Similarity quantification for linear stochastic systems

Automatica 144 (2022) 110476

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Brief paper

Similarity quantification for linear stochastic systems: A coupling compensator approach☆

Birgit C. van Huijgevoort *, Sofie Haesaert

Electrical Engineering Department, Eindhoven University of Technology, The Netherlands

ARTICLE INFO

Article history:
Received 17 July 2020
Received in revised form 15 January 2022
Accepted 31 May 2022
Available online xxxx

Keywords:
Control synthesis
Approximate simulation relations
Stochastic systems
Temporal logic

ABSTRACT

For the formal verification and design of control systems, abstractions with quantified accuracy are crucial. This is especially the case when considering accurate deviation bounds between a stochastic continuous-state model and its finite (reduced-order) abstraction. In this work, we introduce a coupling compensator to parameterize the set of relevant couplings and we give a comprehensive computational approach and analysis for linear stochastic systems. More precisely, we develop a computational method that characterizes the set of possible simulation relations and gives a trade-off between the error contributions on the systems output and deviations in the transition probability. We show the effect of this error trade-off on the guaranteed satisfaction probability for case studies where a formal specification is given as a temporal logic formula.

1. Introduction

Airplanes, cars, and power systems are examples of safety-critical control systems, whose reliable and autonomous functioning is critical. It is of interest to design controllers for these systems that provably satisfy formal specifications such as linear temporal logic (LTL) formulae (Pnueli, 1977). These formal specifications have to be verified probabilistically for systems described by stochastic discrete-time models. Despite recent advances (Cauchi & Abate, 2019; Desharnais, Gupta, Jagadeesan, & Panangaden, 2003; Haesaert & Soudjani, 2020; Haesaert, Soudjani and Abate, 2017; Julius & Pappas, 2009; Lavaei, Khaled, Soudjani, & Zamani, 2020; Lavaei, Soudjani, & Zamani, 2019, 2021; Soudjani, Gevaerts, & Abate, 2015; Zamani, Esfahani, Majumdar, Abate, & Lygeros, 2014), the provably correct design of controllers for such stochastic models with continuous state spaces remains a challenging problem. Many of those methods (Cauchi & Abate, 2019; Haesaert & Soudjani, 2020; Haesaert, Soudjani et al., 2017; Lavaei et al., 2020; Soudjani et al., 2015; Zamani et al., 2014) rely on constructing a stochastic finite-state model or abstraction that approximates the original model. These methods are often more suitable for complex temporal logic specifications, but their application to real-world problems tends to suffer from scalability issues and conservative lower bounds on the satisfaction probability.

A key factor in the conservatism is the quantification of the similarity between the original and abstract model for which approximate simulation relations (Desharnais et al., 2003; Haesaert & Soudjani, 2020; Haesaert, Soudjani et al., 2017; Zamani et al., 2014) and stochastic simulation functions (Julius & Pappas, 2009; Lavaei et al., 2019) can be used. These methods inherently build on an implicit coupling of probabilistic transitions (Segala & Lynch, 1994; Tkachev & Abate, 2014). The latter shows that the coupling between stochastic processes is crucial, and omitting its explicit choice may lead to conservative results. Hence, we investigate the explicit design of the coupling to find efficient approximate stochastic simulation relations.

Besides abstraction-based methods that leverage finite-state approximations, discretization-free methods also exist. Next to methods that target specific model classes and limited reach-(avoid) specifications (Kariotoglou, Kamgarpour, Summers, & Lygeros, 2017; Vinod, Gleason, & Oishi, 2019), recent results based on barrier certificates (Huang, Chen, Lin, Yang, & Li, 2017; Jagtap, Soudjani, & Zamani, 2020) are able to handle larger sets of specifications. Even though these methods suffer less from the curse of dimensionality, they are often restricted to specific model structures or specifications. For example the barrier certificates in Jagtap et al. (2020) only work for LTL specifications on finite traces. Furthermore, it is not known whether a solution can be found even if one exists and the computational complexity grows substantially with the length and complexity of the specification.

On the other hand, discretization-based methods are very common in the provably correct design of controllers (Cauchi

☆ The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Maria Prandini under the direction of Editor Sophie Tarbouriech.

* Corresponding author.
E-mail addresses: b.c.v.huijgevoort@tue.nl (B.C. van Huijgevoort), s.haesaert@tue.nl (S. Haesaert).

https://doi.org/10.1016/j.automatica.2022.110476

& Abate, 2019; Haesaert & Soudjani, 2020; Haesaert, Soudjani et al., 2017; Lavaei et al., 2020; Soudjani et al., 2015; Zamani et al., 2014) and they can in general handle more challenging specifications. In Lavaei et al. (2021), it has been shown that (ϵ, δ)-stochastic simulation relations (Haesaert & Soudjani, 2020; Haesaert, Soudjani et al., 2017) that quantify both the probabilistic deviation and the deviation in (output) trajectories can be used for compositional verification of large scale stochastic systems with nonlinear dynamics and that this outperforms results that leverage simulation functions. Therefore, we focus on the design of efficient (ϵ, δ)-stochastic simulation relations via tailored coupling designs. Moreover, we will show that this allows us to characterize the set of coupling simulations and to trade off the error contributions of the systems output with deviations in the transition probability.

This work introduces a coupling compensator, to leverage the freedom in coupling-based similarity relations, such as Haesaert, Soudjani et al. (2017), via computationally attractive set-theoretic methods. To achieve this, we exploit the use of coupling probability measures through a coupling compensator (Section 3). In Section 4, we develop a method to efficiently compute the deviation bounds for finite-state abstractions by formulating it as a set-theoretic problem using the concept of controlled-invariant sets. Similarly, in Section 5, we apply the coupling compensator to reduced-order models. We limit our comprehensive analysis and computational approach to linear stochastic systems, however, the application of the coupling compensator is not restricted to linear systems nor to approximate simulation relations. To evaluate the benefits of this method, we consider specifications written using syntactically co-safe linear temporal logic (Belta, Yordanov, & Gol, 2017; Kupferman & Vardi, 2001), and analyze the influence of both the deviation bounds on the satisfaction probability (Section 6).

2. Preliminaries

We denote the set of positive real numbers by $\mathbb{R}^+$ and the n-dimensional identity matrix by I_n. We limit us to spaces that are finite, Euclidean or Polish. Furthermore, we denote a Borel measurable space as $(\mathbb{X}, \mathcal{B}(\mathbb{X}))$ where $\mathbb{X}$ is an arbitrary set and $\mathcal{B}(\mathbb{X})$ are the Borel sets. A probability measure $\mathbb{P}$ over this space has realizations $x \sim \mathbb{P}$, with $x \in \mathbb{X}$. Denote the set of probability measures on the measurable space $(\mathbb{X}, \mathcal{B}(\mathbb{X}))$ as $\mathcal{P}(\mathbb{X})$.

Model. We consider systems whose behavior is modeled by a stochastic difference equation

$$M : \begin{cases} x(t+1) &= f(x(t), u(t), w(t)) \\ y(t) &= h(x(t)), \quad \forall t \in \{0, 1, 2, \dots\}, \end{cases} \tag{1}$$

initialized with $x(0) = x_0$ and with state $x \in \mathbb{X}$, input $u \in \mathbb{U}$, disturbance $w \in \mathbb{W}$, and output $y \in \mathbb{Y}$. We assume that the functions $f : \mathbb{X} \times \mathbb{U} \times \mathbb{W} \to \mathbb{X}$ and $h : \mathbb{X} \to \mathbb{Y}$ are Borel measurable. Furthermore, $w(t)$ is an independently and identically distributed (i.i.d.) noise signal with realizations $w(t) \sim \mathbb{P}_w$. A (finite) path $\boldsymbol{\omega}_{\to t} := x_0, u_0, x_1, u_1, \dots, x_t$ of M consists of states x_k and inputs u_k, for which $x_{k+1} = x(k+1)$ follow (1) for a given state $x(k) = x_k$, input $u(k) = u_k$ and disturbance $w(k)$ at time steps k. A control strategy $\boldsymbol{\mu} := \mu_0, \mu_1, \mu_2 \dots$ consists of maps $\mu_t(\boldsymbol{\omega}_{\to t}) \in \mathbb{U}$ assigning an input $u(t)$ to each finite path $\boldsymbol{\omega}_{\to t}$ generated by the model (1). In this work, we consider control strategies, denoted as C represented with finite memory and we denote the controlled system with $M \times C$.

Specifications. Consider specifications written using syntactically co-safe linear temporal logic (scLTL) (Belta et al., 2017; Kupferman & Vardi, 2001) a subset of LTL (Pnueli, 1977). Denote with $\mathrm{AP} = \{p_1, \dots, p_N\}$ the set of atomic propositions, and let 2^{AP} be the alphabet with letters $\pi \in 2^{\mathrm{AP}}$. An infinite string of letters is a word $\boldsymbol{\pi} = \pi_0\pi_1\pi_2\dots$ with associated suffix $\boldsymbol{\pi}_t = \pi_t\pi_{t+1}\pi_{t+2}\dots$. An scLTL formula ϕ is defined as

$$\phi ::= p|\neg p|\phi_1 \wedge \phi_2|\phi_1 \vee \phi_2| \bigcirc \phi|\phi_1 \cup \phi_2,$$

with $p \in AP$. The semantics of scLTL is defined for the suffices $\boldsymbol{\pi}_t$ as follows. An atomic proposition $\boldsymbol{\pi}_t \models p$ holds if $p \in \pi_t$, while a negation $\boldsymbol{\pi}_t \models \neg p$ holds if $\boldsymbol{\pi}_t \not\models p$. A conjunction $\boldsymbol{\pi}_t \models \phi_1 \wedge \phi_2$ holds if both $\boldsymbol{\pi}_t \models \phi_1$ and $\boldsymbol{\pi}_t \models \phi_2$ hold. A disjunction $\boldsymbol{\pi}_t \models \phi_1 \vee \phi_2$ holds if either $\boldsymbol{\pi}_t \models \phi_1$ or $\boldsymbol{\pi}_t \models \phi_2$ holds. A next operator $\boldsymbol{\pi}_t \models \bigcirc\phi$ holds if $\boldsymbol{\pi}_{t+1} \models \phi$ is true. An until operator $\boldsymbol{\pi}_t \models \phi_1 \cup \phi_2$ holds if there exists an $i \in \mathbb{N}$ such that $\boldsymbol{\pi}_{t+i} \models \phi_2$ and for all $j \in \mathbb{N}, 0 \le j < i$ we have $\boldsymbol{\pi}_{t+j} \models \phi_1$. By combining multiple operators, the *eventually* operator $\lozenge\phi := \mathrm{true} \cup \phi$ can also be defined. A labeling function $L : \mathbb{Y} \to 2^{AP}$ assigns letters $\pi = L(y)$ to outputs $y \in \mathbb{Y}$. A state trajectory $\mathbf{x} := x_0x_1x_2\dots$ satisfies a specification ϕ, written $\mathbf{x} \models \phi$, iff the generated word $\boldsymbol{\pi}$ satisfies ϕ at time 0, i.e., $\boldsymbol{\pi}_0 \models \phi$. The satisfaction probability of a specification is the probability that words generated by the controlled system $M \times C$ satisfy the specification ϕ, denoted as $\mathbb{P}(M \times C \models \phi)$.

3. Similarity quantification: Problem statement and approach

The design of controller C and its exact quantification $\mathbb{P}(M \times C \models \phi)$ is computationally hard for continuous-state stochastic models (Abate, Prandini, Lygeros, & Sastry, 2008). Therefore, the approximation and similarity quantification of continuous-state models is a basic step in the provably correct design of controllers. This section proposes an approach to efficiently solve the coupling problem. These definitions are not restricted to linear time-invariant systems, so we keep them general in this section.

Problem statement. Suppose that model M given in (1), has an abstraction written as

$$\hat{M} : \begin{cases} \hat{x}(t+1) &= \hat{f}(\hat{x}(t), \hat{u}(t), \hat{w}(t)), \\ \hat{y}(t) &= \hat{h}(\hat{x}(t)), \end{cases} \tag{2}$$

initialized with $\hat{x}(0) = \hat{x}_0$ and with functions $\hat{h} : \hat{\mathbb{X}} \to \mathbb{Y}$ and $\hat{f} : \hat{\mathbb{X}} \times \hat{\mathbb{U}} \times \mathbb{W} \to \hat{\mathbb{X}}$. Here, $\hat{\mathbb{X}}$ and $\hat{\mathbb{U}}$ can be finite and $\hat{w}(t)$ is an i.i.d. noise sequence with realizations $\mathbb{P}_{\hat{w}}$. Note also that we have $\hat{\mathbb{Y}} = \mathbb{Y}$.

We quantify the difference between the original model M and the abstract model $\hat{M}$ by bounding the difference between the outputs y and $\hat{y}$. For this we need to resolve the choice of inputs $u, \hat{u}$ and the stochastic disturbance. The former is often done by equating $u(t) = \hat{u}(t)$ and analyzing the worst case error. An interface function (Girard & Pappas, 2009) generalizes this by refining the control input $\hat{u}$ to u as a function of the current states

$$\mathcal{U}_v : \hat{\mathbb{U}} \times \hat{\mathbb{X}} \times \mathbb{X} \to \mathbb{U}. \tag{3}$$

In a similar way, we can resolve the stochastic disturbance. We first relate the probability measures $\mathbb{P}_{\hat{w}}$ and $\mathbb{P}_w$ of the stochastic disturbances $\hat{w}$ and w as follows.

Definition 1 (*Coupling of Probability Measures*). A coupling (den Hollander, 2012) of two probability measures $\mathbb{P}_{\hat{w}}$ and $\mathbb{P}_w$ on the same measurable space $(\mathbb{W}, \mathcal{B}(\mathbb{W}))$ is any probability measure $\mathcal{W}$ on the product measurable space $(\mathbb{W} \times \mathbb{W}, \mathcal{B}(\mathbb{W} \times \mathbb{W}))$ whose marginals are $\mathbb{P}_{\hat{w}}$ and $\mathbb{P}_w$, that is,[1]

$$\mathbb{P}_{\hat{w}} = \mathcal{W} \cdot \hat{\pi}^{-1}, \quad \mathbb{P}_w = \mathcal{W} \cdot \pi^{-1}, \tag{4}$$

[1] Requirement (4) on $\mathcal{W}$ can be equivalently given as
$\mathcal{W}(\hat{A} \times \mathbb{W}) = \mathbb{P}_{\hat{w}}(\hat{A})$ for all $\hat{A} \in \mathcal{B}(\mathbb{W})$
$\mathcal{W}(\mathbb{W} \times A) = \mathbb{P}_w(A)$ for all $A \in \mathcal{B}(\mathbb{W})$.
.

for which $\hat{\pi}$ and π are projections, respectively defined by

$$\hat{\pi}(\hat{w}, w) = \hat{w}, \quad \pi(\hat{w}, w) = w, \ \forall(\hat{w}, w) \in \mathbb{W} \times \mathbb{W}.$$

We can also design $\mathcal{W}$ as a measurable function of the current state pair and actions, similarly to the interface function. This yields a Borel measurable stochastic kernel associating to each $(u, \hat{x}, x)$ a probability measure

$$\mathcal{W} : \hat{\mathbb{U}} \times \hat{\mathbb{X}} \times \mathbb{X} \to \mathcal{P}(\mathbb{W}^2) \tag{5}$$

that couples probability measures $\mathbb{P}_{\hat{w}}$ and $\mathbb{P}_w$ as in Definition 1. We can now define a composed model as follows.

Definition 2 (*Composed Model*)**.** Given a coupling measure (5) and interface function (3) resolving the disturbances and inputs, respectively, the model $\hat{M} \parallel M$ composed of models $\hat{M}$ and M can be defined as

$$\begin{bmatrix}\hat{x}(t+1)\\ x(t+1)\end{bmatrix} = \begin{bmatrix}\hat{f}(\hat{x}(t), \hat{u}(t), \hat{w}(t))\\ f(x(t), \mathcal{U}_v(\hat{u}(t), \hat{x}(t), x(t)), w(t))\end{bmatrix}$$
$$\begin{bmatrix}\hat{y}(t)\\ y(t)\end{bmatrix} = \begin{bmatrix}\hat{h}(\hat{x}(t))\\ h(x(t))\end{bmatrix} \tag{6}$$

with states $(\hat{x}, x) \in \hat{\mathbb{X}} \times \mathbb{X}$, inputs $\hat{u} \in \hat{\mathbb{U}}$, coupled disturbances $(\hat{w}, w) \sim \mathcal{W}(\,\cdot\,|\hat{u}, \hat{x}, x)$ and outputs $\hat{y}, y \in \mathbb{Y}$.

The deviation between $\hat{M}$ and M can be expressed as the metric $\mathbf{d}_{\mathbb{Y}}(\hat{y}, y) := \|y - \hat{y}\|$, with $\hat{y}, y \in \mathbb{Y}$ for the traces of the composed model. Similar notions have been used in inter alia (Haesaert & Soudjani, 2020; Julius & Pappas, 2009; Zamani et al., 2014). Note that the choice of coupling is a critical part of this model composition. The problem can now be formulated as follows.

Problem 3. Explicitly design the coupling of probabilistic transitions to efficiently quantify the similarity between models $\hat{M}$ and M as in (1) and (2).

A coupling compensator approach. As in Haesaert, Soudjani et al. (2017), consider an approximate simulation relation to quantify the similarity between the stochastic models $\hat{M}$ and M. The following definition is a special case of Def. 9 in Haesaert, Soudjani et al. (2017) applicable to stochastic difference equations.

Definition 4 (*(ϵ, δ)-stochastic Simulation Relation*)**.** Let stochastic difference equations $\hat{M}$ and M with metric output space $(\mathbb{Y}, \mathbf{d}_{\mathbb{Y}})$ be composed into $\hat{M} \parallel M$ based on the interface function $\mathcal{U}_v$ (3) and the Borel measurable stochastic kernel $\mathcal{W}$ (5). If there exists a measurable relation $\mathcal{R} \subseteq \hat{\mathbb{X}} \times \mathbb{X}$, such that

(1) $(\hat{x}_0, x_0) \in \mathcal{R}$,
(2) $\forall(\hat{x}, x) \in \mathcal{R} : \mathbf{d}_{\mathbb{Y}}(\hat{y}, y) \le \epsilon$, and
(3) $\forall(\hat{x}, x) \in \mathcal{R}$, $\forall \hat{u} \in \hat{\mathbb{U}} : (\hat{x}^+, x^+) \in \mathcal{R}$ holds with probability at least $1 - \delta$,

then $\hat{M}$ is (ϵ, δ)-stochastically simulated by M, and this simulation relation is denoted as $\hat{M} \preceq_\epsilon^\delta M$.

Here, ϵ and δ denote the output and probability deviation respectively. Furthermore, state updates $\hat{x}^+$ and x^+ are the abbreviations of $\hat{x}(t+1)$ and $x(t+1)$. The choice of interface $\mathcal{U}_v$ impacts how much of the deviations between $x(t)$ and $\hat{x}(t)$ is compensated at the next time instance $x(t+1)$ and $\hat{x}(t+1)$. Similarly, the coupling $\mathcal{W}$ induces a term $w - \hat{w}$ that can compensate for state deviations. We can choose to explicitly parameterize the coupling based on this compensator term. To this end the notion of a coupling compensator is defined next.

Definition 5 (*Coupling Compensator*)**.** Consider probability measures $\mathbb{P}_{\hat{w}}$ and $\mathbb{P}_w$ on the same measurable space $(\mathbb{W}, \mathcal{B}(\mathbb{W}))$. Given a bounded set Γ and a probability $1 - \delta$, we say that $\mathcal{W}_\gamma$ is a coupling compensator if it parameterizes the coupling, such that for any compensator value $\gamma \in \Gamma$ we obtain the event $w - \hat{w} = \gamma$ with probability at least $1 - \delta$, that is, $\mathcal{W}_\gamma(w - \hat{w} = \gamma) \ge 1 - \delta$.

In the remainder of this paper, we resolve Problem 3 for (ϵ, δ)-simulation relations by either choosing the coupling compensator as a linear mapping of the state deviations when $\hat{\mathbb{X}} \subset \mathbb{X}$, that is, $\mathcal{W}(\cdot|\hat{u}, \hat{x}, x) = \mathcal{W}_\gamma$ with $\gamma = F(x - \hat{x})$ or as a linear mapping of the projected state deviation when $\hat{\mathbb{X}}$ and $\mathbb{X}$ are of a different dimension.

4. Coupling compensator for finite abstractions

Consider a linear time-invariant (LTI) system whose behavior is modeled by the stochastic difference equation

$$M : \begin{cases} x(t+1) &= Ax(t) + Bu(t) + B_w w(t) \\ y(t) &= Cx(t), \end{cases} \tag{7}$$

initialized with x_0 and with matrices $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, $B_w \in \mathbb{R}^{n\times d}$, $C \in \mathbb{R}^{m\times n}$, state $x \in \mathbb{X} \subset \mathbb{R}^n$, input $u \in \mathbb{U} \subset \mathbb{R}^m$ and output $y \in \mathbb{Y} \subset \mathbb{R}^m$. Furthermore, the stochastic disturbance $w \in \mathbb{W} \subseteq \mathbb{R}^d$ is an i.i.d Gaussian process. Without loss of generality, we assume that $w(t)$ has mean 0 and variance identity, that is, $w \sim \mathcal{N}(0, I)$. To leverage model checking results (Baier & Katoen, 2008) for finite-state Markov decision processes, we can abstract the model (7) to a finite-state representation.

Finite-state abstraction $\hat{M}$. To obtain a finite-state model $\hat{M}$, partition the state space $\mathbb{X}$ in a finite number of regions $\mathbb{A}_i \subset \mathbb{X}$, such that $\bigcup_i \mathbb{A}_i = \mathbb{X}$ and $\mathbb{A}_i \cap \mathbb{A}_j = \emptyset$ for $i \neq j$. Choose a representative point in each region, $\hat{X}_i \in \mathbb{A}_i$, and define the set of abstract states $\hat{x} \in \hat{\mathbb{X}}$ based on these representative points,[2] that is, $\hat{\mathbb{X}} := \{\hat{X}_1, \hat{X}_2, \hat{X}_3, \ldots, \hat{X}_\alpha\}$, where α is the (finite) number of regions. Furthermore, a finite set of inputs is selected from $\mathbb{U}$ and defines $\hat{\mathbb{U}}$. To define the dynamics of the abstract model, consider the operator $\Pi : \mathbb{X} \to \hat{\mathbb{X}}$ that maps states $x \in \mathbb{A}_i$ to their representative points $\hat{X}_i \in \mathbb{A}_i$. Using Π to obtain a finite-state abstraction of M, we get the abstract model $\hat{M}$

$$\hat{M} : \begin{cases} \hat{x}(t+1) &= \Pi(A\hat{x}(t) + B\hat{u}(t) + B_w \hat{w}(t)) \\ \hat{y}(t) &= C\hat{x}(t), \end{cases} \tag{8}$$

with $\hat{x} \in \hat{\mathbb{X}} \subset \mathbb{X}$, $\hat{u} \in \hat{\mathbb{U}} \subset \mathbb{U}$, and $\hat{w} \sim \mathcal{N}(0, I)$ and initialized with $\hat{x}_0$. This initial state is the associated representative point, that is $\hat{x}_0 = \hat{X}_i$ if $x_0 \in \mathbb{A}_i$ or equivalently $\hat{x}_0 = \Pi(x_0)$. The abstract model $\hat{M}$ can also be written as the following LTI system

$$\hat{M} : \begin{cases} \hat{x}(t+1) &= A\hat{x}(t) + B\hat{u}(t) + B_w \hat{w}(t) + \beta(t) \\ \hat{y}(t) &= C\hat{x}(t), \end{cases} \tag{9}$$

by introducing the deviation $\beta(t)$ as in Haesaert and Soudjani (2020). The $\beta(t)$-term denotes the deviation caused by the mapping Π in (8) and takes values in the following bounded set $\mathcal{B} := \bigcup_i \{\hat{X}_i - x_i | x_i \in \mathbb{A}_i\}$. At each time step t, the deviation $\beta(t) \in \mathcal{B} \subseteq \mathbb{R}^n$ is a function of $\hat{x}(t)$, $\hat{u}(t)$ and $\hat{w}(t)$, however, for simplicity we write $\beta(t)$.

Similarity quantification of $\hat{M}$. To quantify the similarity between the abstract model $\hat{M}$ and the original model M, we use the notion of (ϵ, δ)-stochastic simulation relation given in Definition 4. Next, we show that a coupling compensator can be

[2] Beyond the given representative points, one generally adds a sink state to both the continuous- and the finite-state model to capture transitions that leave the bounded set of states.

computed based on the maximal coupling between two probability measures and that the linear compensator can be used to solve the similarity quantification efficiently. Without loss of generality we limit the interface function to

$$u(t) := \hat{u}(t). \tag{10}$$

Based on the composed model (cf., Definition 2), we can define the error dynamics between (7) and (9) as

$$x_\Delta^+(t) = Ax_\Delta(t) + B_w(w(t) - \hat{w}(t)) - \beta(t), \tag{11}$$

where the state x_Δ and state update x_Δ^+ are the abbreviations of $x_\Delta(t) := x(t) - \hat{x}(t)$ and $x_\Delta(t+1)$, respectively. Furthermore, the stochastic disturbances $(\hat{w}, w)$ are generated by the coupling compensator $\mathcal{W}_\gamma$ as in (5) with $w - \hat{w}$ the *coupling compensator term*.

The error dynamics can be used to efficiently compute the simulation relation, denoted as $\mathcal{R}$. In contrast to Blute, Desharnais, Edalat, and Panangaden (1997), Desharnais, Gupta, Jagadeesan, and Panangaden (2004) and Julius and Pappas (2009), which quantify the deviation between the abstract and original model either completely on ϵ or completely on δ by fixing $\mathcal{W}_\gamma$, we design a coupling compensator $\mathcal{W}_\gamma$ with compensator value γ to achieve a preferred trade-off between ϵ and δ. Conditioned on event $w - \hat{w} = \gamma$ as in Definition 5 the error dynamics (11) reduce to

$$x_\Delta^+(t) = Ax_\Delta(t) + B_w\gamma(t) - \beta(t) \tag{12}$$

and hold with a probability of $\mathcal{W}(w - \hat{w} = \gamma \mid \hat{u}, \hat{x}, x) = \mathcal{W}_\gamma(w - \hat{w} = \gamma)$ that is at least bigger than $1 - \delta$ for all $\gamma \in \Gamma$. For a given $\gamma \in \Gamma$, we can compute an optimal coupling $\mathcal{W}_\gamma$ as follows. First, we introduce random variable $\hat{w}_\gamma \sim \mathcal{N}(\gamma, I)$ to replace the abstract disturbance

$$\hat{w}(t) = \hat{w}_\gamma(t) - \gamma(t). \tag{13}$$

Next, we find the coupling $\mathcal{W}_\gamma$ for $\hat{w}$ and w by finding a maximal coupling of $\hat{w}_\gamma$ and w after which we can directly obtain $\mathcal{W}_\gamma$ for $\hat{w}_\gamma$ and w. The computation of a maximal coupling in $\mathcal{P}(\mathbb{W} \times \mathbb{W})$ can be found in den Hollander (2012) and builds on top of maximizing the probability mass that can be located on the diagonal $w - \hat{w}_\gamma = 0$. Denote with $\rho(\cdot|0, I)$ and $\hat{\rho}(\cdot|\gamma, I)$ the respective probability density functions of $w \sim \mathcal{N}(0, I)$ and $\hat{w}_\gamma \sim \mathcal{N}(\gamma, I)$. As in den Hollander (2012), we construct a maximal coupling $\mathcal{W}_\gamma$ that has on its diagonal $w - \hat{w}_\gamma = 0$ the sub-probability distribution

$$\rho \wedge \hat{\rho} := \min(\rho, \hat{\rho}), \tag{14}$$

where min denotes the minimal value of the probability density function for different values of w. We can now establish a relation between deviation δ and value γ.

Lemma 6. *Consider two normal distributions $\mathbb{P}_w := \mathcal{N}(0, I)$ and $\mathbb{P}_{\hat{w}_\gamma} := \mathcal{N}(\gamma, I)$ with $\gamma \in \Gamma$. Then there exists a coupled distribution $\mathcal{W}_\gamma$ such that*

$$w - \hat{w}_\gamma = 0 \text{ for } (\hat{w}_\gamma, w) \sim \mathcal{W}_\gamma$$

with probability at least

$$1 - \delta := \inf_{\gamma \in \Gamma} 2\,\mathrm{cdf}(-\frac{1}{2}\|\gamma\|). \tag{15}$$

Here, cdf(·) denotes the cumulative distribution function of a one-dimensional Gaussian distribution $\mathcal{N}(0, 1)$. The full proof of Lemma 6 is given in Appendix A. This lemma shows that by choosing a *maximal coupling* the error dynamics (12) hold with a probability of at least $1 - \delta$. We can now quantify the similarity via robust controlled positively invariant sets, also referred to as controlled-invariant sets in the remainder of the paper. Here, we consider the error dynamics (12) as a system with constrained input γ and bounded disturbance β.

Definition 7 (*Controlled Invariance*). A set S is a (robust) controlled (positively) invariant set (Blanchini & Miani, 2008) for the error dynamics given in (12) with $\gamma \in \Gamma$ and $\beta \in \mathcal{B}$, if for all states $x_\Delta \in S$, there exists an input $\gamma \in \Gamma$, such that for any disturbance $\beta \in \mathcal{B}$ the next state satisfies $x_\Delta^+ \in S$.

We can quantify the similarity as follows.

Theorem 8. *Consider models M and $\hat{M}$ with error dynamics (12) for which controlled-invariant set S is given.*

If $\epsilon \geq \sup_{x_\Delta \in S} \|Cx_\Delta\|$ *and* $\delta \geq \sup_{\gamma \in \Gamma} 1 - 2\,\mathrm{cdf}(-\frac{1}{2}\|\gamma\|)$

then $\hat{M}$ is (ϵ, δ)-stochastically simulated by M as in Definition 4, denoted as $\hat{M} \preceq_\epsilon^\delta M$.

The proof is based on Lemma 6 and simulation relation

$$\mathcal{R} := \left\{(\hat{x}, x) \in \hat{\mathbb{X}} \times \mathbb{X} \mid (\hat{x}, x) \in S\right\}. \tag{16}$$

The inequality $\epsilon \geq \sup_{x_\Delta \in S} \|Cx_\Delta\|$ yields

$$\forall (\hat{x}, x) \in \mathcal{R} : \|Cx_\Delta\| \leq \epsilon, \tag{17}$$

and therefore also implies the second condition of an (ϵ, δ)-stochastic simulation relation as in Definition 4. The full proof of Theorem 8 is given in Appendix B.

Comparison to available methods. As mentioned before, in Haesaert and Soudjani (2020), Julius and Pappas (2009) and Blute et al. (1997), Desharnais et al. (2004), Soudjani et al. (2015) the deviation between the abstract and original model is quantified either completely on ϵ or completely on δ by fixing $\mathcal{W}_\gamma$. This can now be recovered by choosing a specific compensator value γ. More specifically, the deviation is completely quantified on ϵ, when $\delta = 0$. This result is obtained by choosing $\gamma = 0$, hence by choosing $\mathcal{W}_\gamma$ such that $w - \hat{w} = 0$ holds with probability 1, we recover the results in Haesaert and Soudjani (2020).

Similarly, the deviation is completely quantified on δ, when ϵ is fully defined by the gridsize. This is obtained by choosing $\gamma(t) = -B_w^{-1}Ax_\Delta(t)$ such that $x_\Delta(t+1) = -\beta(t)$. Hence we recover the results in Blute et al. (1997), Desharnais et al. (2004) and Soudjani et al. (2015) that also only hold for non-degenerate systems for which B_w is invertible.

Computation of deviation bounds. Consider interface function (10), relation (16), and an ellipsoidal controlled-invariant set S, that is

$$S := \left\{(\hat{x}, x) \in \hat{\mathbb{X}} \times \mathbb{X} \mid \|x - \hat{x}\|_D \leq \epsilon\right\}, \tag{18}$$

where $\|x\|_D$ denotes the weighted 2-norm, that is, $\|x\|_D = \sqrt{x^T Dx}$ with D a symmetric positive-definite matrix $D = D^T \succ 0$. The constraints in Theorem 8 can now be implemented as matrix inequalities for the error dynamics (12) with the linear parameterization of the compensator value as extra design variable, i.e., $\gamma = Fx_\Delta$. More precisely, we can formulate an optimization problem that minimizes the deviation bound ϵ for a given bound δ subject to the existence of an (ϵ, δ)-stochastic simulation relation between models $\hat{M}$ and M as given in Theorem 8. Given δ, we can compute a bound on input γ and define a suitable set Γ as

$$\gamma \in \Gamma := \left\{\gamma \in \mathbb{R}^d \mid \|\gamma\| \leq r = |2\,\mathrm{idf}\left(\frac{1-\delta}{2}\right)|\right\}, \tag{19}$$

which is a sphere of dimension d with radius r. Here idf is the inverse distribution function, i.e., the inverse of the cumulative distribution function. We will show that given bound δ, we can optimize bound ϵ and matrix D as in (18) by solving the following optimization problem

$$\min_{D_{inv},L,\epsilon} -\frac{1}{\epsilon^2} \tag{20a}$$

$$\text{s.t. } D_{inv} \succ 0,$$

$$\begin{bmatrix} D_{inv} & D_{inv}C^T \\ CD_{inv} & I \end{bmatrix} \succeq 0, \qquad (\epsilon\text{-}deviation) \tag{20b}$$

$$\begin{bmatrix} r^2 D_{inv} & L^T \\ L & \frac{1}{\epsilon^2} I \end{bmatrix} \succeq 0, \qquad (input\ bound) \tag{20c}$$

$$\begin{bmatrix} \lambda D_{inv} & * & * \\ 0 & (1-\lambda)\frac{1}{\epsilon^2} & * \\ AD_{inv}+B_w L & -\frac{1}{\epsilon^2}\beta_l & D_{inv} \end{bmatrix} \succeq 0 \qquad (invariance) \tag{20d}$$

where $D_{inv} = D^{-1}$, $L = FD_{inv}$, $\beta_l \in vert(\mathcal{B})$ and $l \in \{0, 1, \dots, q\}$. This optimization problem is parameterized in λ. We say that (20) has a feasible solution for values of $\delta, \epsilon \geq 0$, if there exist values for λ and D_{inv}, L such that the matrix inequalities in (20) hold. Now, we can conclude the following.

Theorem 9. *Consider models M and $\hat{M}$ and their error dynamics (12). If a pair $\delta, \epsilon \geq 0$ yields a feasible solution to (20), then $\hat{M}$ is (ϵ, δ)-stochastically simulated by M.*

Leveraging Theorem 9, an algorithm to search the minimal deviation ϵ can be composed as follows.

Algorithm 1 Optimizing ϵ given δ such that $\hat{M} \preceq_{\epsilon}^{\delta} M$

1: **Input:** $M, \hat{M}, \delta$
2: Compute r based on δ as in (19)
3: **for** λ between 0 and 1 **do**
4: $D_{inv}, L, \epsilon \leftarrow$ Solve optimization problem (20)
5: Set $D := (D_{inv})^{-1}$, $F := LD$,
6: Save parameters D, F, ϵ
7: **end for**
8: Take minimal value of ϵ and corresponding matrices D and F.

The efficiency of this algorithm depends on the efficiency of the line-search algorithm for λ (cf. line 3) and on the optimization problem (cf. line 4). The latter problem can be solved as a semi-definite programming problem with matrix inequalities as a function of $1/\epsilon^2$.

The full proof of Theorem 9 is given in Appendix C and is based on the following observations with respect to matrix inequalities (20b)–(20d). The ϵ-*deviation* requirement $\epsilon \geq \sup_{x_\Delta \in S} \|Cx_\Delta\|$ (cf. Theorem 8) can be simplified to the following implication

$$x_\Delta^T D x_\Delta \leq \epsilon^2 \implies x_\Delta^T C^T C x_\Delta \leq \epsilon^2. \tag{21}$$

For this $C^T C \preceq D$, or equivalently, the ϵ-deviation inequality (20b) is a sufficient condition.

The *input bound* $\gamma \in \Gamma$ with $\gamma = Fx_\Delta$ has to hold for all $x_\Delta \in S$. This reduces to

$$x_\Delta^T D x_\Delta \leq \epsilon^2 \implies x_\Delta^T F^T F x_\Delta \leq r^2 \tag{22}$$

for which $F^T F \preceq \frac{r^2}{\epsilon^2} D$ and the *input bound* (20c) are equivalent sufficient constraints.

For S to be a controlled-invariant set we need to have that for all states $x_\Delta \in S$, there exists an input $\gamma = Fx_\Delta \in \Gamma$, such that for any disturbance $\beta \in \mathcal{B}$ the next state satisfies $x_\Delta^+ \in S$. To achieve this it is sufficient to require that for any $\beta \in \mathcal{B}$

$$x_\Delta^T D x_\Delta \leq \epsilon^2 \implies \tag{23}$$
$$((A + B_w F)x_\Delta - \beta)^T D \left((A + B_w F)x_\Delta - \beta\right) \leq \epsilon^2.$$

Via the S-procedure this yields the invariance constraint (20d) as a sufficient condition. The corresponding details can be found in the appendix.

Concluding, the introduction of the coupling compensator in Section 3 allows the use of the well-studied theory of controlled-invariant sets to quantify the deviation between the original and abstract model on bounds ϵ and δ. Furthermore, it leads to an efficient computation of the deviation bounds as a set-theoretic problem. By considering an ellipsoidal controlled-invariant set, this computation can be formulated as an optimization problem constrained by parameterized matrix inequalities.

5. A coupling compensator for model order reduction

The provably correct design of controllers faces the curse of dimensionality. For some models this can be mitigated by including model order reduction in the abstraction. This additional abstraction step, yielding a lower dimensional continuous-state model, decreases the dimension of the abstract model and hence decreases the computation time. In this section, we show how the coupling compensator applies to model reduction.

First, we construct a reduced-order model M_r, based on (7), with state space $\mathbb{X}_r \subset \mathbb{R}^{n_r}$ with $n_r < n$ by using projection matrix $P \in \mathbb{R}^{n \times n_r}$ that maps the states of the reduced-order model to the original model, that is $x = Px_r$. The dynamics of M_r are given as

$$M_r : \begin{cases} x_r(t+1) &= A_r x_r(t) + B_r u_r(t) + B_{rw} w_r(t) \\ y_r(t) &= C_r x_r(t), \end{cases} \tag{24}$$

initialized with x_{r0} and with state $x_r \in \mathbb{X}_r$, input $u_r \in \mathbb{U}$, output $y_r \in \mathbb{Y}$ and disturbance $w_r \in \mathbb{W}$ that satisfy a Gaussian distribution $w_r \sim \mathcal{N}(0, I)$.

Similarity quantification of M_r. As in Haesaert, Soudjani et al. (2017), we resolve the inputs of models M (7) and M_r (24) by choosing interface function

$$u(t) := Ru_r(t) + Qx_r(t) + K(x(t) - Px_r(t)) \tag{25}$$

for some matrices R, Q, K, P, such that the Sylvester equation $PA_r = AP + BQ$ and $C_r = CP$ hold. The resulting error dynamics between (7) and (24) are

$$x_{r\Delta}^+ = \bar{A}x_{r\Delta} + \bar{B}u_r + B_w(w - w_r) + \bar{B}_w w_r, \tag{26}$$

where the stochastic disturbances (w_r, w) are generated by the coupled probability measure $\mathcal{W}_\gamma$ as in (5) and where the state $x_{r\Delta}$ and state update $x_{r\Delta}^+$ are the abbreviations of $x_{r\Delta}(t) := x(t) - P\hat{x}_r(t)$ and $x_{r\Delta}(t+1)$, respectively. Furthermore, we have $\bar{A} = A + BK$, $\bar{B} = BR - PB_r$ and $\bar{B}_w = B_w - PB_{rw}$. The term $(w - w_r)$ can now be used as a *coupling compensator term*.

Unlike existing work (Haesaert, Cauchi and Abate, 2017; Haesaert, Soudjani et al., 2017), we now use an approach similar to the one used in the previous section and substitute $w_r = w_\gamma - \gamma_r$ for w_r. Subsequently, we choose $\mathcal{W}_\gamma$ again as the coupling that maximizes the probability of event $w - w_\gamma = 0$. The error dynamics conditioned on this event reduce to

$$x_{r\Delta}^+ = \bar{A}x_{r\Delta} + \bar{B}u_r + B_w \gamma_r + \bar{B}_w w_r. \tag{27}$$

Lemma 6 still applies and can be used to compute $1-\delta$. If $\bar{B}_w = 0$ then (27) reduces to a set-theoretic control problem. In contrast, if this does not hold then by truncating the stochastic influence w_r, the error dynamics are still bounded and the probability δ can be modified to $\delta_r = \delta + \delta_{trunc}$, where δ_{trunc} is the error introduced by truncating w_r to the bounded set W. We consider the resulting error dynamics (27) as a system with constrained input γ_r and bounded disturbance $z = \bar{B}u_r + \bar{B}_w w_r$. This is very similar to the error dynamics in (12), however, now instead of bounded disturbance β we have $z \in Z = \bar{B}\mathbb{U} + \bar{B}_w W$, with W the set of the truncated disturbance w_r. If we now consider simulation relation

$$\mathcal{R}_{MOR} = \left\{(x_r, x) \in \mathbb{X}_r \times \mathbb{X} \mid \|x - Px_r\|_{D_r} \leq \epsilon_r\right\} \tag{28}$$

then we can recover the results in Theorem 8 to achieve an (ϵ_r, δ_r)-simulation relation between M_r and M.

Computation of deviation bounds. Consider interface function (25) and simulation relation (28). Given bound δ_r and matrices P, Q, R, we can optimize bound ϵ_r and matrix D_r as in (28) by solving an optimization problem similar to (20). Since model order reduction influences the error dynamics, the invariance constraint in (20d) has to be altered to

$$\begin{bmatrix} \lambda D_{r,inv} & * & * \\ 0 & (1-\lambda)\frac{1}{\epsilon_r^2} & * \\ AD_{inv}+BE+B_w L & \frac{1}{\epsilon_r^2} z_l & D_{r,inv} \end{bmatrix} \succeq 0, \tag{29}$$

where $E = KD_{r,inv}$ and $z_l \in vert(Z)$.

To make sure that the bound $u \in \mathbb{U}$ is satisfied an additional constraint can be formulated for matrix K in the exact same way as the matrix inequality for the input bound in (20c).

Similarity quantification between M and $\hat{M}_r$. The finite-state abstract model $\hat{M}_r$ of M_r (24) will now be substantially smaller than the finite-state abstraction of M. Given the (ϵ_r, δ_r)-simulation relation between M_r and M, the relation between $\hat{M}_r$ and M can be computed by considering the relation between $\hat{M}_r$ and M_r. More precisely, we can follow Section 4 and compute a pair $(\epsilon_{abs}, \delta_{abs})$ that guarantees that $\hat{M}_r$ is $(\epsilon_{abs}, \delta_{abs})$-stochastically simulated by M_r. Following Theorem 5 in Haesaert, Soudjani et al. (2017) on transitivity of $\preceq_\epsilon^\delta$ we have that if $M \preceq_{\epsilon_r}^{\delta_r} M_r$ and $M_r \preceq_{\epsilon_{abs}}^{\delta_{abs}} \hat{M}_r$ both hold, the simulation relation $M \preceq_{\epsilon_{abs}+\epsilon_r}^{\delta_{abs}+\delta_r} \hat{M}_r$ holds as well.

6. Case studies

In this section, we consider three case studies. For robust control synthesis, we use the robust dynamic programming mappings derived in Haesaert and Soudjani (2020), since given a robust satisfaction probability $\mathbb{R}_{\epsilon,\delta}(\hat{M} \times \hat{C} \models \phi)$ there always exists a controller C such that

$$\mathbb{P}(M \times C \models \phi) \geq \mathbb{R}_{\epsilon,\delta}(\hat{M} \times \hat{C} \models \phi).$$

The lower bound $\mathbb{R}_{\epsilon,\delta}$ is robust in the sense that it takes the approximation errors, ϵ and δ, into account. The robust satisfaction probability is computed by performing a value iteration based on computing a fixed-point solution for a robust Bellman operator as detailed in Haesaert and Soudjani (2020).

Car parking in 1D and 2D. First, we consider a one-dimensional (1D) case study of parking a car. The dynamics of the car are modeled using (7) with $A = 0.9, B = 0.5$ and $B_w = C = 1$ and with states $x \in \mathbb{X} = [-10, 10]$, input $u \in \mathbb{U} = [-1, 1]$ and output $y \in \mathbb{Y} = \mathbb{X}$. The unpredictable changes of the position of the car are captured by Gaussian noise $w \sim \mathcal{N}(0, 1)$. The goal of the controller is to guarantee that the car will be parked in parking spot P_1, while avoiding parking spot P_2. Using scLTL, this can be written as $\phi_{park} = \neg P_2 \cup P_1$. Here, we have chosen the regions $P_1 = [4.75, 6.25\rangle$ and $P_2 = [6.25, 10]$. First, we have computed a finite-state abstract model $\hat{M}$ in the form of (9) by partitioning the state space with regions of size 0.1. Next, we have selected optimal values for deviation bounds ϵ and δ based on the optimization problem given in (20). Finally, we have computed the satisfaction probability using Python and achieved a computation time of approximately 16 s and a memory usage of 6.16 MB. The results are shown in Fig. 1. Quantifying all the error on ϵ (green line) yields a relatively low overall satisfaction probability that slightly decreases the further you are from the region P_1. The low overall probability is caused by the large ϵ value, which makes reaching the desired parking spot P_1 very difficult. On the other hand, quantifying all the error on δ (blue line) yields a probability that starts relatively high, but steeply decreases the further you are from the region P_1. The presented method can achieve a full trade off of ϵ and δ (cf., the orange line) thereby achieving a higher satisfaction probability for part of the state space.

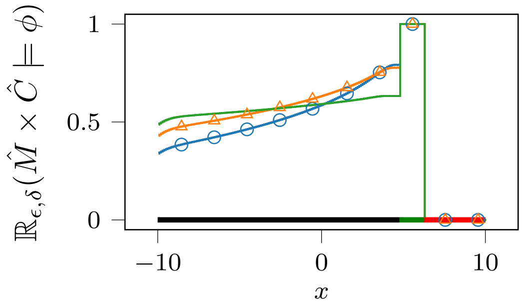
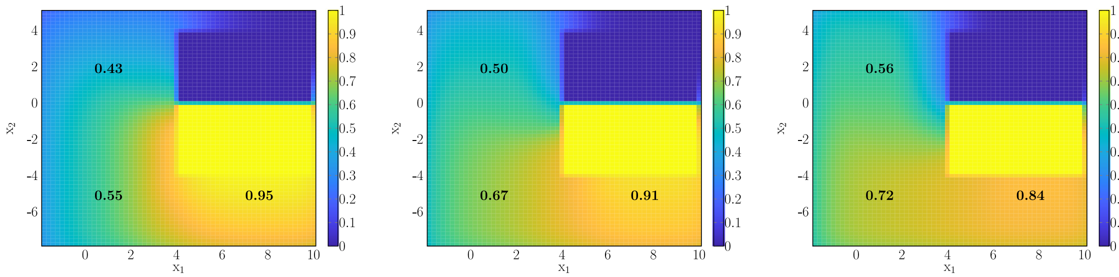


Fig. 1. Satisfaction probability of the 1D car parking example, where the blue circles, orange triangles and green line are obtained with (ϵ, δ) equal to $(0.05, 0.018)$, $(0.2, 0.012)$ and $(0.5, 0)$ respectively. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

As a second case study, we have considered parking a car in a two-dimensional (2D) space. More specifically, we have considered the model (7) with $A = 0.9I_2$, $B = 0.7I_2$, $B_w = C = I_2$ and state $x \in \mathbb{X} = \left\{(x_1, x_2)^T \in \mathbb{R}^2 | -2 \leq x_1 \leq 10, -8 \leq x_2 \leq 5\right\}$, input $u \in \mathbb{U} = [-1, 1]^2$, output $y \in \mathbb{Y} = \mathbb{X}$ and disturbance $w \sim \mathcal{N}(0, I_2)$. We wanted to synthesize a controller such that specification $\phi_{park} = \neg P_2 \cup P_1$, with regions $P_1 = \left\{ (x_1, x_2)^T \in \mathbb{R}^2 \mid 4 \leq x_1 \leq 10, -4 \leq x_2 < 0 \right\}$ and $P_2 = \left\{ (x_1, x_2)^T \in \mathbb{R}^2 \mid 4 \leq x_1 \leq 10, 0 \leq x_2 \leq 4 \right\}$ is satisfied. First, we have computed a finite-state abstract model $\hat{M}$ in the form of (9) by partitioning the state space with square regions of size 0.2. Next we have selected optimal values for deviation bounds ϵ and δ based on the optimization problem given in (20). Finally, we have computed the satisfaction probability using Python and achieved a computation time of approximately 594 s and a memory usage of 6.88 GB. The results are shown in Fig. 2 and are very similar to the 1D case, however, the influence from the avoid region (P_2) is more apparent in 2D. Furthermore, dividing the deviation between ϵ and δ (Fig. 2(b)) shows a decent trade-off between quantifying the deviation completely on δ (Fig. 2(a)) and ϵ (Fig. 2(c)). In the sense that the satisfaction probability is relatively high overall, while not steeply decreasing the further you are from the region P_1 (or closer to region P_2).

Building Automation System. As a third case study, we have considered a Building Automation System (BAS) (Cauchi & Abate, 2018) that is used in the benchmark study in Abate et al. (2020). The system consists of two heated zones with a common air supply. It has a 7-dimensional state with a 6-dimensional disturbance and a one-dimensional control input as described in Cauchi and Abate (2018, Sec.3.2). The goal is to control the temperature in zone 1 such that it does not deviate from the set point (20 °C) by more than 0.5 °C over a time horizon equal to 1.5 h, i.e., $\phi_T = \bigwedge_{i=0}^{5} \bigcirc^i P_1$ with $P_1 = \left\{x \in \mathbb{R}^7 \mid 19.5 \leq x_1 \leq 20.5\right\}$. We have subsequently reduced the model to a 2 dimensional system and gridded the state space. We obtained $(\epsilon_r, \delta_r) = (0.2413, 0.0161)$ and $(\epsilon_{abs}, \delta_{abs}) = (0.1087, 0)$ for a $\|\beta\| \leq 1.8 \cdot 10^{-3}$. This leads to a total deviation bound of $(\epsilon, \delta) = (0.35, 0.0161)$. Note that these results have been obtained for a slightly enlarged input set $u(t) \in$



(a) $(\epsilon, \delta) = (0.141, 0.051)$ (b) $(\epsilon, \delta) = (1.005, 0.016)$ (c) $(\epsilon, \delta) = (1.414, 0)$

Fig. 2. Satisfaction probability of the 2D car parking case study for different couplings. Figs. 2(a) and 2(c) represent quantifying the deviation completely on δ or on ϵ respectively, while Fig. 2(b) corresponds to dividing the deviation between ϵ and δ.

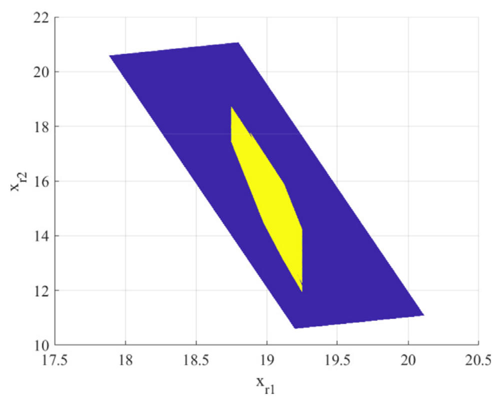


Fig. 3. Satisfaction probability for the BAS case study with initial state $x_r(0) = [x_{r1}, x_{r2}]^\top$. The blue and yellow regions correspond to a probability of 0 and 0.9035 respectively. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Table 1
Results of the BAS case study for different tools. This table contains the results from Abate et al. (2020) together with the results of our method (ϵ, δ)-CC.

Method	Run time (s)	Max. reach probability
FAUST^2	–	–
StocHy	3910.41	$\geq 0.8 \pm 0.23$
AMYTISS	2.9	≈ 0.8
SReachTools	1.33	≥ 0.99
(ϵ, δ)-CC	190.34	≥ 0.9035

[15, 33], originally $u(t) \in [15, 30]$. The satisfaction probability of 0.9035 as shown in Fig. 3 is consistent with Abate et al. (2020). The computation is performed in Matlab and required a memory usage of 3.06 GB.[3]

Comparison to available software tools. In Abate et al. (2020), the BAS benchmark has been used to compare the performance of AMYTISS (Lavaei et al., 2020), FAUST^2 (Soudjani et al., 2015), SReachTools (Vinod et al., 2019) and StocHy (Cauchi & Abate, 2019). These tools all target the verification of stochastic systems with continuous state space. Of these tools, SReachTools is the most limited. It can only handle a very specific set of models with specifications limited to reach(-avoid) and invariance. In contrast, the tools AMYTISS, FAUST^2 and StocHy are all abstraction-based methods that can handle a wider set of temporal specifications. In comparison to the numerical results presented in the previous paragraph, which follow from a basic Matlab implementation, these tools are more matured. StocHy is implemented in C++ and combines several advanced techniques such as symbolic probabilistic kernels and multi-threading. AMYTISS goes even further and utilizes parallel computations. If we compare our results, with those of these tools as summarized in Table 1, we notice that our implementation is performing on equal footing. As indicated in the table, FAUST^2 was unable to run this case study. StocHy required a very fine grid resulting in a very large computation time. Both AMYTISS and SReachTools obtain good results, since they achieve a reasonable or high reach probability in a short time. Our method yielded the second least conservative computation probability, only SReachTools does better. Though, this already shows that the given results are promising, future study is needed to develop a mature tool implemented in C++ that leverages parallelized computations and benchmark it fairly.

7. Conclusion and discussion

We have shown that the introduction of a coupling compensator increases the accuracy of the satisfaction probability of methods that use $(\epsilon, \delta)-$stochastic simulation relations. For this, we have defined a structured methodology based on set-theoretic methods for linear stochastic difference equations. These set-theoretic methods leverage the freedom in coupling-based similarity relations and allow us to tailor the deviation bounds to the considered synthesis problem. We have applied this to compute the deviation bounds expressed with $(\epsilon, \delta)-$stochastic simulation relations for finite-state abstractions, reduced-order abstractions, and for a combination thereof. We have illustrated that tailored deviation bounds that trade-off between output and probability deviations can be beneficial to the satisfaction probability. In future work, this approach will also be instrumental to build more advanced results where different levels of accuracy bounds are combined to tackle challenging temporal logic specification (van Huijgevoort & Haesaert, 2021).

Future work includes extending these results to more general nonlinear stochastic difference equations as in Lavaei et al. (2021) and to other types of similarity quantifications such as simulation functions (Lavaei et al., 2019). The former should enable extending the results in this paper to large-scale nonlinear stochastic systems.

Acknowledgments

This publication is part of the project CODEC (with project number 18244) of the research programme Veni which is (partly) financed by the Dutch Research Council (NWO).

[3] Here, memory usage is computed based on the sizes of the matrices stored in the workspace. Note that the Python and Matlab tool are implemented differently, which significantly impacts the memory usage.

Appendix A. Proof of Lemma 6

First, an analytical expression for the maximal coupling of two disturbances $w \sim \mathcal{N}(0, I)$ and $\hat{w}_\gamma \sim \mathcal{N}(\gamma, I)$ is derived. Their probability density functions are denoted by $\rho(\,\cdot\,|0, I)$ and $\hat{\rho}(\,\cdot\,|\gamma, I)$, respectively. The maximal coupling is based on Eq. (14). The probability density function of this maximal coupling is denoted as $\rho_w : \mathbb{W} \times \mathbb{W} \to \mathbb{R}^+$ and can be computed as follows. Denote the sub-probability density function $\rho_{\min}(w) = \min(\rho(w), \hat{\rho}(w))$, with $\Delta_\gamma = \int_{\mathbb{R}^d} \rho_{\min}(w)\mathrm{d}w$ and define the coupling density function as

$$\rho_w(w, \hat{w}_\gamma) = \rho_{\min}(w)\delta_{\hat{w}_\gamma}(w) \qquad \text{(A.1)}$$
$$+ (\rho(w) - \rho_{\min}(w))(\hat{\rho}(\hat{w}_\gamma) - \rho_{\min}(\hat{w}_\gamma))/(1 - \Delta_\gamma),$$

with $\delta_{\hat{w}_\gamma}(w)$ the shifted Dirac delta function equal to $+\infty$ if equality $w = \hat{w}_\gamma$ holds and 0 otherwise. The first term of the coupling (A.1) puts only weight on the diagonal $w = \hat{w}_\gamma$. The second term puts the remaining probability density in an independent fashion. The sub-probability Δ_γ can be computed as

$$\Delta_\gamma = \int_{\mathbb{R}^d} \min(\rho(w), \hat{\rho}(w))dw = \int_E \rho(w)\mathrm{d}w + \int_{\hat{E}} \hat{\rho}(\hat{w}_\gamma)\mathrm{d}\hat{w}_\gamma. \qquad \text{(A.2)}$$

Here, half spaces $\hat{E}$ and E denote the respective regions satisfying $\rho > \hat{\rho}$ and $\rho \leq \hat{\rho}$. These regions can be represented as d-dimensional half spaces.

As mentioned before, $\rho(\,\cdot\,|0, I)$ and $\hat{\rho}(\,\cdot\,|\gamma, I)$ are probability density functions of Gaussian distributions w and $\hat{w}_\gamma$ and therefore, ρ and $\hat{\rho}$ are strictly decreasing functions for increasing values of $\|w\|$ and $\|w - \gamma\|$ respectively. Furthermore, these two functions are equal except for a γ-shift. This implies that for a given point w if

- $\|w\| < \|w - \gamma\|$ then $\rho(w) > \hat{\rho}(w)$ (half space $\hat{E}$)
- $\|w\| \geq \|w - \gamma\|$ then $\rho(w) \leq \hat{\rho}(w)$ (half space E).

This last item shows that the half spaces $\hat{E}$ (1st item) and E (2nd item) are separated by a hyper-plane through the point $w = \frac{1}{2}\gamma$ and perpendicular to the vector γ. This hyper-plane, denoted by H is characterized by $H := \left\{w \in \mathbb{R}^d \mid \gamma^T w - \frac{1}{2}\|\gamma\|^2 = 0\right\}$, and illustrated in Fig. A.1. Since ρ and $\hat{\rho}$ are Gaussian density distribution that are equal up to γ-shift, as depicted in 2D in Fig. A.1, the integrals in (A.2) are equal to each other and $\Delta_\gamma = 2\int_E \rho(w)\mathrm{d}w$. It is trivial to see that this integral evaluates to $\Delta_\gamma = 2\,\mathrm{cdf}(-\frac{1}{2}\|\gamma\|)$. To obtain the worst case probability as in (15) we need to take into account all possible values of γ as $1 - \delta := \inf_{\gamma \in \Gamma} \Delta_\gamma = \inf_{\gamma \in \Gamma} 2\,\mathrm{cdf}(-\frac{1}{2}\|\gamma\|)$. This concludes the proof of Lemma 6.

Appendix B. Proof of Theorem 8

To prove that $\hat{M}$ is (ϵ, δ)-stochastically simulated by M under the conditions given in Theorem 8, the simulation relation in Definition 4 is proven point by point.

(1) *Initial condition.* Since $\hat{x}_0$ is inside the region that x_0 is in, the distance between $\hat{x}_0$ and x_0 is bounded by $\mathcal{B}$, that is, $\hat{x}_0 - x_0 \in \mathcal{B}$. Since it trivially holds that $\mathcal{B} \subseteq S$, (q.v. Theorem 5.2 in Blanchini and Miani (2008)) we also have $x_\Delta(0) = x_0 - \hat{x}_0 \in S$. This implies that the inclusion $(\hat{x}_0, x_0) \in \mathcal{R}$ holds for simulation relation (16).

(2) ϵ*-Accuracy.* For LTI-systems M (7) and $\hat{M}$ (9), condition (17) can be written as $\forall(\hat{x}, x) \in \mathcal{R} : \|y - \hat{y}\| \leq \epsilon$. Hence, since $\epsilon \geq \sup_{x_\Delta \in S} \|Cx_\Delta\|$ this condition holds.

(3) *Invariance.* Let $\gamma(t) \in \Gamma$ then according to Lemma 6 there exists a coupled distribution $\mathcal{W}$ such that with probability $1 - \delta$ the error dynamics in (11) can equivalently be written as (12). The latter implies that $(\hat{x}^+, x^+) \in \mathcal{R}$ holds with probability at least $1 - \delta$, which proves the third statement in Definition 4.

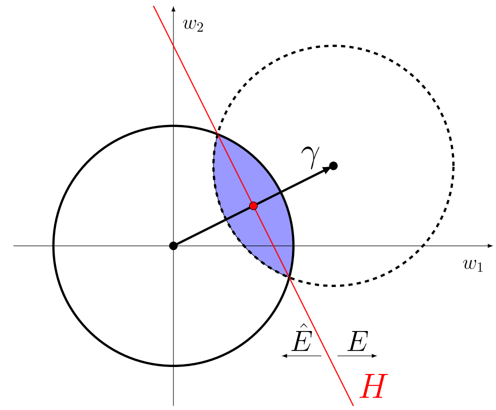


Fig. A.1. Level sets of probability density functions $\rho(\cdot|0, I)$ (black circle) and $\hat{\rho}(\cdot|\gamma, I)$ (dashed circle). Half spaces $\hat{E}$ and E are respectively the $\mathbb{R}^2$-plane left and right of hyper-plane H (red line). The area underneath $\min(\rho, \hat{\rho})$ *for these level sets* is indicated in blue. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Items one until three prove that $\hat{M}$ is (ϵ, δ)-stochastically simulated by M under the conditions given in Theorem 8.

Appendix C. Proof of Theorem 9

To prove Theorem 9, we show that the derived conditions in Section 4 can be written as the matrix inequalities in (20) and that they represent a set of sufficient conditions for the (ϵ, δ)-stochastic simulation relation.

First inequality constraint: In (18) we define an ellipsoidal controlled-invariant set S, with D a symmetric positive definite matrix, $D = D^T \succ 0$. This constraint can equivalently be written as $D_{inv} = D^{-1} \succ 0$.

Second inequality constraint (ϵ-deviation): The implication (21) holds if the inequality $C^T C \preceq D$ is satisfied. Applying the Schur complement on this inequality and performing a congruence transformation with non-singular matrix $\left[\begin{smallmatrix} D^{-1} & 0 \\ 0 & I \end{smallmatrix}\right]$ yields constraint (20b). Hence, if constraint (20b) is satisfied, the inequality $C^T C \preceq D$ holds and the bound on ϵ also holds.

Third inequality constraint (input bound): Similarly, the implication (22) holds if $F^T F \preceq \frac{r^2}{\epsilon^2} D$ is satisfied. This inequality can be rewritten in the exact same way as inequality $C^T C \preceq D$ and yields constraint (20c), where we denoted $L = FD_{inv}$. Hence, if constraint (20c) is satisfied, the inequality $F^T F \preceq \frac{r^2}{\epsilon^2} D$ holds and the input bound also holds.

Fourth inequality constraint (invariance): Next, we show that the constraint such that S is a controlled-invariant set as given by the implication in (23) can equivalently be written as constraint (20d) in (20). First, we use the S-procedure (Boyd, El Ghaoui, Feron, & Balakrishnan, 1994, p. 23) and Schur complement (with $D \succ 0$) and conclude that the implication in (23) holds for any $\beta \in \mathcal{B}$ if there exists $\lambda \geq 0$ such that for any $\beta \in \mathcal{B}$

$$\begin{bmatrix} \lambda D & 0 & (A+B_w F)^T D \\ 0 & (1-\lambda)\epsilon^2 & -\beta^T D \\ D(A+B_w F) & -D\beta & D \end{bmatrix} \succeq 0$$

holds. Performing a congruence transformation with non-singular matrix $\begin{bmatrix} D^{-1} & 0 & 0 \\ 0 & \frac{1}{\epsilon^2}I & 0 \\ 0 & 0 & D^{-1} \end{bmatrix}$ yields

$$\begin{bmatrix} \lambda D_{inv} & 0 & D_{inv}A^T + L^T B_w^T \\ 0 & (1-\lambda)\frac{1}{\epsilon^2} & -\beta^T \\ AD_{inv} + B_w L & -\beta & D_{inv} \end{bmatrix} \succeq 0, \tag{C.1}$$

with $D_{inv} = D^{-1}$ and $L = FD_{inv}$. It is computationally impossible to verify this matrix inequality point by point for any $\beta \in \mathcal{B}$. However, if $\mathcal{B}$ is a polytope, which we represent as $\mathcal{B} = \{\beta = bz, \bar{1}^T z \leq 1, z \geq 0, \}$ with b consisting of the q vectors β_l and $\bar{1} = [\,1\;1\;\ldots\;1\,]^T$. Then we only have to consider the q vertices of $\mathcal{B}$ and we conclude that the implication holds for any $\beta \in \mathcal{B}$ if there exists $\lambda \geq 0$ such that constraint (20d) in (20) is satisfied.

Concluding, if a pair $\delta, \epsilon \geq 0$ yields a feasible solution to (20), then the implications (21), (22) and (23) hold. Consequently, the bounds in Theorem 8 are satisfied and S is a controlled-invariant set. Based on Theorem 8 we conclude that $\hat{M}$ is (ϵ, δ)-stochastically simulated by M.

References

Abate, A., Blom, H., Cauchi, N., Delicaris, J., Hartmanns, A., Khaled, M., et al. (2020). *EPiC series in computing*: *vol. 74*, *ARCH-COMP20 category report: Stochastic models* (pp. 76–106).

Abate, A., Prandini, M., Lygeros, J., & Sastry, S. (2008). Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems. *Automatica*, *44*(11), 2724–2734.

Baier, C., & Katoen, J.-P. (2008). *Principles of model checking*. MIT Press.

Belta, C., Yordanov, B., & Gol, E. A. (2017). *Formal methods for discrete-time dynamical systems, Vol. 15*. Springer.

Blanchini, F., & Miani, S. (2008). *Set-theoretic methods in control*. Springer.

Blute, R., Desharnais, J., Edalat, A., & Panangaden, P. (1997). Bisimulation for labelled Markov processes. In *Proc. of 12th annual IEEE symposium on logic in computer science* (pp. 149–158). IEEE.

Boyd, S., El Ghaoui, L., Feron, E., & Balakrishnan, V. (1994). *Linear matrix inequalities in system and control theory*. SIAM.

Cauchi, N., & Abate, A. (2018). Benchmarks for cyber-physical systems: A modular model library for building automation systems. *IFAC-PapersOnLine*, *51*(16), 49–54.

Cauchi, N., & Abate, A. (2019). StocHy-automated verification and synthesis of stochastic processes. In *Proc. of the 22nd ACM international conference on hybrid systems: computation and control* (pp. 258–259).

den Hollander, F. (2012). *Lecture notes*, *Probability theory: The coupling method*. The Netherlands: Math. Inst. Leiden Univ.

Desharnais, J., Gupta, V., Jagadeesan, R., & Panangaden, P. (2003). Approximating labelled Markov processes. *Information and Computation*, *184*(1), 160–200.

Desharnais, J., Gupta, V., Jagadeesan, R., & Panangaden, P. (2004). Metrics for labelled Markov processes. *Theoretical Computer Science*, *318*(3), 323–354.

Girard, A., & Pappas, G. J. (2009). Hierarchical control system design using approximate simulation. *Automatica*, *45*(2), 566–571.

Haesaert, S., Cauchi, N., & Abate, A. (2017). Certified policy synthesis for general Markov decision processes: An application in building automation systems. *Performance Evaluation*, *117*, 75–103.

Haesaert, S., & Soudjani, S. (2020). Robust dynamic programming for temporal logic control of stochastic systems. *IEEE Transactions on Automatic Control*, *66*(6), 2496–2511.

Haesaert, S., Soudjani, S., & Abate, A. (2017). Verification of general Markov decision processes by approximate similarity relations and policy refinement. *SIAM Journal on Control and Optimization*, *55*(4), 2333–2367.

Huang, C., Chen, X., Lin, W., Yang, Z., & Li, X. (2017). Probabilistic safety verification of stochastic hybrid systems using barrier certificates. *ACM Transactions on Embedded Computing Systems*, *16*(5s), 1–19.

Jagtap, P., Soudjani, S., & Zamani, M. (2020). Formal synthesis of stochastic systems via control barrier certificates. *IEEE Transactions on Automatic Control*.

Julius, A. A., & Pappas, G. J. (2009). Approximations of stochastic hybrid systems. *IEEE Transactions on Automatic Control*, *54*(6), 1193–1203.

Kariotoglou, N., Kamgarpour, M., Summers, T. H., & Lygeros, J. (2017). The linear programming approach to reach-avoid problems for Markov decision processes. *Journal of Artificial Intelligence Research*, *60*, 263–285.

Kupferman, O., & Vardi, M. Y. (2001). Model checking of safety properties. *Formal Methods in System Design*, *19*(3), 291–314.

Lavaei, A., Khaled, M., Soudjani, S., & Zamani, M. (2020). AMYTISS: Parallelized automated controller synthesis for large-scale stochastic systems. In *International conference on computer aided verification* (pp. 461–474). Springer.

Lavaei, A., Soudjani, S., & Zamani, M. (2019). Compositional construction of infinite abstractions for networks of stochastic control systems. *Automatica*, *107*, 125–137.

Lavaei, A., Soudjani, S., & Zamani, M. (2021). Compositional abstraction-based synthesis of general MDPs via approximate probabilistic relations. *Nonlinear Analysis. Hybrid Systems*, *39*, 100991.

Pnueli, A. (1977). The temporal logic of programs. In *18th annual symposium on foundations of computer science* (pp. 46–57). IEEE.

Segala, R., & Lynch, N. (1994). Probabilistic simulations for probabilistic processes. In *International conference on concurrency theory* (pp. 481–496). Springer.

Soudjani, S., Gevaerts, C., & Abate, A. (2015). FAUST^2: Formal Abstractions of Uncountable-STate STochastic Processes. In *LNCS*, *TACAS* (pp. 272–286). Springer Berlin.

Tkachev, I., & Abate, A. (2014). On approximation metrics for linear temporal model-checking of stochastic systems. In *Proc. of the 17th international conference on hybrid systems: computation and control* (pp. 193–202).

van Huijgevoort, B. C., & Haesaert, S. (2021). Multi-layered simulation relations for linear stochastic systems. In *2021 European control conference (ECC)* (pp. 728–733).

Vinod, A., Gleason, J., & Oishi, M. (2019). SReachTools: A MATLAB stochastic reachability toolbox. In *Proc. of the 22nd ACM international conference on hybrid systems: computation and control* (pp. 33–38).

Zamani, M., Esfahani, P. M., Majumdar, R., Abate, A., & Lygeros, J. (2014). Symbolic control of stochastic systems via approximately bisimilar finite abstractions. *IEEE Transactions on Automatic Control*, *59*(12), 3135–3150.

Birgit C. van Huijgevoort is a promovendus at the Control Systems group, Department of Electrical Engineering, Eindhoven University of Technology (TU/e), The Netherlands. She received her B.Sc. degree cum laude in Electrical Engineering (Automotive) in 2016 and her M.Sc. degree cum laude in Systems & Control in 2018 from Eindhoven University of Technology.

Her research interests are in the field of correct-by-design control synthesis for stochastic cyber–physical systems with respect to temporal logic specifications.

Sofie Haesaert is an Assistant Professor at the Control Systems group, Department of Electrical Engineering, Eindhoven University of Technology (TU/e), The Netherlands. From 2017 to 2018, she was a postdoctoral scholar at Caltech. She received her Ph.D. from TU/e in 2017. She received her B.Sc. degree cum laude in Mechanical Engineering in 2010 at the Delft University of Technology. In 2012, she received her M.Sc. degree cum laude in Systems & Control at the Delft University of Technology, The Netherlands.

Her research interests are in the identification, verification, and control of cyber–physical systems for temporal logic specifications and performance objectives.