficient. Nevertheless, we aim to show that this impractical computational blowup can be avoided in some cases by exploiting the inherent structure of the system's dynamics. Our proposed approach results in an IMC abstraction with conservative transition probability ranges, which remains sufficient for verification.

In particular, we consider a class of stochastic systems for which the dynamics exhibits a *mixed monotone* property [11], [12]. Mixed monotonicity generalizes the property of monotonicity for dynamical systems for which trajectories maintain a partial ordering on states [13], [14], [15]. Many physical systems have been shown to be monotone or mixed monotone such as biological systems [16] and transportation networks [17], [18], [19]. This mixed monotone property enables efficient computation of reachable sets: a rectangular over-approximation of the one-step reachable set from any rectangular discrete state is determined by evaluating a certain decomposition function at the least and the greatest point of that state. The significance of mixed monotonicity in computing reachable sets for discrete abstractions was revealed in [12]. Similar approaches were developed in [20], [21] for monotone systems, a special case of mixed monotone systems.

In this paper, we study mixed monotone systems that are subject to an affine random disturbance vector whose components are mutually independent and for which the probability distribution for each component is unimodal and symmetric. For such systems, we show that an upper bound and a lower bound on the probability of transitions between states of a rectangular partition are found by evaluating only two integrals per dimension and per transition. We make use of these bounds to create an IMC abstraction of the original system that is suitable for verification against, *e.g.*, complex PCTL formulas. Next, we relax our assumptions and allow for an affine disturbance whose distribution is only approximately unimodal and symmetric in each component. We show that the probability intervals of the IMC abstrac-

M. Dutreix is with the School of Electrical and Computer Engineering, Georgia Institute of Technology, maxdutreix@gatech.edu. S. Coogan is with the School of Electrical and Computer Engineering and the School of Civil and Environmental Engineering, Georgia Institute of Technology, sam.coogan@gatech.edu.

tion can be expanded to accommodate this approximation. Finally, we briefly discuss refinement techniques to reduce the uncertainty of a rectangular partition against three types of PCTL formulas.

We organize the paper as follows: Section 2 introduces key concepts and notations. Section 3 is a formal statement of the problem. In Section 4, we derive the core properties facilitating the computation of IMCs for stochastic mixed monotone systems with affine, unimodal, symmetric disturbances. In Section 5, we propose an algorithm for generating an IMC when the affine disturbance is not unimodal and symmetric. Section 6 discusses algorithms for state-space refinement. Section 7 demonstrates the performance of our techniques through several case studies. All proofs are contained in the Appendix.

II. Preliminaries

Throughout, all inequalities are interpreted elementwise so that, for $x, y \in \mathbb{R}^n$, $x \leq y$ means $x_i \leq y_i$ for $i = 1, \ldots, n$, and similarly for $\geq, <$ and $>$.

Let $D \subset \mathbb{R}^n$ be a compact rectangular set, i.e., $D = \{x : d^1 \leq x \leq d^2\}$ for some $d^1, d^2 \in \mathbb{R}^n$ satisfying $d^1 \leq d^2$. A *rectangular partition* P of the domain $D \subset \mathbb{R}^n$ is a collection of discrete states $P = \{Q_j\}_{j=1}^m$, $Q_j \subset D$, satisfying

- $Q_j = \{x : a^j \leq x \leq b^j\}$ for some $a^j, b^j \in \mathbb{R}^n$ such that $a^j \leq b^j$, $\forall j = 1, \ldots, m$,
- $\bigcup_{j=1}^m Q_j = D$,
- $\mathbf{int}(Q_j) \cap \mathbf{int}(Q_\ell) = \emptyset \ \ \forall j, \ell, \ j \neq \ell$

where $\mathbf{int}$ denotes interior.

For $Q_j \in P$, $Q_j = \{x : a^j \leq x \leq b^j\}$ is a compact rectangular set and a^j, b^j are respectively called the *least point* and the *greatest point* of Q_j. For vectors, we reserve the subscript to index elements of the vector so that, *e.g.*, a_i^j for $i \in \{1, \ldots, n\}$ denotes the i-th element of $a^j \in \mathbb{R}^n$.

An *Interval-Valued Markov Chain (IMC)* is a triple $\mathscr{I} = (Q, \check{T}, \hat{T})$ where:

- Q is a finite set of states,
- $\check{T} : Q \times Q \to [0, 1]$ maps pairs of states to a lower transition bound so that $\check{T}_{Q_j \to Q_\ell} := \check{T}(Q_j, Q_\ell)$ denotes the lower bound of the transition probability from state Q_j to state Q_ℓ, and
- $\hat{T} : Q \times Q \to [0, 1]$ maps pairs of states to an upper transition bound so that $\hat{T}_{Q_j \to Q_\ell} := \hat{T}(Q_j, Q_\ell)$ denotes the upper bound of the transition probability from state Q_j to state Q_ℓ,

and $\check{T}$ and $\hat{T}$ satisfy $\check{T}(Q_j, Q_\ell) \leq \hat{T}(Q_j, Q_\ell)$ for all $Q_j, Q_\ell \in Q$ and

$$\sum_{Q_\ell \in P} \check{T}(Q_j, Q_\ell) \leq 1 \leq \sum_{Q_\ell \in P} \hat{T}(Q_j, Q_\ell) \tag{1}$$

for all $Q_j \in P$.

IMCs generalize Markov chains by assigning a range of transition probabilities between any pair of states Q_j and Q_ℓ. When $\check{T} = \hat{T}$, the IMC becomes a Markov chain. Trajectories of an IMC evolve in the following way: when the IMC transitions from some state Q_j, a collection of transition probabilities to other states is realized such that the transition probabilities satisfy the constraints imposed by $\check{T}$ and $\hat{T}$. If the IMC visits state Q_j again at some point in the future, it is possible that a different collection of transition probabilities is realized.

In this paper, our primary interest in IMCs is for their use in verifying probabilistic system properties such as "the probability that the goal state Q_ℓ is eventually reached is at least 98%" or "the probability that an undesirable state Q_ℓ is reached in the next 5 steps is less than 1%". Such system properties can be succinctly stated in, *e.g.*, Probabilistic Computation Tree Logic (PCTL), and we wish to verify such properties against all possible instantiations of transition probabilities for the IMC. As such, we assume that transition probabilities are nondeterministically realized at each step of the IMC's evolution. Thus, for the verification problem, we will reason about worst-case realizations.

III. Problem Formulation

We consider the discrete-time stochastic system

$$x[k+1] = \mathscr{F}(x[k], w[k]) \tag{2}$$

where $x[k] \in D \subset \mathbb{R}^n$ is the state of the system at time k, domain D is a compact rectangle, $w[k] \in W \subset \mathbb{R}^p$ is a random disturbance, and $\mathscr{F} : D \times W \to D$ is a continuous map. At each time-step k, the random disturbance $w[k]$ is sampled from a probability distribution with density function $f_w : \mathbb{R}^p \to \mathbb{R}_{\geq 0}$ satisfying $f_w(z) = 0$ if $z \notin W$.

Definition 1 (IMC Abstraction)**.** *Given the system* (2) *evolving on a domain $D \subset \mathbb{R}^n$ and a partition $P = \{Q_j\}_{j=1}^m$ of D, an IMC $\mathscr{I} = (Q, \check{T}, \hat{T})$ is an* abstraction *of* (2) *if:*

- *$P = Q$, that is, the finite set of states of the IMC is the partition set P, and*
- *For all $Q_j, Q_\ell \in P$,*

$$\check{T}_{Q_j \to Q_\ell} \leq \min_{x \in Q_j} Pr(\mathscr{F}(x, w) \in Q_\ell), \text{ and} \tag{3}$$

$$\hat{T}_{Q_j \to Q_\ell} \geq \max_{x \in Q_j} Pr(\mathscr{F}(x, w) \in Q_\ell), \tag{4}$$

where $Pr(\mathscr{F}(x, w) \in Q_\ell)$ for fixed x denotes the probability that (2) *transitions from x to some state $x' = F(x, w)$ contained in Q_ℓ.*

The IMC abstraction $\mathscr{I}$ is said to be tight *if* (3) *and* (4) *hold with equality.*

The potential of IMCs as a tool for model-checking stochastic systems motivates this approach [6]. To that end, for any pair of states Q_j and Q_ℓ belonging to P, we seek to find an upper and a lower bound on the probability of transition from Q_j to Q_ℓ as in (3) and (4).

We remark that evaluating the right-hand side of (3) and (4) requires a search over all $x \in Q_j$ in the general case. Moreover, evaluating $Pr(\mathscr{F}(x, w) \in Q_\ell)$ generally involves

integrating the stochastic kernel induced by the system (2) over the set Q_ℓ.

Therefore, it is generally impractical to solve these expressions for equality in order to find the tightest IMC. Several methods for over-approximating these transition bounds have been proposed. In [22] and [23], the authors use a point representation of each state in a grid partition to derive bounds on the transition probabilities. However, these derivations rely on Lipschitz bounds of the system's transition kernel, which can result in overly conservative approximations. The work in [6] proposes to approximate each state in the state-space by a large finite set of points over which (3) and (4) are estimated. We show in this paper that potentially less conservative and more efficient techniques can be used for a wide class of systems. We underline the fact that evaluating a PCTL formula from an over-approximation of the tightest IMC is sufficient for verification, as proved in [23].

Our goal is to construct an abstraction of system (2) in the form of an IMC to be used for system verification. Specifically, we address the following two problems.

Problem 1: Given stochastic system (2) and rectangular partition P, construct an IMC abstraction of (2).

Problem 2: If necessary, refine the partition P in order to construct an IMC abstraction with tighter transitions bounds for system verification.

It is apparent that there always exists an IMC abstraction induced by any partition P since we may trivially take $\check{T}_{Q_i \to Q_j} = 0$ and $\widehat{T}_{Q_i \to Q_j} = 1$ for all $Q_i, Q_j \in P$. Thus, in Problem 1, we seek an IMC such that the transition bounds are not overly conservative and such that that IMC is sufficient for system verification where "sufficiency" depends on the problem specification, desired level of accuracy, *etc.*, as illustrated in the case studies of Section VIII. To solve Problem 2, inspired by the refinement approach proposed in [6], we discuss a refinement procedure particularly well-suited for a certain class of PCTL formulas and for the rectangular partitions studied in this paper. The efficiency of this approach is also demonstrated in the case studies.

IV. Mixed Monotone Systems Affine in Disturbance

In the remainder of this paper, we study a large class of stochastic systems that proves amenable to efficient computation. In particular, we consider affine-in-disturbance systems of the form

$$x[k+1] = \mathscr{F}(x[k]) + w[k] \tag{5}$$

with specific assumptions on F and the distribution of the random disturbance w. We first introduce several definitions and then specify these assumptions.

Definition 2 (Mixed monotone function)**.** *A function $\mathscr{F} : D \to D$ with D a rectangular domain is* mixed monotone *if there exists a* decomposition function $g : D \times D \to D$ *satisfying [11], [12]:*

- $\forall x \in D : \mathscr{F}(x) = g(x, x)$
- $\forall x^1, x^2, y \in D : x^1 \leq x^2$ *implies* $g(x^1, y) \leq g(x^2, y)$
- $\forall x, y^1, y^2 \in D : y^1 \leq y^2$ *implies* $g(x, y^2) \leq g(x, y^1)$

Mixed monotonicity generalizes the notion of monotonicity in dynamical systems, which is recovered when $g(x, y) = F(x)$ for all x, y. Systems with monotone state update maps exhibit considerable structure useful for analysis and control [24], [25], [15], [14]. More recently, systems with mixed monotone state update maps have been shown to enjoy many of these same structural properties [12], [11]. For example, for mixed monotone $\mathscr{F}$ with decomposition function g, for $x, y, z \in D$ satisfying $x \leq z \leq y$, we have $g(x, y) \leq \mathscr{F}(z) \leq g(y, x)$. This leads to the following proposition.

Proposition 1 ([12, Theorem 1])**.** *Let $\mathscr{F} : D \to D$ be mixed monotone with decomposition function $g : D \times D \to D$, and let $a, b \in D$ satisfy $a \leq b$. Then*

$$\{\mathscr{F}(x) : a \leq x \leq b\} \subseteq \{z : g(a, b) \leq z \leq g(b, a)\}.$$

Proposition 1 implies that the one-step reachable set from the rectangular region bounded between a and b is overapproximated by the rectangular region bounded by the two points $g(a, b)$ and $g(b, a)$. This property will prove key for efficient computation of IMC abstractions.

Definition 3 (Unimodal distribution)**.** *For a random disturbance $\omega \in \Omega \subset \mathbb{R}$ with Ω an interval, its probability density function $f_\omega : \mathbb{R} \to \mathbb{R}$ is* unimodal *if f_ω is differentiable on Ω and there exists a unique number $c \in \mathbb{R}$, referred as the mode of the distribution, such that, for $x \in \Omega$:*

- $x < c \Rightarrow f'_\omega(x) \geq 0$,
- $x = c \Rightarrow f'_\omega(x) = 0$, *and*
- $x > c \Rightarrow f'_\omega(x) \leq 0$.

For simplicity, we will only consider distributions without a "flat" peak, that is, unimodal distributions with a unique mode c.

Definition 4 (Symmetric distribution)**.** *For a random disturbance $\omega \in \Omega \subset \mathbb{R}$ with Ω an interval, its probability density function $f_\omega : \mathbb{R} \to \mathbb{R}$ is* symmetric *if there exists a number $d \in \mathbb{R}$ such that $f_\omega(d - x) = f_\omega(d + x)$ for all x.*

Note that if f_ω is unimodal with mode c and symmetric, then it must be that $f_\omega(c - x) = f_\omega(c + x)$.

Throughout the remainder of the paper, we make the following assumptions.

Assumption 1. *$\mathscr{F}(x)$ in* (5) *is mixed monotone with decomposition function $g(x, y)$.*

Assumption 2. *The random disturbance $w[k]$ in* (5) *is of the form $w[k] = \begin{bmatrix} w_1[k] & w_2[k] & \dots & w_n[k] \end{bmatrix}^T$, where each $w_i \in W_i \subset \mathbb{R}$ has probability density function $f_{w_i}(x_i)$, W_i is an interval, and the collection $\{w_i\}_{i=1}^n$ is mutually independent. Denote by $F_{w_i}(x) = \int_{-\infty}^{x} f_{w_i}(\sigma) d\sigma$ the cumulative distribution function for w_i.*

Moreover, until Section VI, we make the following additional assumption.

Assumption 3. *The probability density function f_{w_i} for each random variable w_i is symmetric and unimodal with mode c_i.*

In Section VI, we will relax Assumption 3 to allow for affine disturbances that are only approximately symmetric and unimodal.

V. Approximating Transition Probabilities for Mixed Monotone Dynamics

We decompose our procedure for bounding the transition probability from a state Q_1 to a state Q_2 in two steps: first, we compute the rectangular over-approximation of the $\mathscr{F}$-reachable set from state Q_1 by taking advantage of the mixed monotonicity property. Next, we determine the positions of f_w within this rectangular region that respectively minimize and maximize its overlap with Q_2. In the next section, we exploit the characteristics of w previously evoked to streamline the calculation of these extremum points.

Proposition 2. *Consider system* (5) *under Assumptions 1–3. Let $Q_1 = \{x : a^1 \leq x \leq b^1\}$ and $Q_2 = \{x : a^2 \leq x \leq b^2\}$ be two nonempty rectangular sets with least point a^j and greatest point b^j for $j = 1, 2$. Then*

$$\min_{x \in Q_1} Pr(\mathscr{F}(x) + w \in Q_2) \geq \prod_{i=1}^{n} \min_{z_i \in [g_i(a^1,b^1), g_i(b^1,a^1)]} \int_{a_i^2}^{b_i^2} f_{w_i}(x - z_i) dx \quad (6)$$

and

$$\max_{x \in Q_1} Pr(\mathscr{F}(x) + w \in Q_2) \leq \prod_{i=1}^{n} \max_{z_i \in [g_i(a^1,b^1), g_i(b^1,a^1)]} \int_{a_i^2}^{b_i^2} f_{w_i}(x - z_i) dx \quad (7)$$

where g_i denotes the i-th element of $g(x, y)$, the decomposition function of $\mathscr{F}$.

Recall that all proofs are found in the appendix. Before generalizing to higher dimensions, we treat a 1-dimensional version of our original problem. In Lemma 1, we prove that for a fixed interval $[a, b] \subset \mathbb{R}$, there exists a unique position for a unimodal and symmetric distribution which maximizes its integral over $[a, b]$.

Lemma 1. *Let $\omega \in \Omega \subset \mathbb{R}$ with Ω an interval be a random variable with symmetric and unimodal probability density function $f_\omega : \mathbb{R} \to \mathbb{R}$ and mode $c \in \mathbb{R}$. For any $a, b \in \mathbb{R}$ satisfying $a \leq b$ and any $r_1, r_2 \in \mathbb{R}$ satisfying $r_1 \leq r_2$, let*

$$s_{max} = \frac{a+b}{2} - c$$

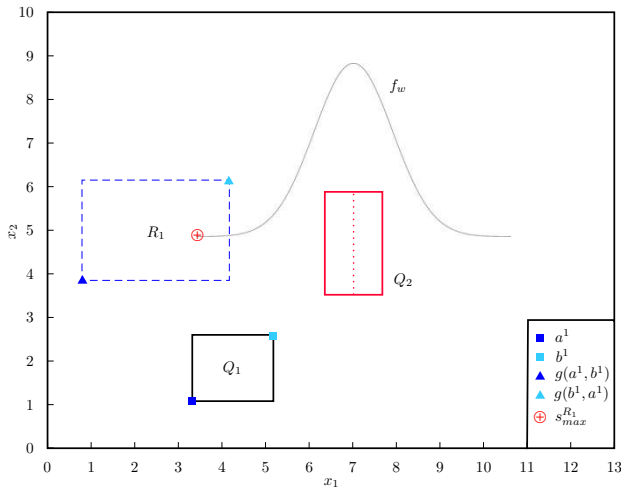

Fig. 1. Schematic depiction of the procedure for computing an upper bound on the probability of transition from Q_1 to Q_2. First, the one-step reachable set R_1 from Q_1 is over-approximated by evaluating the decomposition function at only two extremal points, regardless of the state-space dimension. Then, the distribution of $z+w$ is positioned as close to the center of Q_2 as possible under the restriction that $z \in R_1$. A lower bound on the transition probability is achieved by positioning the distribution as far from the center of Q_2 as possible.

and define

$$s_{max}^r = \arg\min_{s \in [r_1, r_2]} |s_{max} - s| = \begin{cases} s_{max}, & \text{if } s_{max} \in [r_1, r_2] \\ r_2, & \text{if } s_{max} > r_2 \\ r_1, & \text{if } s_{max} < r_1, \end{cases}$$

$$s_{min}^r = \arg\max_{s \in [r_1, r_2]} |s_{max} - s| = \begin{cases} r_1, & \text{if } s_{max} < \frac{r_1 + r_2}{2} \\ r_2, & \text{otherwise.} \end{cases}$$

Then

$$\max_{s \in [r_1, r_2]} \int_a^b f_\omega(x - s)\, dx = \int_a^b f_\omega(x - s_{max}^r)\, dx \quad (8)$$

$$\min_{s \in [r_1, r_2]} \int_a^b f_w(x - s)\, dx = \int_a^b f_\omega(x - s_{min}^r)\, dx. \quad (9)$$

When $s_{max} \in [r_1, r_2]$ in Lemma 1, the lemma confirms the intuitive idea that the integral of a unimodal, symmetric distribution over some interval $I = [a, b]$ is maximized when the peak of its probability distribution lies at the center of I. However, for the type of systems considered in this work, the shift of such distributions will always be restricted to take values within a given rectangular set $[r_1, r_2]$ so that, when $s_{max} \notin [r_1, r_2]$, the shift $s \in [r_1, r_2]$ maximizing the overlap of the density function over I is the one closest to the global maximizing shift s_{max}. Conversely, a shift $s \in [r_1, r_2]$ minimizing this overlap is the one furthest from s_{max}.

Theorem 1 combines Lemma 1 and Proposition 2 in order to provide a procedure for efficiently constructing an IMC abstraction for (5) given a rectangular partition of its domain D.

Theorem 1. *Consider system* (5) *under Assumptions 1–3 and let* $P = \{Q_j\}_{j=1}^m$ *be a rectangular partition of* D *with each* $Q_j = \{x : a^j \leq x \leq b^j\}$ *for some* $a^j, b^j \in \mathbb{R}^n$ *satisfying* $a^j \leq b^j$. *For all* $Q_j, Q_\ell \in P$, *let*

$$s_{i,max}^{\ell} = \frac{a_i^\ell + b_i^\ell}{2} - c_i \text{ for } i = 1, \ldots, n, \tag{10}$$
$$\breve{r}^j = g(a^j, b^j),$$
$$\widehat{r}^j = g(b^j, a^j),$$

and define

$$\widehat{T}_{Q_j \to Q_\ell} = \prod_{i=1}^{n} \int_{a_i^\ell}^{b_i^\ell} f_{w_i}(x_i - s_{i,max}^{j\to\ell})\, dx_i, \tag{11}$$
$$= \prod_{i=1}^{n} \left(F_{w_i}(b_i^\ell - s_{i,max}^{j\to\ell}) - F_{w_i}(a_i^\ell - s_{i,max}^{j\to\ell}) \right),$$

$$\breve{T}_{Q_j \to Q_\ell} = \prod_{i=1}^{n} \int_{a_i^\ell}^{b_i^\ell} f_{w_i}(x_i - s_{i,min}^{j\to\ell})\, dx_i \tag{12}$$
$$= \prod_{i=1}^{n} \left(F_{w_i}(b_i^\ell - s_{i,min}^{j\to\ell}) - F_{w_i}(a_i^\ell - s_{i,min}^{j\to\ell}) \right)$$

where F_{w_i} *is the cumulative distribution function for* w_i *and*

$$s_{i,max}^{j\to\ell} = \begin{cases} s_{i,max}^{\ell}, & \text{if } s_{i,max}^{\ell} \in [\breve{r}_i^j, \widehat{r}_i^j] \\ \widehat{r}_i^j, & \text{if } s_{i,max}^{\ell} > \widehat{r}_i^j \\ \breve{r}_i^j, & \text{if } s_{i,max}^{\ell} < \breve{r}_i^j, \end{cases} \tag{13}$$

$$s_{i,min}^{j\to\ell} = \begin{cases} \breve{r}_i^j, & \text{if } s_{max} < \frac{\breve{r}_i^j + \widehat{r}_i^j}{2} \\ \widehat{r}_i^j, & \text{otherwise}. \end{cases} \tag{14}$$

Then $\mathscr{I} = (P, \breve{T}, \widehat{T})$ *is an IMC abstraction of* (5).

Theorem 1 is a main contribution of this work. Given a system of the form (5) satisfying Assumptions 1 to 3, and a rectangular partition P, it shows that an IMC abstraction of (5) can be computed efficiently. Specifically, for any state in P, we establish an over-approximation of its one-step reachable set by evaluating the system's decomposition function at only two points. Likewise, finding the maximizing and minimizing shifts inside the reachable sets decouples along each coordinate and involves a number of operations and conditional statements that is linear in the dimension n of the state-space, according to (13) and (14). Finally, we see in (11) and (12) that n integral evaluations are needed per transition bound. Presuming the cumulative distribution function F_{w_i} for each w_i is available to us, this last step amounts to $2n$ function evaluations per bound. The practical implications of Theorem 1 can then be implemented in the form of Algorithm 1.

Algorithm 1: Computation of an IMC abstraction for a rectangular partition P

Input : Partition $P = \{Q_j\}_{j=1}^m$,
Probability density functions f_{w_i} and modes $c_i \in \mathbb{R}$ for each component of disturbance,
Cumulative distribution functions F_{w_i} of f_{w_i}
System decomposition function g
Output: IMC abstraction $\mathscr{I}$ of (5)

```
for j = 1, 2, ..., n do
    Set r̂^j = g(b^j, a^j) and r̆^j = g(a^j, b^j)
    for ℓ = 1, 2, ..., n do
        for i = 1, 2, ..., n do
            Compute s^ℓ_{i,max} according to (10)
            Compute s^{j→ℓ}_{i,max} and s^{j→ℓ}_{i,min} according to (13) and (14)
        end
        Compute T̂_{Q_j→Q_ℓ} and T̆_{Q_j→Q_ℓ} according to (11) and (12)
    end
end
return I = (P, T̆, T̂)
```

VI. IMC Abstraction for Arbitrary Affine Disturbances

In Section 4, we exploited the crucial facts that each component of the random disturbance w of system (5) was unimodal and symmetric in order to efficiently construct an IMC approximation. Unfortunately, real-world systems rarely encounter disturbances displaying these two properties. In such instances, one could resort to purely numerical techniques to generate an IMC. We instead develop an alternate solution by approximating the original distribution with another one which is unimodal and symmetric. Then, the tools derived in Section 3 can be utilized on the approximation distribution. In this section, we introduce a method for generating an IMC abstraction of the original system: we first compute an IMC using the approximation distribution, and then adjust its transition bounds appropriately.

To that end, consider random disturbance $w \in \mathbb{R}^n$ of (5) and suppose the collection $\{w_i\}_{i=1}^n$ remains mutually independent, but we no longer assume that each w_i is unimodal and symmetric, *i.e.*, Assumption 3 no longer holds. However, we assume that each w_i is reasonably approximated by a unimodal and symmetric distribution. To this end, many metrics exist to quantify the similarity between two probability distributions. Here, the maximum absolute difference between the original distribution w and its approximation v is our metric of choice, and we replace Assumption 3 with the following Assumption.

Assumption 3b. *There exists a mutually independent collection of random variables* $\{v_i\}_{i=1}^n$ *and constants* $\{\delta_i\}_{i=1}^n$ *such that* $v_i \in V_i$, *the probability density function* f_{v_i} *for each* v_i *is unimodal and symmetric with mode* $\tilde{c}_i$, *and*

$$\delta_i \geq \max_{x_i \in \mathbb{R}} |f_{v_i}(x_i) - f_{w_i}(x_i)|.$$

In Assumption 3b, recall that f_{w_i} is the probability density

function of $w_i \in W_i$, the i-th component of the random disturbance w.

The main result of this section, Theorem 2 below, states that we are able to determine an upper and a lower bound on the probabilities of transition between any two states in system (5) subject to disturbance w through an efficient computation of the bounds assuming instead that the system is subject to the random disturbance v.

Theorem 2. *Consider system* (5) *under Assumptions 1, 2, and 3b, and let $P = \{Q_j\}_{j=1}^m$ be a rectangular partition of D with each $Q_j = \{x : a^j \leq x \leq b^j\}$ for some $a^j, b^j \in \mathbb{R}^n$ satisfying $a^j \leq b^j$. For all $Q_j, Q_\ell \in P$, let*

$$\tilde{s}_{i,max}^{\ell} = \frac{a_i^\ell + b_i^\ell}{2} - \tilde{c}_i$$

and let $\breve{r}^j = g(a^j, b^j)$ and $\widehat{r}^j = g(b^j, a^j)$. Define

$$\widehat{T}^*_{Q_j \to Q_\ell} = \prod_{i=1}^{n} \left(\int_{a_i^\ell}^{b_i^\ell} f_{v_i}(x_i - \tilde{s}_{i,max}^{j\to\ell})\, dx_i + \delta_i(b_i^\ell - a_i^\ell) \right), \tag{15}$$

$$\breve{T}^*_{Q_j \to Q_\ell} = \prod_{i=1}^{n} \left(\int_{a_i^\ell}^{b_i^\ell} f_{v_i}(x_i - \tilde{s}_{i,min}^{j\to\ell})\, dx_i - \delta_i(b_i^\ell - a_i^\ell) \right) \tag{16}$$

where

$$\tilde{s}_{i,max}^{j\to\ell} = \begin{cases} \tilde{s}_{i,max}^{\ell}, & \text{if } \tilde{s}_{i,max}^{\ell} \in [\breve{r}_i^j, \widehat{r}_i^j] \\ \widehat{r}_i^j, & \text{if } \tilde{s}_{i,max}^{\ell} > \widehat{r}_i^j \\ \breve{r}_i^j, & \text{if } \tilde{s}_{i,max}^{\ell} < \breve{r}_i^j, \end{cases}$$

$$\tilde{s}_{i,min}^{j\to\ell} = \begin{cases} \breve{r}_i^j, & \text{if } \tilde{s}_{max} < \frac{\breve{r}_i^j + \widehat{r}_i^j}{2} \\ \widehat{r}_i^j, & \text{otherwise}. \end{cases}$$

Then $\mathscr{I} = (P, \breve{T}^*, \widehat{T}^*)$ is an IMC abstraction of (5).

Although similar to Theorem 1, Theorem 2 relaxes Assumption 3 and considers an arbitrary disturbance w to system (5). It assumes the existence of a random disturbance v that is unimodal, symmetric and characterized by its maximum absolute difference with w as stated in Assumption 3b. This allows us to efficiently compute an IMC abstraction for (5) by applying the equations in Theorem 1 to disturbance v with the addition of an error term in the bounds (15) and (16). The error terms solely involve the multiplication of two known quantities and do not significantly affect the complexity of computing the IMC as compared to Theorem 1. However, it should be noted that the conservatism of an IMC generated from Theorem 2 strongly depends on the δ_i parameters. The latter are scaled by the size of the destination states and added to the IMC bounds, meaning that a large maximum absolute distance between w and v can only be compensated by a reduction of the states' size and an increase in the number of states in the partition. As such, even though this method can be applied to arbitrary disturbances, it is most practical if w originally displays a probability density profile that is almost symmetric and unimodal.

The proof of Theorem 2 requires the following lemma in which we first restrict ourselves to a one-dimensional framework.

Lemma 2. *Let $\omega \in \Omega \subset \mathbb{R}$ with Ω an interval be a random variable with probability density function $f_\omega : \mathbb{R} \to \mathbb{R}$. Let $\nu \in \Omega \subset \mathbb{R}$ be another random variable with symmetric and unimodal probability density function $f_\nu : \mathbb{R} \to \mathbb{R}$ with mode $\tilde{c}$, and let δ satisfy $\delta \geq \max_{x\in\mathbb{R}} |f_\omega(x) - f_\nu(x)|$. For any $a, b \in \mathbb{R}$ satisfying $a \leq b$ and any $r_1, r_2 \in \mathbb{R}$ satisfying $r_1 \leq r_2$,*

$$\begin{aligned} &\max_{s\in[r_1,r_2]} \int_a^b f_\omega(x-s)\, dx \\ &\qquad \leq \max_{s\in[r_1,r_2]} \int_a^b f_\nu(x-s)\, dx + \delta(b-a) \\ &\min_{s\in[r_1,r_2]} \int_a^b f_\omega(x-s)\, dx \\ &\qquad \geq \min_{s\in[r_1,r_2]} \int_a^b f_\nu(x-s)\, dx - \delta(b-a). \end{aligned}$$

Lemma 2 is the enabling step in the proof Theorem 2 in the appendix.

VII. State-space Refinement

Once an IMC abstraction of the system has been produced, we seek to exploit it to perform verification. A standard logic for expressing specifications in probabilistic terms is PCTL. A PCTL formula ϕ is of the form

$$\phi = \mathscr{P}_{\bowtie p_{sat}}[\Psi]$$

where $\bowtie \in \{\leq, <, \geq, >\}$, $p_{sat} \in [0, 1]$ is a probability and Ψ is a path formula [2]. A *path formula* expresses a specification over trajectories of the dynamical system. For example, the specification "the trajectory always remains in region A" is a path formula which can be written symbolically as $\Box A$ where $\Box$ is the "always" temporal operator. A state $x^0 \in D$ *satisfies* ϕ if the probability that trajectories $x[k]$ initialized with $x[0] = x^0$ satisfy Ψ is less than or equal to p_{sat} in the case that $\bowtie = \leq$, and similarly for the other possibilities for $\bowtie$. Examples of several PCTL formulas and their interpretations are given alongside the case studies of Section VIII. For further details on the syntax and semantics of PCTL, see [2].

Given a state-space partition P of $D \subset \mathbb{R}^n$, we model check against ϕ by assigning a probability interval $[p_{min}^j, p_{max}^j]$ of satisfying Ψ for all states $Q_j \in P$. The techniques for determining these intervals from an IMC are not the focus of this paper and we apply the same procedure as in [6]. Any state Q_j such that $p_{sat} \in]p_{min}^j, p_{max}^j[$ when $\bowtie \in \{\leq, \geq\}$, or $p_{sat} \in [p_{min}^j, p_{max}^j]$ when $\bowtie \in \{<, >\}$, is undecided with respect to ϕ and we write $Q_j \in Q^?$. The remaining states in P either satisfy ϕ or do not satisfy ϕ. The sets of states satisfying a PCTL formula ϕ are denoted by Q^{yes}, while those not satisfying ϕ belong to the set Q^{no}.

That is, for any $Q^j \in Q^{yes}$, all $x \in Q^j$ satisfy ϕ, and for any $Q^j \in Q^{no}$, all $x \in Q^j$ are guaranteed to not satisfy ϕ.

Upon completion of verification, P is characterized by the volume of uncertain states $Q^?$. We address the issue of reducing the uncertain volume and briefly suggest refinement heuristics for the "next", "until" and "bounded until" path formulas. These algorithms terminate once $I_d^{max} < I_d$, where $I_d^{max} = \max_{i \text{ s.t. } Q_j \in Q^?} |p_{max}^j - p_{min}^j|$ and $I_d \in [0,1]$ is a user-specified precision parameter.

A. Next Path Formula

Given a set $\mathscr{D} \subset \mathbb{R}^n$, a PCTL formula $\phi = \mathscr{P}_{\bowtie p_{sat}}[X\mathscr{D}]$ including the Next operator X raises the question:

"Which states in P have a probability of reaching a state labeled by $\mathscr{D}$ in one time-step that is less (or greater) than p_{sat}?"

Presume $Q_j \in Q^?$. We want to reduce the size $|p_{max}^j - p_{min}^j|$ of the transition probability interval of reaching $\mathscr{D}$ from Q_j. A standard technique for achieving this is to create a new partition P' by dividing a selection of states in P into smaller ones. This process causes P' to be a new partition of D with reduced uncertainty [6].

In this particular case, only local refinement of Q_j is necessary. Indeed, subdividing another state Q_ℓ does not affect the one-time-step reachability properties of Q_j. Furthermore, we must ensure that P' is a rectangular partition of D. Hence, we propose the following refinement procedure:

1) $\forall Q_j \in Q^?$, split Q_j into two hyperrectangles along its largest dimension.
2) Compute the probability intervals of transition for the new partition and perform model-checking.
3) If $I_d^{max} > I_d$, return to step 1. Else, terminate.

Note that only the transitions from the states in $Q^?$ need to be computed when evaluating this one-time-step formula. This renders verification against Next operators computationally efficient as compared to formulas comprising multiple-time-steps operators.

B. Until and Bounded Until Operators Path Formulas

PCTL formulas with Until and Bounded Until Operators are respectively of the form

$$\phi_a = \mathscr{P}_{\bowtie p_{sat}}[\mathscr{D}' \, \mathcal{U} \, \mathscr{D}]$$
$$\phi_b = \mathscr{P}_{\bowtie p_{sat}}[\mathscr{D}' \, \mathcal{U}^{\leq k} \, \mathscr{D}]$$

where $\mathscr{D}' = \{Q_{j'}\}_{j'=1}^m$ and $\mathscr{D} = \{Q_j\}_{j=1}^l$, $Q_{j'}, Q_j \subset \mathbb{R}^n$, are two sets of states. ϕ_a asks

"Which states in P have a probability of reaching a state labeled by $\mathscr{D}$ before reaching a state not in $\mathscr{D}'$ that is less (or greater) than p_{sat}?"

while ϕ_b requests

"Which states in P have a probability of reaching a state labeled by $\mathscr{D}$ in k time steps or less before reaching a state not in $\mathscr{D}'$ that is less (or greater) than p_{sat}?"

Here, local refinement of states in $Q^?$ may not be the most appropriate method to reduce uncertainty in the IMC. When the operator involves multiple time steps, the behavior of the successor states of a given Q_j affects the probability of reaching some state in k steps from Q_j. Thus, refining states in Q^{yes} and Q^{no} may contribute to reducing the size of the $[p_{min}, p_{max}]$ interval for some states in $Q^?$.

To account for that fact, we implement the following refinement algorithm:

1) $\forall Q_j \in Q^{yes} \cup Q^{no}$, compute a score $\sigma_j = (p_{max}^j - p_{min}^j) \times \sum_{Q_\ell \in P} (\widehat{T}_{Q_\ell \to Q_j} - \check{T}_{Q_\ell \to Q_j})$. p_{max}^j and p_{min}^j are bounds on the probability of satisfying the formula of interest from state Q_j in the current partition. Score σ_j can be interpreted as a measure of the uncertainty caused by state Q_j in the abstraction.
2) $\forall Q_j \in Q^?$, split Q_j into two hyperrectangles along its largest dimension. Then, split the states in $Q^{yes} \cup Q^{no}$ with the n greatest (non-zero) scores in the same fashion, where n is a user-dependent parameter.
3) Compute the probability intervals of transition in the new partition and perform model-checking.
4) If $I_d^{max} > I_d$, return to step 1. Else, terminate.

These heuristics are implemented in the next section for our case studies. Refining Q^{no} states appears to significantly improve the runtime in comparison to algorithms focusing primarily on $Q^?$ states, Q^{yes} states, and their spatial neighbors, as it is the case in [6]. Nevertheless, a complete refinement approach for general PCTL formulas remains a subject for future research.

VIII. Case Studies

In this section, we perform verification on two mixed monotone systems with affine disturbance against various PCTL specifications. IMCs are computed according to Section 3 and 4, while the model-checking procedures are the same as in [6].

A. Planar System

We investigate two case studies proposed in [6, Section VIII-A]. Consider the system $x[k+1] = Ax[k] + w[k]$ with

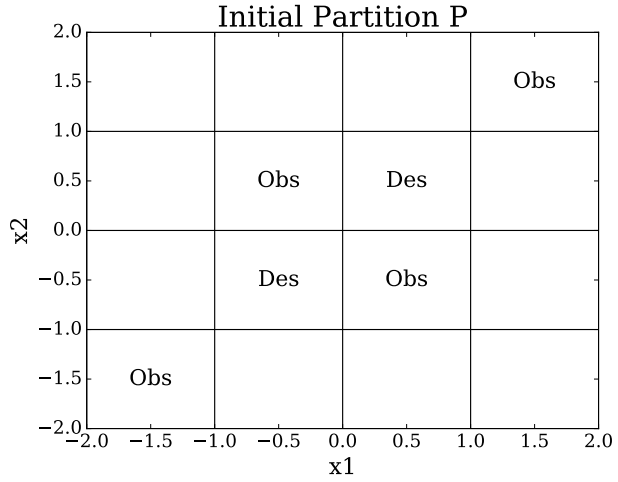

Fig. 2. Initial partition P of the state space displaying the Obstacle (**Obs**) and Destination (**Des**) regions for the case studies in Section VIII-A.

$w[k] \in W$ where

$$A = \begin{bmatrix} 0.4 & 0.1 \\ 0 & 0.5 \end{bmatrix},$$
$$W = \left\{ x \in \mathbb{R}^2 : \begin{bmatrix} -0.4 \\ -0.4 \end{bmatrix} \leq x \leq \begin{bmatrix} 0.4 \\ 0.4 \end{bmatrix} \right\}.$$

In addition, w is drawn from the truncated Normal distribution f_w given by

$$f_w(y) = \begin{cases} \frac{\mathcal{N}(y,0,0.09I)}{\int_W \mathcal{N}(z,0,0.09I)dz} & \text{if } y \in W \\ 0 & \text{Otherwise} \end{cases}$$

where I is the identity matrix and $\mathcal{N}(\cdot, 0, 0.09I)$ is the zero-mean Normal distribution with covariance matrix $0.09I$. We note that this system is monotone—a special case of mixed monotone systems—and the procedure derived in the previous sections can be applied to it. In particular, we take $g(x, y) = Ax$ as the decomposition function for $\mathscr{F}(x) = Ax$.

Our goal is to find a set of initial states satisfying some specification written as a PCTL formula, and, following [6], we consider the two PCTL formulas

$$\phi_1 = P_{<0.05}[X\textbf{Obs}],$$
$$\phi_2 = P_{\geq 0.90}[\neg\textbf{Obs}\, \mathcal{U}\, \textbf{Des}],$$

where $\neg$ denotes the 'Not' operator, **Obs** $\subset \mathbb{R}^2$ is the union of four rectangular "obstacle" regions, and **Des** $\subset \mathbb{R}^2$ is the union of two "destination" regions as shown in Figure 2. Thus, ϕ_1 states "the probability that the state of the system in the next time-step is within the obstacle region is less than 0.05," and ϕ_2 states "the probability that the system remains outside of the obstacle region until reaching the destination region is greater than or equal to 0.90".

For both specifications, we initially perform model checking using an initial course partition P as shown in Fig. 2. The results for this step are displayed in the top plots of Fig. 3 and Fig. 4. Next, we execute the refinement algorithm of Section VII on P until the interval of satisfaction for Ψ_i for all $Q^?$ states has size smaller than $I_d = 0.05$ where $\Psi_1 = X\textbf{Obs}$ and $\Psi_2 = \neg\textbf{Obs}\ \mathcal{U}\ \textbf{Des}$ in accordance with ϕ_1 and ϕ_2; recall that $Q^?$ states are those partition regions for which we cannot conclude with certainty whether the specification is satisfied or not because the interval of satisfaction contains p_{sat} ($p_{sat} = 0.05$ in the case of ϕ_1 and $p_{sat} = 0.90$ in the case of ϕ_2).

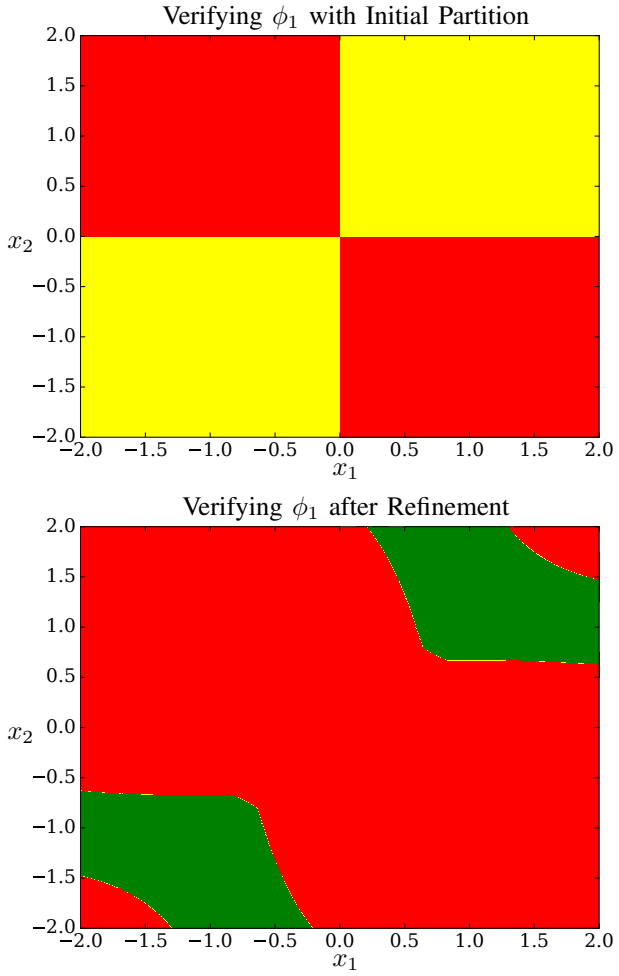

Fig. 3. Results for specification ϕ_1 with the initial partition (top) and the final partition after refinement when $I_d = 0.001$ (bottom). Red states do not satisfy the specification, green states satisfy the specification, while yellow states are undecided.

We use Python as our programming language for all simulations. The latter were conducted on a OS X 10.16 computer endowed with 8 GB of memory and a 3.3 GHz Intel Core i7 processor. The total computation times for the initial abstraction generation, verification and refinement all together were 1.14 and 14.3 seconds for ϕ_1 and ϕ_2 respectively. In [6], the authors employed a sampling-based technique to construct an IMC abstraction, requiring multiple expensive integral evaluations, and achieved the same level of precision in 4.8 and 51.4 hours respectively. Moreover, our refinement algorithm generated 210 states for ϕ_1 and 452 states for ϕ_2, while approximately twice as many states

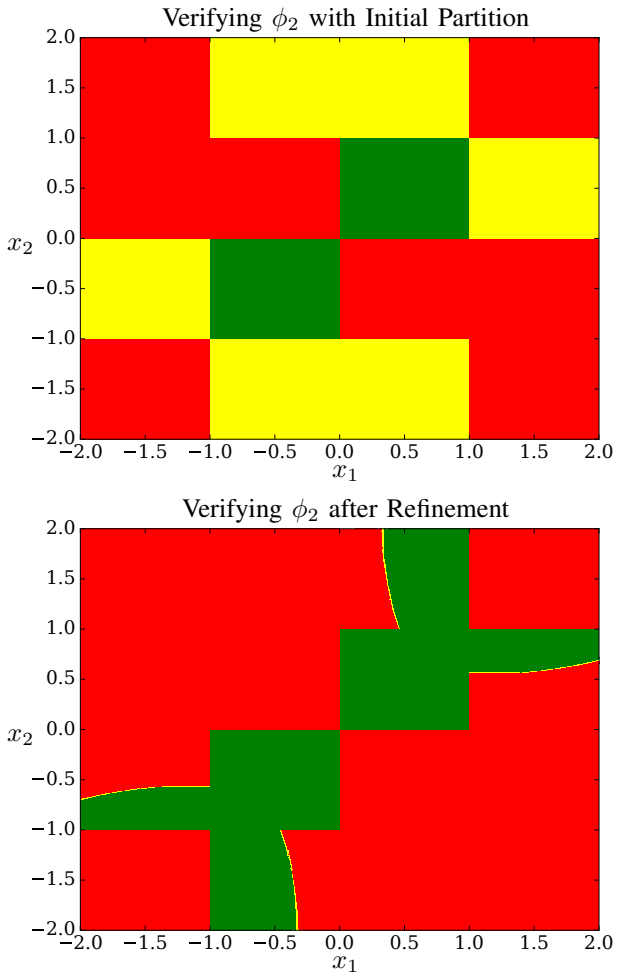

Fig. 4. Results for specification ϕ_2 with the initial partition (top) and the final partition after refinement when $I_d = 0.005$ (bottom). Red states do not satisfy the specification, green states satisfy the specification, while yellow states are undecided.

were produced in [6] for the same level of precision. We hypothesize that these computational improvements were due to both a more efficient abstraction generation and a better targeted refinement, although further work is required to fully understand the separate contributions of these improvements to the overall computation time.

In addition, we increase the precision of our results by a factor of 50 for the specification ϕ_1 by reducing the size of I_d to 0.001. For specification ϕ_2, we enhance the precision by a factor of 10 and choose $I_d = 0.005$. We show the final model-checked state-spaces in Fig. 3 and Fig.4. The algorithm terminated in 33.15 minutes and produced 10388 states for the specification ϕ_1, while verifying against ϕ_2 took 15.5 hours to run and generated 15329 states.

We remark that our method is particularly powerful when the disturbance takes values from a compact set. Via the over-approximation of the reachable set, we can quickly check whether the affine disturbance can attain a given state or not, avoiding unnecessary integral evaluations.

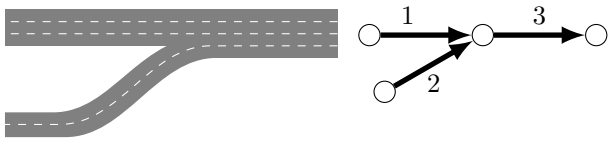

Fig. 5. Sketch of a merging junction consisting of three links.

B. Merging Traffic Junction: Gaussian Approximation of Poisson Distributions

We now present a 3-dimensional case study for a model of a merging traffic junction as displayed in Fig. 5. This example demonstrates the applicability of our technique to a nonlinear system, as well as the practical relevance of the derivations in Section VI. Traffic flow results in mixed monotone dynamics [26], and new vehicles entering traffic networks can readily be interpreted as affine disturbances. The following monotone discrete-time system describes the time evolution of the junction in Fig. 5 and is a slight modification of the model contained in [27]:

$$x^1[k+1] = x^1[k] - \min\left\{D(x^1[k]), \frac{\alpha}{\beta}S(x^3[k])\right\} + w_1 \tag{17}$$

$$x^2[k+1] = x^2[k] - \min\{D(x^2[k]), \bar{\alpha}S(x^3[k]), u[k]\} + w_2 \tag{18}$$

$$\begin{aligned} x^3[k+1] = x^3[k] &+ \min\{\beta D(x^1[k]), \alpha S(x^3[k])\} \\ &+ \min\{D(x^2[k]), \bar{\alpha}S(x^3[k]), u[k]\} \\ &- D(x^3[k]) - w_3 \end{aligned} \tag{19}$$

where $x^1[k]$, $x^2[k]$, $x^3[k]$ are the queue lengths of links 1, 2 and 3 respectively at time k; $D(x) = \min\{c, vx\}$ is a traffic demand function with c and v respectively denoting the capacity and free-flow speed; $S(x) = \bar{w}(\bar{x} - x)$ is a traffic supply function where $\bar{w}$ is a coefficient relating the available space on a given link and the supply on that link and $\bar{x}$ stands for the jam occupancy; α and $\bar{\alpha}$ denote supply weights for link 1 and 2 and respectively; β determines the fraction of vehicles leaving link 1 to enter link 3 at each time step; $u[k]$ is a parameter representing the maximum number of cars allowed to drive from link 2 to link 3 in one time step; w_1 and w_2 are disturbances corresponding to a random flow of cars entering the system through link 1 and 2 at each time step, while w_3 is a random number of cars exiting the system along link 3.

In reality, the arrival rates at Link 1 and 2, as well as the departure rate at Link 3, can only take integer values and are appropriately modeled by Poisson distributions. Although unimodal, Poisson distributions are not symmetric and the techniques developed in Section 3 do not directly apply. We thus choose to approximate each w_i by a unimodal, symmetric distribution v_i. We exploit the property that, for large λ, $Poisson(\lambda) \simeq \mathcal{N}(\lambda, \lambda)$. We denote by λ_i the mean arrival (or departure) rate of Link i and make the following

Parameter	Value
c	100
v	0.5
α	1
$\bar{\alpha}$	5
β	0.75
$\bar{x}$	800
$\bar{w}$	0.5/3
$u[k] = u$	60

TABLE I

PARAMETER VALUES FOR SYSTEM (26)

approximations:

$$w_1 \sim Poisson(\lambda_1 = 100) \simeq v_1 \sim \mathcal{N}(100, 100)$$
$$w_2 \sim Poisson(\lambda_2 = 100) \simeq v_2 \sim \mathcal{N}(100, 100)$$
$$w_3 \sim Poisson(\lambda_3 = 60) \simeq v_3 \sim \mathcal{N}(60, 60).$$

We determine that $\delta_1 = 0.000895$, $\delta_2 = 0.000895$ and $\delta_3 = 0.0015$ satisfies $\delta_i \geq \max_{x_i \in \mathbb{R}} |v_i(x) - w_i(x)|$.

The initial partition P is shown in Fig. 5. We aim to model-check system (28) against the specification

$$\phi_3 = P_{\geq 0.90}[true\, \mathcal{U}^{\leq 3}\ \textbf{Des}]$$

where $\textbf{Des} = \{x \in \mathbb{R}^3 : 0 \leq x_i < 400 \text{ for } i = 1, 2, 3\}$ is the set of states that have all three queue lengths strictly smaller than 400. We interpret ϕ_3 as *"What are the set of states that reach a queue length shorter than 400 for all 3 links, within 3 time steps, with probability greater than or equal to 0.90?"*.

We evaluate ϕ_3 over the initial partition P using these approximations and conduct refinement with precision $I_d = 0.20$. We stop the refinement process after the volume of the uncertain states $Q^?$ falls below 5 percent. The running time was 15 hours and 35 minutes. The final partition is shown in Fig. 6 and contains 16403 states. Green-colored states are certain to satisfy ϕ_3, red-colored stats are certain to not satisfy ϕ_3, and yellow-colored may or may not satisfy ϕ_3.

IX. CONCLUSIONS

We have developed an efficient algorithm for computing the IMC of a mixed monotone system with affine disturbance over rectangular partitions. We demonstrated our techniques through two case studies and significantly reduced the computational cost of verification and refinement compared to other approaches previously employed.

Exploring the potential of mixed monotonicity for solving synthesis problems in stochastic controlled systems is a natural step for future work. In addition, the implementation of more efficient refinement procedures is necessary to improve the scalability of IMCs to higher dimensions. Finally, alternative local approximations of arbitrary distributions may be examined to reduce conservatism in the bounds derived in Section 4.

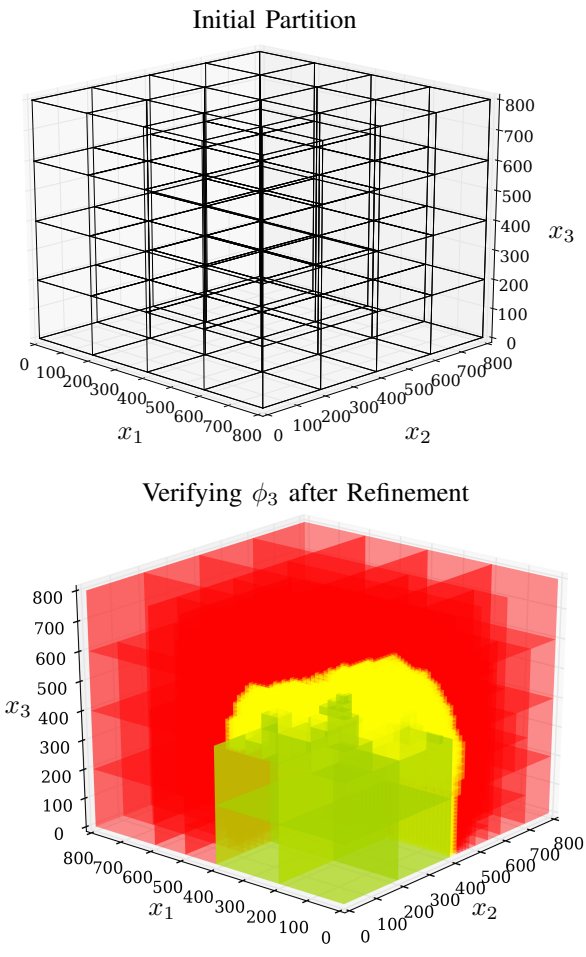

Fig. 6. The initial partition P of the state-space for system (17)–(19) (top) and the results of verification against ϕ_3 after refinement (bottom). Refinement was interrupted when the volume of $Q^?$ states reached 5 percent of the total state-space volume. Red states do not satisfy the specification, green states satisfy the specification, while yellow states are undecided.

REFERENCES

[1] E. M. Clarke, O. Grumberg, and D. A. Peled, *Model checking*. MIT press, 1999.

[2] C. Baier and J. Katoen, *Principles of Model Checking*. MIT Press, 2008.

[3] P. Tabuada, *Verification and control of hybrid systems: A symbolic approach*. Springer, 2009.

[4] L. V. Utkin and I. O. Kozine, "Computing system reliability given interval-valued characteristics of the components," *Reliable computing*, vol. 11, no. 1, pp. 19–34, 2005.

[5] D. Škulj, "Discrete time markov chains with interval probabilities," *International journal of approximate reasoning*, vol. 50, no. 8, pp. 1314–1329, 2009.

[6] M. Lahijanian, S. B. Andersson, and C. Belta, "Formal verification and synthesis for discrete-time stochastic systems," *IEEE Transactions on Automatic Control*, vol. 60, no. 8, pp. 2031–2045, 2015.

[7] K. Sen, M. Viswanathan, and G. Agha, "Model-checking markov chains in the presence of uncertainties," in *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pp. 394–410, Springer, 2006.

[8] K. Chatterjee, K. Sen, and T. A. Henzinger, "Model-checking ω-regular properties of interval markov chains," in *International Conference on Foundations of Software Science and Computational Structures*, pp. 302–317, Springer, 2008.

[9] H. Hansson and B. Jonsson, "A logic for reasoning about time and reliability," *Formal aspects of computing*, vol. 6, no. 5, pp. 512–535, 1994.
[10] C. Baier, J.-P. Katoen, and K. G. Larsen, *Principles of model checking*. MIT press, 2008.
[11] H. Smith, "Global stability for mixed monotone systems," *Journal of Difference Equations and Applications*, vol. 14, no. 10-11, pp. 1159–1164, 2008.
[12] S. Coogan and M. Arcak, "Efficient finite abstraction of mixed monotone systems," in *Proceedings of the 18th International Conference on Hybrid Systems: Computation and Control*, pp. 58–67, ACM, 2015.
[13] M. W. Hirsch, "Systems of differential equations that are competitive or cooperative II: Convergence almost everywhere," *SIAM Journal on Mathematical Analysis*, vol. 16, no. 3, pp. 423–439, 1985.
[14] H. L. Smith, *Monotone dynamical systems: An introduction to the theory of competitive and cooperative systems*. American Mathematical Society, 1995.
[15] D. Angeli and E. Sontag, "Monotone control systems," *IEEE Transactions on Automatic Control*, vol. 48, no. 10, pp. 1684–1698, 2003.
[16] E. D. Sontag, "Monotone and near-monotone biochemical networks," *Systems and Synthetic Biology*, vol. 1, no. 2, pp. 59–87, 2007.
[17] G. Gomes, R. Horowitz, A. A. Kurzhanskiy, P. Varaiya, and J. Kwon, "Behavior of the cell transmission model and effectiveness of ramp metering," *Transportation Research Part C: Emerging Technologies*, vol. 16, no. 4, pp. 485–513, 2008.
[18] E. Lovisari, G. Como, and K. Savla, "Stability of monotone dynamical flow networks," in *Proceedings of the 53rd Conference on Decision and Control*, pp. 2384–2389, 2014.
[19] S. Coogan, M. Arcak, and A. A. Kurzhanskiy, "Mixed monotonicity of partial first-in-first-out traffic flow models," in *IEEE Conference on Decision and Control*, pp. 7611–7616, 2016.
[20] T. Moor and J. Raisch, "Abstraction based supervisory controller synthesis for high order monotone continuous systems," in *Modelling, Analysis, and Design of Hybrid Systems*, pp. 247–265, Springer, 2002.
[21] D. Gromov and J. Raisch, "Detecting and enforcing monotonicity for hybrid control systems synthesis," *IFAC Proceedings Volumes*, vol. 39, no. 5, pp. 395–401, 2006.
[22] A. Abate, A. D'Innocenzo, and M. D. Di Benedetto, "Approximate abstractions of stochastic hybrid systems," *IEEE Transactions on Automatic Control*, vol. 56, no. 11, pp. 2688–2694, 2011.
[23] 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.
[24] M. Hirsch and H. Smith, "Monotone dynamical systems," *Handbook of differential equations: Ordinary differential equations*, vol. 2, pp. 239–357, 2005.
[25] M. Hirsch and H. Smith, "Monotone maps: a review," *Journal of Difference Equations and Applications*, vol. 11, no. 4-5, pp. 379–398, 2005.
[26] S. Coogan, E. A. Gol, M. Arcak, and C. Belta, "Traffic network control from temporal logic specifications," *IEEE Transactions on Control of Network Systems*, vol. 3, no. 2, pp. 162–172, 2016.
[27] S. Coogan and M. Arcak, "Freeway traffic control from linear temporal logic specifications," in *Proceedings of the 5th ACM/IEEE International Conference on Cyber-Physical Systems*, pp. 36–47, 2014.

APPENDIX

A. Proof of Proposition 2

Proof. By Proposition 1, we observe

$$\{\mathscr{F}(x) : x \in Q_1\} \subseteq \{z : g(a^1, b^1) \leq z \leq g(b^1, a^1)\}. \quad (20)$$

To prove (6), we have

$$\begin{aligned}
&\min_{x \in Q_1} Pr(\mathscr{F}(x) + w \in Q_2) \\
&\geq \min_{z : g(a^1,b^1) \leq z \leq g(b^1,a^1)} Pr(z + w \in Q_2) && (21) \\
&= \min_{z : g(a^1,b^1) \leq z \leq g(b^1,a^1)} \prod_{i=1}^{n} Pr(z_i + w_i \in [a_i^2, b_i^2]) && (22) \\
&= \prod_{i=1}^{n} \min_{z_i : g_i(a^1,b^1) \leq z_i \leq g_i(b^1,a^1)} Pr(z_i + w_i \in [a_i^2, b_i^2]) && (23)
\end{aligned}$$

where (21) follows from (20), (22) follows from the mutual independence of all components of w in Assumption 2, and (23) holds because $g(a^1, b^1) \leq z \leq g(b^1, a^1)$ if and only if $g_i(a^1, b^1) \leq z_i \leq g_i(b^1, a^1)$ for all $i = 1, \ldots, n$. Then (6) holds because $Pr(z_i + w_i \in [a_i^2, b_i^2]) = \int_{a_i^2}^{b_i^2} f_{w_i}(x - z_i)dx$. Finally, (7) holds by a symmetric argument as above, replacing $\min$ with $\max$. □

B. Proof Lemma 1

Proof. For $s \in \mathbb{R}$, define $H(s) = \int_a^b f_\omega(x - s)\, dx$. We claim

$$H(s_{max}) = \max_{s \in \mathbb{R}} H(s),$$

and, moreover, for all $s_1, s_2 \in \mathbb{R}$ such that $|s_{max} - s_1| \geq |s_{max} - s_2|$, it holds that $H(s_1) \leq H(s_2)$, that is, $H(s)$ monotonically decreases as $|s_{max} - s|$ increases. Assuming the claim to be true, it follows that $\max_{s \in [r_1, r_2]} H(s) = H(s^r_{max})$ and $\min_{s \in [r_1, r_2]} H(s) = H(s^r_{min})$, *i.e.*, (8) and (9), completing the proof.

To prove the claim, we have, for all $s \in \mathbb{R}$,

$$\begin{aligned}
&H(s_{max}) - H(s) \\
&= \int_a^b f_\omega(x - s_{max})\, dx - \int_a^b f_\omega(x - s)\, dx \\
&= \int_{a - s_{max}}^{b - s_{max}} f_\omega(x)\, dx - \int_{a-s}^{b-s} f_\omega(x)\, dx \\
&= \int_{a - s_{max}}^{a-s} f_\omega(x)\, dx - \int_{b - s_{max}}^{b-s} f_\omega(x)\, dx \\
&= \int_0^{s_{max} - s} \left[f_\omega(x + \tfrac{a-b}{2} - c) - f_\omega(x + \tfrac{b-a}{2} - c) \right] dx. \qquad (24)
\end{aligned}$$

Moreover, because f_ω is symmetric and unimodal with mode c, $f_\omega(x + \frac{a-b}{2} - c) - f_\omega(x + \frac{b-a}{2} - c)$ is an odd function of x and is negative for $x > 0$ and positive for $x < 0$. Therefore, the integral in (24) is nonnegative and monotonically decreases as $|s_{max} - s|$ increases, thus proving the claim.

□

C. Proof of Theorem 1

Proof. For all $Q_j, Q_\ell \in P$ and $i = 1, \ldots, n$, by Lemma 1,

$$\min_{z_i \in [g_i(a^j, b^j), g_i(b^j, a^j)]} \int_{a_i^\ell}^{b_i^\ell} f_{w_i}(x - z_i) dx = \int_{a_i^\ell}^{b_i^\ell} f_{w_i}(x_i - s_{i,min}^{j \to \ell})\, dx_i,$$

$$\max_{z_i \in [g_i(a^j, b^j), g_i(b^j, a^j)]} \int_{a_i^\ell}^{b_i^\ell} f_{w_i}(x - z_i) dx = \int_{a_i^\ell}^{b_i^\ell} f_{w_i}(x_i - s_{i,max}^{j \to \ell})\, dx_i,$$

Then, by Proposition 2,

$$\min_{x \in Q_j} Pr(\mathscr{F}(x) + w \in Q_\ell) \geq \prod_{i=1}^{n} \int_{a_i^\ell}^{b_i^\ell} f_{w_i}(x_i - s_{i,min}^{j \to \ell})\, dx_i \tag{25}$$

$$\max_{x \in Q_j} Pr(\mathscr{F}(x) + w \in Q_\ell) \leq \prod_{i=1}^{n} \int_{a_i^\ell}^{b_i^\ell} f_{w_i}(x_i - s_{i,max}^{j \to \ell})\, dx_i, \tag{26}$$

so that (11)–(12) implies (3)–(4). Furthermore, (25)–(26) implies $\breve{T}(Q_j, Q_\ell) \leq \widehat{T}(Q_j, Q_\ell)$ and (3)–(4) implies (1) so that $\mathscr{I} = (P, \breve{T}, \widehat{T})$ is a valid IMC, concluding the proof. □

D. Proof of Lemma 2

Proof. Let s_{max}^ω and s_{min}^ω satisfy

$$\int_a^b f_\omega(x - s_{max}^\omega)\, dx = \max_{s \in [r_1, r_2]} \int_a^b f_\omega(x - s)\, dx,$$
$$\int_a^b f_\omega(x - s_{min}^\omega)\, dx = \min_{s \in [r_1, r_2]} \int_a^b f_\omega(x - s)\, dx.$$

Since $|f_\omega(x) - f_\nu(x)| \leq \delta\ \forall x$, we have

$$f_\omega(x - s_{max}^\omega) \leq f_\nu(x - s_{max}^\omega) + \delta\ \ \forall x$$

and it follows that

$$\int_a^b f_\omega(x - s_{max}^\omega)\, dx \leq \int_a^b f_\nu(x - s_{max}^\omega)\, dx + \delta(b - a) \leq \max_{s \in [r_1, r_2]} \int_a^b f_\nu(x - s)\, dx + \delta(b - a).$$

Similarly,

$$f_\omega(x - s_{min}^\omega) \geq f_\nu(x - s_{min}^\omega) - \delta\ \ \forall x$$

so that

$$\int_a^b f_\omega(x - s_{min}^\omega)\, dx \geq \int_a^b f_\nu(x - s_{min}^\omega)\, dx - \delta(b - a) \geq \min_{s \in [r_1, r_2]} \int_a^b f_\nu(x - s)\, dx - \delta(b - a).$$

□

E. Proof of Theorem 2

Proof. For all $Q_j, Q_\ell \in P$ and $i = 1, \ldots, n$, by Lemma 1 and Lemma 2,

$$\min_{z_i \in [g_i(a^1, b^1), g_i(b^1, a^1)]} \int_{a_i^2}^{b_i^2} f_{w_i}(x - z_i) dx \geq \int_{a_i^\ell}^{b_i^\ell} f_{v_i}(x_i - \tilde{s}_{i,min}^{j \to \ell})\, dx_i - \delta_i(b_i^\ell - a_i^\ell),$$

$$\min_{z_i \in [g_i(a^1, b^1), g_i(b^1, a^1)]} \int_{a_i^2}^{b_i^2} f_{w_i}(x - z_i) dx \leq \int_{a_i^\ell}^{b_i^\ell} f_{v_i}(x_i - \tilde{s}_{i,max}^{j \to \ell})\, dx_i + \delta_i(b_i^\ell - a_i^\ell).$$

The theorem then follows from Proposition 2 by following the same argument as in the proof of Theorem 1. □