Approximate abstractions of stochastic systems: a randomized method

Alessandro Abate and Maria Prandini

***Abstract*— This work introduces a randomized method for the design of an approximate abstraction of a stochastic system and the assessment of its quality. The proposed approach relies on the formulation of the problem as a semi-infinite chance-constrained optimization program and on its solution via randomization. The method has quite general applicability, since it only requires to be able to run multiple executions of the candidate abstract model and of the original system and to compute their distance. Two variants of the notion of distance are considered in view of a possible use of the approximate abstraction for probabilistic safety verification. The approach is tested on a numerical example.**

I. INTRODUCTION

This work is concerned with the design of an approximate abstraction of a stochastic system and the assessment of its quality. The goal is to obtain a simpler abstracted model that is accurate enough so that system verification can be performed on the model in place of the actual system.

An abstraction $\mathcal{M}$ of a system $\mathcal{S}$ is characterized by two properties: first, it has to resemble the behavior of the original system; second, it has to abstract the original system by being structurally simpler. The quantification of how $\mathcal{M}$ is close to $\mathcal{S}$ is clearly a key aspect of any procedure for designing an abstraction.

For deterministic, discrete-state models, abstractions can be precisely defined through the notion of bisimulation, which effectively equates to trace equivalence between $\mathcal{S}$ and $\mathcal{M}$, [3]. As intuitive, a relation based on trace equivalence becomes rather conservative when moving to models with continuous state spaces. Indeed, exact notions of bisimulation [2] for deterministic systems have recently given way to approximate versions [10], where the quality of the approximation between $\mathcal{S}$ and $\mathcal{M}$ is quantified via metrics that specify how close the trajectories of $\mathcal{S}$ and $\mathcal{M}$ are. This approach has led to the study of approximate abstractions for nonlinear [14] and switched systems [11].

Probabilistic, continuous-space models add another level of complexity to the study of abstractions, since realizations of $\mathcal{S}$ and $\mathcal{M}$ should not only be close, but also have the same likelihood. While the notion of bisimilarity for discrete-space probabilistic systems is well-studied [13], the attempts to extend it to continuous-space systems are confined either to specific classes of systems, [9], [15], or too restrictive, [5]. Thus, heading for some notion of approximate abstraction appears as a promising alternative also in a stochastic setting.

In [12], the notion of approximate probabilistic bisimulation between two stochastic hybrid systems $\mathcal{S}$ and $\mathcal{M}$ is introduced, which hinges on the computation of a bisimulation function via Lyapunov techniques. Along similar lines, [1] benefits from contractivity assumptions on the dynamics of $\mathcal{S}$ and $\mathcal{M}$ to extend the results in [12]. These contributions, however, present some limitations, in that, 1) they may lead to quite conservative bounds on the quality of $\mathcal{M}$ as an approximate abstraction of $\mathcal{S}$, 2) restrictive assumptions on the dynamics of the systems are required, and 3) a computational procedure to determine the approximate bisimulation function is given only for certain classes of systems, [12].

In this paper, we put forward a randomized approach to determine an approximate abstraction $\mathcal{M}$ of a stochastic system $\mathcal{S}$, which is as well applicable to a hybrid setting. The proposed approach relies on the formulation of the problem as a semi-infinite chance-constrained optimization program and on its solution via randomization. The method is inspired by [8], where model reduction is briefly discussed as a possible application to systems and control design of the so-called "scenario approach," which was first introduced for solving uncertain convex programs via randomization [6] and then extended to stochastic semi-infinite chance-constrained optimization programs [7].

Unlike [1], [12], we focus on finite time-horizon properties. Our approach is applicable to any stochastic system $\mathcal{S}$ and candidate abstract model $\mathcal{M}$ with no a-priori assumptions on their dynamics, the only requirement being to be able to run multiple executions of both $\mathcal{S}$ and $\mathcal{M}$. When evaluating the quality of the approximate abstraction, we consider two variants of the distance between the executions of $\mathcal{M}$ and $\mathcal{S}$, which are both effective for probabilistic safety analysis. Given that the solution is obtained via randomization and, hence, is a random quantity, results are valid with a certain degree of confidence that, however, is a design parameter and can be chosen as close to 1 as desired. An additional aspect that differentiates this work from previous ones in the literature is that design – and not only the analysis – of an approximate abstraction is addressed. The approach is tested on a numerical example. Proofs are omitted due to space limitations.

II. NOTION OF APPROXIMATE ABSTRACTION

Given a system $\mathcal{S}$ with a stochastic input $w(t)$, suppose that we are interested in verifying a finite time-horizon

Research supported by the European Commission under the MoVeS project FP7-ICT-2009-257005 and the Marie Curie grant MANTRAS 249295, and by NWO under VENI grant 016.103.020.

A. Abate is with the Delft Center for Systems and Control - TU Delft, Mekelweg 2, 2628 CD Delft, The Netherlands - a.abate@tudelft.nl

M. Prandini is with the Dipartimento di Elettronica e Informazione - Politecnico di Milano, piazza Leonardo da Vinci 32, 20133 Milano, Italy - prandini@elet.polimi.it

property of $\mathcal{S}$ that depends on the behavior of its output $y_{\mathcal{S}}(t)$ over some time-horizon $T = [0, t_f]$, with $t_f > 0$. Let the output signal $y_{\mathcal{S}}(t)$ take values in $\mathcal{Y} := \Re^p$.

Consider now a simplified model $\mathcal{M}$ of $\mathcal{S}$, fed by the same input $w(t)$ and with output $y_{\mathcal{M}}(t)$ taking values in $\mathcal{Y}$. Let the approximation error introduced by abstracting $\mathcal{S}$ with model $\mathcal{M}$ be expressed through some function $d_T : \mathcal{Y}^T \times \mathcal{Y}^T \to \Re_+$ that maps each pair of executions $y_{\mathcal{S}}(t)$, $t \in T$, and $y_{\mathcal{M}}(t)$, $t \in T$, into a positive real number $d_T(y_{\mathcal{S}}, y_{\mathcal{M}})$ and that quantifies the extent to which the execution of $\mathcal{S}$ differs from that of $\mathcal{M}$.

Note that $d_T(y_{\mathcal{S}}, y_{\mathcal{M}})$ is a random quantity that depends on the realization of the input $w(t)$ and the possibly stochastic initialization $(x_{\mathcal{S}}(0), x_{\mathcal{M}}(0))$ of $\mathcal{S}$ and $\mathcal{M}$. In order to avoid excessive conservativeness due, for instance, to the fact that some really unlikely realizations of the stochastic input $w(t)$ can cause a large discrepancy between the outputs $y_{\mathcal{S}}(t)$ and $y_{\mathcal{M}}(t)$, we require $\mathcal{M}$ to accurately describe $\mathcal{S}$ for all realizations of $w(t)$ and $(x_{\mathcal{S}}(0), x_{\mathcal{M}}(0))$ except for a violation set of (small) probability $\epsilon \in (0, 1)$.

This motivates the following definition of approximate abstraction. (see Figure 1 for a pictorial representation).

Definition 1 (approximate abstraction): Model $\mathcal{M}$ is a γ-approximate abstraction of $\mathcal{S}$ up to level $1-\epsilon$ if the following condition is satisfied:

$$P\big(d_T(y_{\mathcal{S}}, y_{\mathcal{M}}) \leq \gamma\big) \geq 1 - \epsilon, \tag{1}$$

where $P(\cdot)$ denotes the probability measure induced over the executions of $\mathcal{S}$ and $\mathcal{M}$ by the stochastic process $w(t)$ and the initial conditions $(x_{\mathcal{S}}(0), x_{\mathcal{M}}(0))$. □

Here, we assume that the probability in (1) is well-defined, which is quite straightforward to show for general functions $d_T(\cdot, \cdot)$ in the case of discrete-time systems. Technical issues may instead arise in a continuous-time setting as discussed in [4] with reference to reachability analysis of stochastic hybrid systems.

Remark 1: The smaller is γ in (1), the better is the approximation quality of model $\mathcal{M}$. As ϵ grows to 1, γ decreases towards zero, but, at the same time, the quality of the approximation as measured by γ becomes meaningless since it is guaranteed over a set of uncertainty instances whose probability $1 - \epsilon$ tends to zero. □

Remark 2: If $d_T(y_{\mathcal{S}}, y_{\mathcal{M}})$ is symmetric, i.e., $d_T(y_{\mathcal{S}}, y_{\mathcal{M}}) = d_T(y_{\mathcal{M}}, y_{\mathcal{S}})$ then, the role of $\mathcal{S}$ and $\mathcal{M}$ in Definition 1 can be exchanged, [12], hence $\mathcal{S}$ is a γ-approximate abstraction of $\mathcal{M}$, up to level $1 - \epsilon$. □

In the rest of the paper we consider the following two possible definitions of $d_T(y_{\mathcal{S}}, y_{\mathcal{M}})$:

$$d_T(y_{\mathcal{S}}, y_{\mathcal{M}}) = \sup_{t \in T} \|y_{\mathcal{S}}(t) - y_{\mathcal{M}}(t)\|; \tag{2}$$

$$d_T(y_{\mathcal{S}}, y_{\mathcal{M}}) = \sup_{t \in T} \inf_{\tau \in T} \|y_{\mathcal{S}}(t) - y_{\mathcal{M}}(\tau)\|. \tag{3}$$

The latter one is known as directional Hausdorff distance and, intuitively, quantifies how distant a point in the execution of $\mathcal{S}$ can be from any point in the execution of $\mathcal{M}$, without taking the timing aspect into account. Notice that the directional Hausdorff distance is not symmetric.

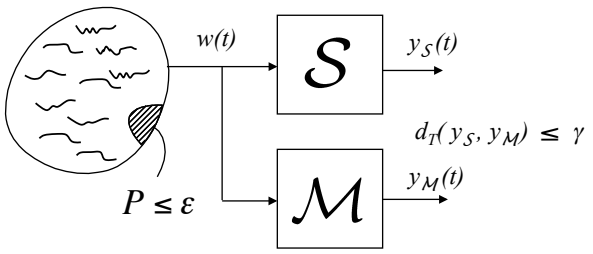

Fig. 1. Pictorial view of model $\mathcal{M}$ as an approximate abstraction of system $\mathcal{S}$, up to level $1 - \epsilon$.

Given that

$$\sup_{t \in T} \inf_{\tau \in T} \|y_{\mathcal{S}}(t) - y_{\mathcal{M}}(\tau)\| \leq \sup_{t \in T} \|y_{\mathcal{S}}(t) - y_{\mathcal{M}}(t)\|, \tag{4}$$

the notion of approximate abstraction based on (2) is stronger than that based on (3), i.e, if $\mathcal{M}$ is a γ-approximate abstraction of $\mathcal{S}$ up to level $1 - \epsilon$ according to (2), then, this implies that $\mathcal{M}$ is also a γ-approximate abstraction of $\mathcal{S}$ up to level $1-\epsilon$ according to (3), but not vice-versa. Also, given some model $\mathcal{M}$, its quality γ as approximate abstraction of $\mathcal{S}$ according to (3) would be typically better (lower) than that according to (2).

Next, we argue that both notions of approximate abstraction can be used for performing safety verification on $\mathcal{S}$. For the verification of more complex reachability properties, such as that of reaching some set only after passing through some region within a given finite time interval, however, the weaker notion of approximate abstraction is not adequate since the timing information is lost.

Suppose that we are interested in estimating the probability that the output $y_{\mathcal{S}}(t)$ of system $\mathcal{S}$ will enter some unsafe set A within the time horizon T. Let $\mathcal{M}$ be a γ-approximate abstraction of $\mathcal{S}$ up to level $1 - \epsilon$. Then, as suggested in [12], we can obtain an estimate of the probability of interest by expanding A as follows:

$$A_{\tilde{\gamma}} = \{y | \, \exists y' \in A \text{ such that } \|y - y'\| \leq \tilde{\gamma}\},$$

with $\tilde{\gamma} > \gamma$, and computing the probability that the output $y_{\mathcal{M}}(t)$ of the approximate abstraction $\mathcal{M}$ will enter $A_{\tilde{\gamma}}$. This is particularly convenient when it is easier to analyze the reachability properties of the (simpler) abstracted model $\mathcal{M}$ than those of system $\mathcal{S}$.

Proposition 1: If $\mathcal{M}$ is a γ-approximate abstraction of $\mathcal{S}$ up to level $1 - \epsilon$, then,

$$P(\exists t \in T \text{ such that } y_{\mathcal{S}}(t) \in A) \leq P(\exists t \in T \text{ such that } y_{\mathcal{M}}(t) \in A_{\tilde{\gamma}}) + \epsilon. \quad \square$$

III. Assessment of the quality of a model as an approximate abstraction

The quality γ of a model $\mathcal{M}$ as an approximate abstraction of $\mathcal{S}$ up to level $1-\epsilon$ can be assessed by solving the following chance-constrained optimization program:

$$\min_{\gamma \in \Re} \gamma \quad \text{subject to:} \quad P\big(d_T(y_{\mathcal{S}}, y_{\mathcal{M}}) \leq \gamma\big) \geq 1 - \epsilon. \tag{5}$$

This is a semi-infinite program since the number of optimization variables (γ) is finite, whereas the number of constraints is typically infinite (it is in fact given by $d_T(y_{\mathcal{S}}, y_{\mathcal{M}}) \leq \gamma$ for all executions $y_{\mathcal{S}}$, $y_{\mathcal{M}}$ in a set of probability at least $1-\epsilon$).

Let γ_ϵ denote the solution of (5). Then, model $\mathcal{M}$ is a γ_ϵ-approximate abstraction of $\mathcal{S}$ up to level $1-\epsilon$.

Computing γ_ϵ is generally difficult since it involves determining, among all the sets of executions of probability $1-\epsilon$, the one that provides the best (lowest) value for $d_T(y_{\mathcal{S}}, y_{\mathcal{M}})$. Interestingly, this computational issue can be solved using a randomized approach, as in Algorithm 1, which provides an estimate of γ_ϵ with provable approximation guarantees.

Algorithm 1 Randomized quality assessment

1: extract N realizations of the stochastic input $w^{(i)}(t)$, $t \in T$, $i = 1, 2, \ldots, N$, and N samples of the initial condition $(x_{\mathcal{S}}(0), x_{\mathcal{M}}(0))^{(i)}$, $i = 1, 2, \ldots, N$;

2: run the corresponding N executions of $\mathcal{M}$ and $\mathcal{S}$, thus obtaining N realizations of the output signals $y_{\mathcal{S}}^{(i)}(t)$ and $y_{\mathcal{M}}^{(i)}(t)$, $t \in T$, $i = 1, 2, \ldots, N$;

2: discard the $k(< N)$ largest values of

$$\hat{\gamma}^{(i)} := d_T(y_{\mathcal{S}}^{(i)}, y_{\mathcal{M}}^{(i)}),\ i = 1, 2, \ldots, N;$$

3: set

$$\hat{\gamma}_\epsilon := \max_{i \in \{1,2,\ldots,N\} \setminus \{h_1, h_2, \ldots h_k\}} \hat{\gamma}^{(i)},$$

where $\{h_1, h_2, \ldots h_k\} \subset \{1, 2, \ldots, N\}$ denote the indices of the discarded values of the $\hat{\gamma}^{(i)}$'s.

By extracting at random N possible executions of $\mathcal{M}$ and $\mathcal{S}$ and a-posteriori discarding the fraction $k/N(< \epsilon)$ that corresponds to the largest discrepancy between them, one can improve the quality bound γ while guaranteeing that the violation set has size smaller than or equal to the prescribed ϵ value. This intuition can be posed on solid theoretical grounds and the following result on the quality of the estimate $\hat{\gamma}_\epsilon$ can be proven by a straightforward application of [7, Theorem 2].

Proposition 2: Select a confidence parameter $\beta \in (0, 1)$ and a performance degradation parameter $\nu \in (0, \epsilon)$. If N and k are such that

$$\sum_{i=0}^{k} \binom{N}{i} \epsilon^i (1-\epsilon)^{N-i} + \sum_{i=k+1}^{N} \binom{N}{i} (\epsilon - \nu)^i (1 - \epsilon + \nu)^{N-i} \leq \beta, \qquad (6)$$

then, with probability at least $1-\beta$, the solution $\hat{\gamma}_\epsilon$ to Algorithm 1 satisfies the following feasibility and optimality conditions:

1) $P\big(d_T(y_{\mathcal{S}}, y_{\mathcal{M}}) \leq \hat{\gamma}_\epsilon\big) \geq 1 - \epsilon$,
2) $\gamma_\epsilon \leq \hat{\gamma}_\epsilon \leq \gamma_{\epsilon-\nu}$,

where $\gamma_{\epsilon-\nu}$ denotes the optimal chance-constrained solution when the size of the violation set is $\epsilon - \nu$. □

If we discard the confidence parameter β for a moment, this proposition states that the randomized solution $\hat{\gamma}_\epsilon$ obtained through Algorithm 1 is feasible for the chance-constrained program (5) (condition 1) and is at least as good as the chance-constrained solution when the size of violation set is reduced to $\epsilon - \nu$ (condition 2). As ν tends to zero, $\hat{\gamma}_\epsilon$ approaches the desired optimal chance constrained solution γ_ϵ. In turn, the simulation effort grows unbounded since N and k depends on $1/\nu$ [7].

As for the confidence parameter β, one should note that $\hat{\gamma}_\epsilon$ is a random quantity that depends on the randomly extracted input realizations and initial conditions. It may happen that the extracted samples are not representative enough, in which case the size of the violation set will be larger than ϵ. Parameter β controls the probability that this happens and the final result holds with probability $1-\beta$. N and k satisfying (6) depend logarithmically on $1/\beta$ [7], so that β can be pushed down to small values such as 10^{-10}, to make $1-\beta$ be so close to 1 to lose any practical importance.

IV. Design of an approximate abstraction

Suppose that one has to select the best approximate abstraction of $\mathcal{S}$ up to level $1-\epsilon$ in a given class $\mathcal{C}$. This design problem can be formulated as the following chance-constrained program:

$$\min_{\gamma \in \Re,\ \mathcal{M} \in \mathcal{C}} \gamma \quad \text{subject to:} \quad P\big(d_T(y_{\mathcal{S}}, y_{\mathcal{M}}) \leq \gamma\big) \geq 1 - \epsilon, \qquad (7)$$

which is even more challenging to solve than (5) since the optimization variables are now $\mathcal{M}$ and γ. Let us denote with $\gamma_\epsilon^\star$ and $\mathcal{M}_\epsilon^\star$ the solution to (7). We distinguish between two different cases.

A. Case 1: The model class is finite

If the family $\mathcal{C}$ is finite, i.e., $\mathcal{C} = \{\mathcal{M}_j : j = 1, 2, \ldots, m\}$, one can resort to Algorithm 2, for which Proposition 3 holds.

Proposition 3: Select a confidence parameter $\beta \in (0, 1)$ and a performance degradation parameter $\nu \in (0, \epsilon)$. If N and k satisfy (6), then, with probability at least $1 - m\beta$, the quality estimate $\hat{\gamma}_\epsilon^\star$ of $\hat{\mathcal{M}}_\epsilon^\star$ obtained through Algorithm 2 satisfies both the conditions:

1) $\max_{\mathcal{M} \in \mathcal{C}} P\big(d_T(y_{\mathcal{S}}, y_{\mathcal{M}}) \leq \hat{\gamma}_\epsilon^\star\big) \geq 1 - \epsilon$,
2) $\gamma_{\epsilon, j^\star} \leq \hat{\gamma}_\epsilon^\star \leq \gamma_{\epsilon-\nu, j^\star}$,

where $\gamma_{\alpha,j}$ denotes the solution to the optimal chance-constrained program (5) for model $\mathcal{M}_j$ when the size of the violation set is α. □

According to condition 1) in Proposition 3, the approximation quality $\hat{\gamma}_\epsilon^\star$ is guaranteed with level $1-\epsilon$ within the model family $\mathcal{C}$. This result holds with a confidence parameter value that is deteriorated of a factor m (the cardinality of $\mathcal{C}$) with respect to β.

B. Case 2: The model class is finitely parameterized

Suppose that one has to choose the best approximate abstraction of $\mathcal{S}$ up to level $1-\epsilon$ within some finitely

Algorithm 2 Randomized solution to model selection

1: extract N realizations of the stochastic input $w^{(i)}(t)$, $t \in T$, $i = 1, 2, \ldots, N$, and N samples of the initial condition $(x_{\mathcal{S}}(0), x_{\mathcal{M}}(0))^{(i)}$, $i = 1, 2, \ldots, N$;
2: run the corresponding N executions of $\mathcal{S}$, thus obtaining N realizations of the output signal $y_{\mathcal{S}}^{(i)}(t)$, $t \in T$, $i = 1, 2, \ldots, N$;
3: for each model $\mathcal{M}_j$, $j = 1, 2, \ldots, m$ do the following:
- run the N executions of $\mathcal{M}_j$, thus obtaining N realizations of the output signal $y_{\mathcal{M}_j}^{(i)}(t)$, $t \in T$, $i = 1, 2, \ldots, N$;
- discard the $k(< N)$ largest values of

$$\hat{\gamma}_j^{(i)} := d_T(y_{\mathcal{S}}^{(i)}, y_{\mathcal{M}_j}^{(i)}),\ i = 1, 2, \ldots, N;$$

- set

$$\hat{\gamma}_j := \max_{i \in \{1,2,\ldots,N\} \setminus \{h_1, h_2, \ldots, h_k\}} \hat{\gamma}_j^{(i)},$$

where $\{h_1, h_2, \ldots h_k\} \subset \{1, 2, \ldots, N\}$ denote the indices of the discarded values of the $\hat{\gamma}_j^{(i)}$'s.

4: set $\hat{\mathcal{M}}_\epsilon^\star = \mathcal{M}_{j^\star}$ and $\hat{\gamma}_\epsilon^\star = \hat{\gamma}_{j^\star}$, where $j^\star := \arg\min_{j=1,2,\ldots,m} \hat{\gamma}_j$.

parameterized model class $\{\mathcal{M}(\theta), \theta \in \Theta \subseteq \Re^d\}$. Then, the chance-constrained program (7) can be rewritten as

$$\min_{\gamma \in \Re,\, \theta \in \Theta} \gamma \quad \text{subject to:} \qquad (8)$$
$$P\big(d_T(y_{\mathcal{S}}, y_{\mathcal{M}(\theta)}) \le \gamma\big) \ge 1 - \epsilon,$$

and a randomized solution to (8) can be found through Algorithm 3.

Algorithm 3 Randomized design of an abstraction

1: extract N realizations of the stochastic input $w^{(i)}(t)$, $t \in T$, $i = 1, 2, \ldots, N$, and N samples of the initial condition $(x_{\mathcal{S}}(0), x_{\mathcal{M}}(0))^{(i)}$, $i = 1, 2, \ldots, N$;
2: run the corresponding N executions of $\mathcal{S}$ and $\mathcal{M}$, thus obtaining N realizations of the output signals $y_{\mathcal{S}}^{(i)}(t)$ and $y_{\mathcal{M}}^{(i)}(t)$, $t \in T$, $i = 1, 2, \ldots, N$;
3: select the $k(< N)$ executions to discard such that the value for γ obtained through

$$\min_{\gamma \in \Re,\, \theta \in \Theta} \gamma \quad \text{subject to:} \qquad (9)$$
$$d_T(y_{\mathcal{S}}^{(i)}, y_{\mathcal{M}(\theta)}^{(i)}) \le \gamma, i \in \{1, \ldots, N\} \setminus \{h_1, h_2, \ldots h_k\}$$

is minimal;
4: let $\hat{\gamma}_\epsilon, \hat{\theta}_\epsilon$ be the solution to (9) with $\{h_1, h_2, \ldots h_k\}$ denoting the indices of the executions to be discarded.

If $d_T(y_{\mathcal{S}}, y_{\mathcal{M}(\theta)})$ is convex as a function of θ and Θ is a closed and convex set, then, by [7, Theorem 2] the following result holds.

Proposition 4: Select a confidence parameter $\beta \in (0, 1)$ and a performance degradation parameter $\nu \in (0, \epsilon)$. If N and k are such that

$$\binom{k+d}{k} \sum_{i=0}^{k+d} \binom{N}{i} \epsilon^i (1-\epsilon)^{N-i} + \sum_{i=k+1}^{N} \binom{N}{i} (\epsilon - \nu)^i (1 - \epsilon + \nu)^{N-i} \le \beta, \qquad (10)$$

where d is the dimension of the optimization parameter θ, then, with probability at least $1-\beta$, the solution $\hat{\gamma}_\epsilon, \hat{\theta}_\epsilon$ to Algorithm 3 satisfies the feasibility and optimality conditions:
1) $P\big(d_T(y_{\mathcal{S}}, y_{\mathcal{M}(\hat{\theta}_\epsilon)}) \le \hat{\gamma}_\epsilon\big) \ge 1 - \epsilon$,
2) $\gamma_\epsilon \le \hat{\gamma}_\epsilon \le \gamma_{\epsilon-\nu}$. □

The optimal removal procedure involved in the third step of Algorithm 3 requires to solve $\binom{N}{k}$ finite convex optimization problems, which makes the problem computationally unfeasible for sensible values of ϵ and β. However, if one resorts to a suboptimal removal procedure (e.g. a greedy approach where the k executions to be discarded are chosen one after the other by progressively improving the solution γ instead of all k executions in a single shot), the feasibility condition 1 in Proposition 4 still holds. Moreover, the bound

$$\binom{k+d}{k} \sum_{i=0}^{k+d} \binom{N}{i} \epsilon^i (1-\epsilon)^{N-i} \le \beta$$

can be used in place of (10), with a significant reduction of the values for N and k (see [7, Theorem 1]).

Remark 3: Note that Proposition 4 requires the distance between executions to be convex as a function of the candidate abstracted model parametrization. This can be enforced by adopting a convex over-approximation, at the price of introducing conservativeness in the optimality of the randomized solution. □

V. A NUMERICAL EXAMPLE

We test the randomized approach proposed in this paper on a numerical example inspired by that reported in [12].

Let $\mathcal{S}$ be a stochastic system whose state $x(t) \in \Re^6$ evolves according to a stochastic differential equation (SDE) and, from time to time, is subject to some deterministic reset. More precisely, $x(t)$ is governed by

$$dx(t) = Ax(t)dt + \Sigma\, x(t) dB(t),$$

where $B(t)$ is a standard Brownian motion, $A = \text{diag}(a_1, a_2, a_3)$ is a block-diagonal matrix with

$$a_1 = \begin{bmatrix} -1 & -10 \\ 10 & -1 \end{bmatrix}, a_2 = \begin{bmatrix} -2 & -20 \\ 20 & -1 \end{bmatrix}, a_3 = \begin{bmatrix} -2 & 0 \\ 0 & -2.5 \end{bmatrix},$$

and

$$\Sigma = 0.5 \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

At the jump times $\{t_n\}_{n \ge 0}$, the continuous state $x(t)$ is reset to $x(t_n) = R \lim_{t \uparrow t_n} x(t)$, where $R = 0.7 \cdot I_{6 \times 6}$.

The jump times are determined by a Poisson process $p(t)$ with rate $\lambda = 0.5$ that is independent of the Brownian motion $B(t)$. The initial condition $x(0)$ of $\mathcal{S}$ is a Gaussian random variable with mean $\mu = [1\,1\,1\,1\,0\,0]'$ and variance

$$V = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.01 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.01 \end{bmatrix},$$

that is independent of the stochastic input to the system $w(t) := (B(t), p(t))$. The output of the system is given by

$$y_{\mathcal{S}}(t) = Cx(t),$$

where

$$C = \begin{bmatrix} 0.84 & -1.03 & 1.07 & -0.88 & 0.5 & 0 \\ -0.60 & -1.35 & -0.26 & -0.27 & 0 & -0.5 \end{bmatrix}.$$

We next consider 3 different models, and apply Algorithm 1 to assess their quality as an approximate abstraction of $\mathcal{S}$ over T up to level $1-\epsilon$, with $T = [0, 6]$ and $\epsilon = 0.1$. A step $\Delta t = 6 \cdot 10^{-3}$ was used for the numerical integration (first-order Euler-Maruyama scheme) of the involved SDEs. Algorithm 2 allows assessing the overall outcome.

The results reported refer to the case when the confidence parameter and the performance degradation parameter are set equal to $\beta = 10^{-6}$ and $\nu = 0.05$ respectively, corresponding to $N = 2573$ and $k = 186$ based on the bound (6) in Proposition 2. Since $\beta = 10^{-6}$, the results obtained through Algorithm 1 hold with probability at least $1 - 10^{-6}$.

A. Description of the candidate models

Model $\mathcal{M}_1$ is characterized by a lower-dimensional state $x_1(t)$ governed by the SDE

$$dx_1(t) = A_1 x_1(t)dt + \Sigma_1\, x_1(t)dB(t),$$

where $A_1 = \text{diag}(a_1, a_2)$ and $\Sigma_1 = 0.5 \cdot I_4$, with I_4 denoting the identity matrix of dimension 4. The discrete transitions are determined by the Poisson process $p(t)$, and the reset matrix of state $x_1(t)$ is $R_1 = 0.7 \cdot I_4$. The output of $\mathcal{M}_1$ is $y_{\mathcal{M}_1}(t) = C_1 x_1(t)$, where

$$C_1 = \begin{bmatrix} 0.84 & -1.03 & 1.07 & -0.88 \\ -0.60 & -1.35 & -0.26 & -0.27 \end{bmatrix}.$$

Model $\mathcal{M}_1$ is initialized by setting $x_1(0)$ equal to the first four components of $x(0)$.

Model $\mathcal{M}_2$ is identical to system $\mathcal{S}$ except for matrix Σ that is set equal to zero so as to exclude the influence of the Brownian motion: $dx_2(t) = Ax_2(t)dt$. The discrete transitions are determined by the Poisson process $p(t)$ of rate $\lambda = 0.5$ and the reset matrix of state $x_2(t)$ is R. The output of $\mathcal{M}_2$ is given by $y_{\mathcal{M}_2}(t) = Cx_2(t)$. Model $\mathcal{M}_2$ is initialized at $x_2(0) = x(0)$.

Model $\mathcal{M}_3$ is a stochastic system described by:

$$\begin{cases} dx_3(t) = Ax_3(t)dt + \Sigma x_3(t)dB(t) \\ y_{\mathcal{M}_3}(t) = Cx_3(t), \end{cases}$$

with no jumps, and is initialized at $x_3(0) = x(0)$.

B. Results obtained with $d_T(y_{\mathcal{S}}, y_{\mathcal{M}})$ given by (2)

As for model $\mathcal{M}_1$, the outcome of Algorithm 1 was $\hat{\gamma}_\epsilon = 1.21$, hence, by Proposition 2, we can state that

$$P(\sup_{t\in[0,6]} \|y_{\mathcal{S}}(t) - y_{\mathcal{M}_1}(t)\| \le 1.21) \ge 0.90.$$

In Figure 2, we report a realization of the output signals $y_{\mathcal{S}}(t)$ (solid line) and $y_{\mathcal{M}_1}(t)$ (dashed line) over the time horizon $[0, 6]$ and the corresponding distance $\|y_{\mathcal{S}}(t) - y_{\mathcal{M}_1}(t)\|$. The values of $\sup_{t\in[0,6]} \|y_{\mathcal{S}}(t) - y_{\mathcal{M}_1}(t)\|$ obtained in 1000 experiments are drawn and compared with the threshold 1.21. Since 938 out of 1000 values were found to be smaller than or equal to 1.21, then, $1 - \hat{\epsilon} = 0.938$. This last finding agrees with condition 2 in Proposition 2 that $\hat{\gamma}_\epsilon = 1.21 \le \gamma_{\epsilon-\nu}$, since the estimated size of the violation set $\hat{\epsilon} = 0.062$ satisfies $\epsilon - \nu = 0.05 < \hat{\epsilon} < \epsilon = 0.10$.

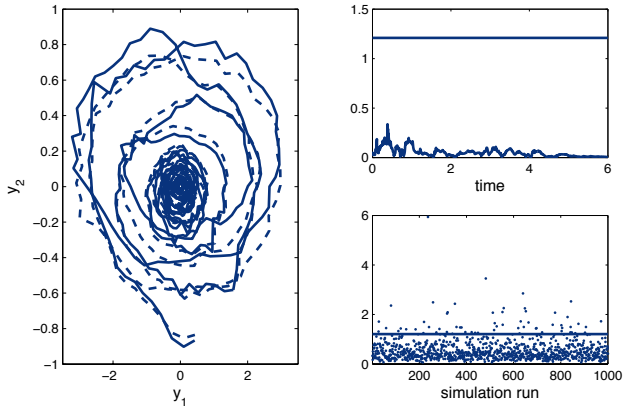

Fig. 2. Application of Algorithm 1 to model $\mathcal{M}_1$: phase plot of a realization of $y_{\mathcal{S}}(t)$ (solid line) and $y_{\mathcal{M}_1}(t)$ (dashed line) over the time horizon T (on the left) and corresponding realization of $\|y_{\mathcal{S}}(t) - y_{\mathcal{M}_1}(t)\|$ (top plot on the right); outcomes $d_T(y_{\mathcal{S}}, y_{\mathcal{M}_1})$ of 1000 Monte Carlo experiments to estimate the actual level $1 - \epsilon$ (bottom plot on the right).

As for model $\mathcal{M}_2$, the outcome of Algorithm 1 was $\hat{\gamma}_\epsilon = 4.14$, hence, by Proposition 2, we can state that

$$P(\sup_{t\in[0,6]} \|y_{\mathcal{S}}(t) - y_{\mathcal{M}_2}(t)\| \le 4.14) \ge 0.90.$$

In Figure 3, we report a realization of the output signals $y_{\mathcal{S}}(t)$ (solid line) and $y_{\mathcal{M}_2}(t)$ (dashed line) over the time horizon $[0, 6]$ and the corresponding distance $\|y_{\mathcal{S}}(t) - y_{\mathcal{M}_2}(t)\|$. The values of $\sup_{t\in[0,6]} \|y_{\mathcal{S}}(t) - y_{\mathcal{M}_2}(t)\|$ obtained in 1000 experiments are drawn and compared with the threshold 4.14. In this case, 932 out of 1000 values were smaller than or equal to 4.14, which corresponds to an estimated level $1 - \hat{\epsilon} = 0.932$. Thus, $\hat{\epsilon} = 0.68$ satisfies $\epsilon - \nu < \hat{\epsilon} < \epsilon$.

As for $\mathcal{M}_3$, we obtained

$$P(\sup_{t\in[0,6]} \|y_{\mathcal{S}}(t) - y_{\mathcal{M}_3}(t)\| \le 2.74) \ge 0.90.$$

In Figure 4, we report a realization of the output signals $y_{\mathcal{S}}(t)$ (solid line) and $y_{\mathcal{M}_3}(t)$ (dashed line) over the time horizon $[0, 6]$ and the corresponding distance $\|y_{\mathcal{S}}(t) -$

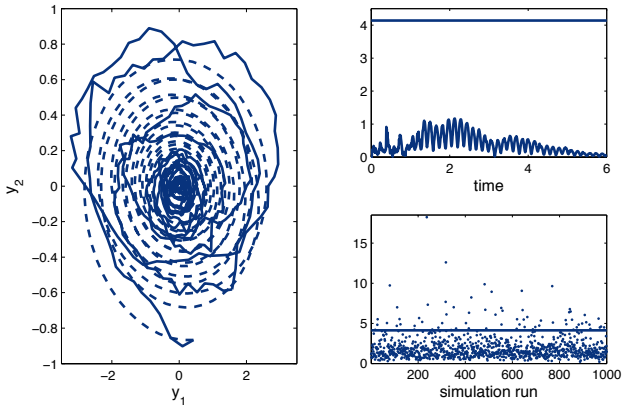

Fig. 3. Application of Algorithm 1 to model $\mathcal{M}_2$: phase plot of a realization of $y_{\mathcal{S}}(t)$ (solid line) and $y_{\mathcal{M}_2}(t)$ (dashed line) over the time horizon T (on the left) and corresponding realization of $\|y_{\mathcal{S}}(t) - y_{\mathcal{M}_2}(t)\|$ (top plot on the right); outcomes $d_T(y_{\mathcal{S}}, y_{\mathcal{M}_2})$ of 1000 Monte Carlo experiments to estimate the actual level $1-\epsilon$ (bottom plot on the right).

$y_{\mathcal{M}_3}(t)\|$. The values of $\sup_{t\in[0,6]} \|y_{\mathcal{S}}(t) - y_{\mathcal{M}_3}(t)\|$ obtained in 1000 experiments are drawn and compared with the threshold 2.74. It was found that 926 out of 1000 values were smaller than or equal to 2.74, hence, the estimated level is $1-\hat{\epsilon} = 0.926$ and $\hat{\epsilon} = 0.074$ satisfies $\epsilon - \nu < \hat{\epsilon} < \epsilon$.

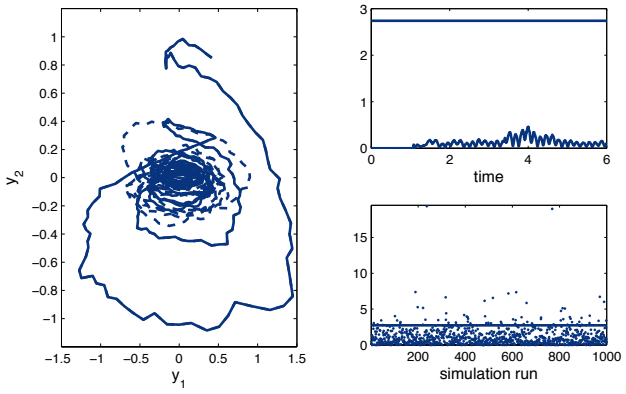

Fig. 4. Application of Algorithm 1 to model $\mathcal{M}_3$: phase plot of a realization of $y_{\mathcal{S}}(t)$ (solid line) and $y_{\mathcal{M}_3}(t)$ (dashed line) over the time horizon T (on the left) and corresponding realization of $\|y_{\mathcal{S}}(t) - y_{\mathcal{M}_3}(t)\|$ (top plot on the right); outcomes $d_T(y_{\mathcal{S}}, y_{\mathcal{M}_3})$ of 1000 Monte Carlo experiments to estimate the actual level $1-\epsilon$ (bottom plot on the right).

C. Results obtained with $d_T(y_{\mathcal{S}}, y_{\mathcal{M}})$ given by (3)

The result of Algorithm 1 for $\mathcal{M}_1$ was $\hat{\gamma}_\epsilon = 0.93$, hence

$$P(\sup_{t\in[0,6]} \inf_{\tau\in[0,6]} \|y_{\mathcal{S}}(t) - y_{\mathcal{M}_1}(\tau)\| \leq 0.93) \geq 0.90.$$

The level associated with $\hat{\gamma}_\epsilon = 0.93$ was estimated through 1000 Monte Carlo experiments and was found to be $1 - \hat{\epsilon} = 0.932$. The estimates of the quality of $\mathcal{M}_2$ and $\mathcal{M}_3$ obtained by Algorithm 1 were 3.03 and 0.87, respectively, which entails that

$$P(\sup_{t\in[0,6]} \inf_{\tau\in[0,6]} \|y_{\mathcal{S}}(t) - y_{\mathcal{M}_2}(\tau)\| \leq 3.03) \geq 0.90,$$
$$P(\sup_{t\in[0,6]} \inf_{\tau\in[0,6]} \|y_{\mathcal{S}}(t) - y_{\mathcal{M}_3}(\tau)\| \leq 0.87) \geq 0.90.$$

The estimated levels $1-\hat{\epsilon}$ were respectively 0.929 and 0.909.

D. Selection of the best approximate model

As expected, the approximation quality γ_ϵ of any model $\mathcal{M}_j$ is better (lower) when evaluated based on (3) than on (2). In particular, the improvement is significant in the case of model $\mathcal{M}_3$, where the state jumps are neglected.

By Proposition 3, we can state with a confidence at least equal to $1-3\beta = 1-3\cdot 10^{-6}$ that the model that guarantees the best quality (2) as an approximate abstraction of $\mathcal{S}$ is $\mathcal{M}_1$. As for the best approximate abstraction according to (3), models $\mathcal{M}_1$ and $\mathcal{M}_3$ are comparable.

ACKNOWLEDGMENTS

The authors would like to thank Dr. Agung Julius for providing better insight into the results in [12].

REFERENCES

[1] A. Abate. A contractivity approach for probabilistic bisimulations of diffusion processes. In *Proceedings of the 48th IEEE Conference of Decision and Control*, pages 2230–2235, Shanghai, PRC, Dec. 2009.

[2] R. Alur, T. Henzinger, G. Lafferriere, and G. Pappas. Discrete abstractions of hybrid systems. *Proceedings of the IEEE*, 88(2):971–984, July 2000.

[3] C. Baier and J.-P. Katoen. *Principles of Model Checking*. The MIT Press, 2008.

[4] M.L. Bujorianu and J. Lygeros. Reachability questions in piecewise deterministic Markov processes. In *Hybrid Systems: Computation and Control (HSCC)*, volume 2623 of *Lecture Notes in Computer Science LNCS*, pages 126–140. Springer, 2003.

[5] M.L. Bujorianu, J. Lygeros, and M.C. Bujorianu. Bisimulation for general stochastic hybrid systems. In *Hybrid Systems: Computation and Control (HSCC)*, pages 198–214. Springer-Verlag, 2005.

[6] G. Calafiore and M.C. Campi. Uncertain convex programs: randomized solutions and confidence levels. *Mathematical Programming*, 102(1):25–46, 2005.

[7] M.C. Campi and S. Garatti. A sampling-and-discarding approach to chance-constrained optimization: feasibility and optimality. *Journal of Optimization Theory and Applications*, 148(2):257–280, 2011.

[8] M.C. Campi, S. Garatti, and M. Prandini. The scenario approach for systems and control design. *Annual Reviews in Control*, 33(2):149–157, 2009.

[9] J. Desharnais, A. Edalat, and P. Panangaden. Bisimulation for labeled Markov processes. *Information and Computation*, 179(2):163–193, 2002.

[10] A. Girard and G.J. Pappas. Approximation metrics for discrete and continuous systems. *IEEE Trans. on Automatic Control*, 52(5):782–798, 2007.

[11] A. Girard, G. Pola, and P. Tabuada. Approximately bisimilar symbolic models for incrementally stable switched systems. *IEEE Transactions on Automatic Control*, 55(1):116–126, Jan 2010.

[12] A.A. Julius and G.J. Pappas. Approximate abstraction of stochastic hybrid systems. *IEEE Trans. Automatic Control*, 54(6):1193–1203, 2009.

[13] K.G. Larsen and A. Skou. Bisimulation through probabilistic testing. *Information and Computation*, 94:1–28, 1991.

[14] G. Pola, A. Girard, and P. Tabuada. Approximately bisimilar symbolic models for nonlinear control systems. *Automatica*, 44(10):2508–2516, October 2008.

[15] S. Strubbe and A. Van Der Schaft. Bisimulation for communicating piecewise deterministic Markov processes (CPDPs). In *Hybrid Systems: Computation and Control (HSCC)*, pages 623–639. Springer-Verlag, 2005.