A coupling compensator approach

B.C. van Huijgevoort and S. Haesaert,
Control Systems group, Electrical Engineering Department, Eindhoven University of Technology

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 system’s 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.

Key words: Control synthesis; approximate simulation relations; stochastic systems; temporal logic

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 et al. 2008, Haesaert & Soudjani 2020, Haesaert, Soudjani & Abate 2017, Julius & Pappas 2009, Lavaei et al. 2020, Zamani et al. 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 & Abate 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. 2008, Haesaert & Soudjani 2020, Haesaert, Soudjani & Abate 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 et al. 2017, Vinod et al. 2019), recent results based on barrier certificates (Huang et al. 2017, Jagtap et al. 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 & Abate 2019, Haesaert & Soudjian 2020). In order to tackle this problem, we consider systems whose behavior is modeled via a stochastic difference equation and in which 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 ($\epsilon, \delta$)-stochastic simulation relations (Haesaert & Soudjian 2020, Soudjian 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 ($\epsilon, \delta$)-stochastic simulation relations (Haesaert & Soudjian 2020) quantitatively capture the set-theoretic approach to linear stochastic systems, however, the application of the coupling compensator is not restricted to linear systems nor to approximate simulation relations.

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 (Tzoulas et al. 2017; Kupferman & Vardi 2001), and analyze the influence of both the deviation in the transition and in the output with deviations in the transition probability. This work introduces a coupling compensator, to leverage the freedom in coupling-based similarity relations, such as (Soudjian 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 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 $(\mathcal{X}, \mathcal{B}(\mathcal{X}))$ where $\mathcal{X}$ is an arbitrary set and $\mathcal{B}(\mathcal{X})$ are the Borel sets. A probability measure $\mathbb{P}$ over this space has realizations $x \sim \mathbb{P}$, with $x \in \mathcal{X}$. Denote the set of probability measures on the measurable space $(\mathcal{X}, \mathcal{B}(\mathcal{X}))$ as $\mathcal{P}(\mathcal{X})$.

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

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

initialized with $x(0) = x_0$ and with state $x \in \mathcal{X}$, input $u \in \mathcal{U}$, disturbance $w \in \mathcal{W}$, and output $y \in \mathcal{Y}$. We assume that the functions $f : \mathcal{X} \times \mathcal{U} \times \mathcal{W} \rightarrow \mathcal{X}$ and $h : \mathcal{X} \rightarrow \mathcal{Y}$ 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 $\omega_{t+1} := x_0, u_0, x_1, u_1, \ldots, x_t$ 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 $\mu := \mu_0, \mu_1, \mu_2, \ldots$ consists of maps $\mu_\ell(\omega_{t+1}) \in \mathcal{U}$ assigning an input $u(t)$ to each finite path $\omega_{t+1}$ 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 $\mathcal{AP} = \{p_1, \ldots, p_N\}$ the set of atomic propositions, and let $2^{\mathcal{AP}}$ be the alphabet with letters $\pi \in 2^{\mathcal{AP}}$. An infinite string of letters is a word $\pi = \pi_0 \pi_1 \pi_2 \ldots$ with associated suffix $\pi_t = \pi_t \pi_{t+1} \pi_{t+2} \ldots$. An scLTL formula $\phi$ is defined as

$$
\phi := p | \neg p | \phi_1 \land \phi_2 | \phi_1 \lor \phi_2 | \bigcirc \phi | \phi_1 \cup \phi_2,
$$

with $p \in \mathcal{AP}$. The semantics of scLTL is defined for the suffixes $\pi_t$ as follows. An atomic proposition $p_t \models \pi_t$ holds if $p \in \pi_t$, while a negation $\neg p \models \pi_t$ holds if $p \notin \pi_t$. A conjunction $\phi_1 \land \phi_2 \models \pi_t$ holds if both $\phi_1 \models \pi_t$ and $\phi_2 \models \pi_t$ hold. A disjunction $\phi_1 \lor \phi_2 \models \pi_t$ holds if either $\phi_1 \models \pi_t$ or $\phi_2 \models \pi_t$ holds. A next operator $\bigcirc \phi \models \pi_t$ holds if $\pi_{t+1} \models \phi$. An until operator $\phi_1 \cup \phi_2 \models \pi_t$ holds if there exists an $i \in \mathbb{N}$ such that $\pi_{t+i} \models \phi_2$ and for all $j \in \mathbb{N}, 0 \leq j < i$ we have $\pi_{t+i} \models \phi_1$. By combining multiple operators, the eventually operator $\diamond \phi := \text{true} \cup \phi$ can also be defined. A labeling function $L : \mathcal{Y} \rightarrow 2^{\mathcal{AP}}$ assigns letters $\pi = L(y)$ to outputs $y \in \mathcal{Y}$. A state trajectory $x := x_0 x_1 x_2 \ldots$ satisfies a specification $\phi$, written $x \models \phi$, iff the generated word $\pi$ satisfies $\phi$ at time 0, i.e., $\pi_0 \models \phi$. The satisfaction probability of a specification is the probability that words generated by the controlled system $M \times C$ satisfy the specification $\phi$, 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 et al. 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

$$
\begin{align*}
\hat{M} : \begin{cases}
\hat{x}(t+1) &= \hat{f}(\hat{x}(t), \hat{u}(t), \hat{w}(t)), \\
\hat{y}(t) &= \hat{h}(\hat{x}(t)),
\end{cases}
\end{align*}
$$
initialized with \( \dot{x}(0) = \dot{x}_0 \) and with functions \( \hat{h} : \hat{X} \to Y \) and \( f : \hat{X} \times \hat{U} \times \hat{W} \to \hat{Y} \). Here, \( \hat{X} \) and \( \hat{U} \) can be finite and \( \hat{w}(t) \) is an i.i.d. noise sequence with realizations \( P_{\hat{w}} \).

Note also that we have \( \hat{Y} = Y \).

We quantify the difference between the original model \( \hat{M} \) and the abstract model \( M \) 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 \( \text{(Girard & Pappas 2009)} \) generalizes this by refining the control input \( \hat{u} \) to \( u \) as a function of the current states \( \mathcal{U}_w : \hat{U} \times \hat{X} \times X \to U \).

In a similar way, we can resolve the stochastic disturbance. We first relate the probability measures \( P_{\hat{w}} \) and \( P_w \) of the stochastic disturbances \( \hat{w} \) and \( w \) as follows.

### Definition 1 (Coupling of probability measures)

A coupling \( \text{[den Hollander 2012]} \) of two probability measures \( P_{\hat{w}} \) and \( P_w \) on the same measurable space \( (\mathcal{W}, B(\mathcal{W})) \) is any probability measure \( \mathcal{W} \) on the product measurable space \( (\mathcal{W} \times \mathcal{W}, B(\mathcal{W} \times \mathcal{W})) \) whose marginals are \( P_{\hat{w}} \) and \( P_w \), that is,

\[
P_{\hat{w}} = \mathcal{W} \cdot \pi_{\hat{w}}^{-1}, \quad P_w = \mathcal{W} \cdot \pi_w^{-1},
\]

for which \( \pi \) and \( \pi_\hat{w} \) are projections, respectively defined by

\[
\hat{\pi}(\hat{w}, w) = \hat{w}, \quad \pi(w, \hat{w}) = w, \quad \forall (\hat{w}, w) \in \mathcal{W} \times \mathcal{W}.
\]

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 \( \mathcal{W} : \hat{U} \times \hat{X} \times X \to \mathcal{P}(\mathcal{W}^2) \) that couples probability measures \( P_{\hat{w}} \) and \( P_w \) as in Def. 1. We can now define a composed model as follows.

### Definition 2 (Composed model)

Given a coupling measure \( (\hat{\pi}, \pi) \) and interface function \( \mathcal{U}_w \) resolving the disturbances and inputs, respectively, the model \( \hat{M} \mid M \) composed of models \( \hat{M} \) and \( M \) can be defined as

\[
\begin{align*}
\hat{x}(t+1) &= f(\hat{x}(t), \hat{u}(t), \hat{w}(t)) \\
x(t+1) &= f(x(t), U_\hat{x}(\hat{u}(t), \hat{x}(t), x(t)), w(t)) \\
\hat{y}(t) &= \hat{h}(\hat{x}(t)) \\
y(t) &= h(x(t))
\end{align*}
\]

(6)

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

The deviation between \( \hat{M} \) and \( M \) can be expressed as the metric \( d_\mathcal{W}(\hat{y}, y) := ||y - \hat{y}|| \), with \( \hat{y}, y \in Y \) for the traces of the composed model. Similar notions have been used in inter alia \( \text{[Haesaert & Soudjani 2020]} \), \( \text{[Julius & Pappas 2009]} \), \( \text{[Zamani et al. 2014]} \). 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 (2) and (1).

#### A coupling compensator approach

As in \( \text{[Haesaert, Soudjani & Abate 2017]} \), 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 \( \text{[Haesaert, Soudjani & Abate 2017]} \) applicable to stochastic difference equations.

### Definition 4 ((\( \epsilon, \delta \))-stochastic simulation relation)

Let stochastic difference equations \( \hat{M} \) and \( M \) with metric output space \( (Y, d_Y) \) be composed into \( \hat{M} \mid M \) based on the interface function \( \mathcal{U}_w \) (3) and the Borel measurable stochastic kernel \( \mathcal{W} \) (5). If there exists a measurable relation \( \mathcal{R} \subseteq \hat{X} \times X \), such that

1. \( (\hat{x}_0, x_0) \in \mathcal{R} \),
2. \( \forall (\hat{x}, x) \in \mathcal{R} : d_Y(\hat{y}, y) \leq \epsilon \), and
3. \( \forall (\hat{x}, x) \in \mathcal{R}, \forall \hat{u} \in \hat{U} : (\hat{x}^+, x^+) \in \mathcal{R} \) holds with probability at least \( 1 - \delta \),

then \( \hat{M} \) is \( (\epsilon, \delta) \)-stochastically simulated by \( M \), and this simulation relation is denoted as \( \hat{M} \leq^d_\mathcal{W} M \).

Here, \( \epsilon \) and \( \delta \) 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 \( \mathcal{U}_w \) 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 \( P_{\hat{w}} \) and \( P_w \) on the same measurable space \( (\mathcal{W}, B(\mathcal{W})) \). Given a bounded set \( \Gamma \) 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, \( \mathcal{W}_\gamma(w - \hat{w} = \gamma) \geq 1 - \delta \).

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

\[ M : \begin{cases} x(t + 1) = Ax(t) + Bu(t) + B_w w(t) \\ y(t) = Cx(t) \end{cases} \]  

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 \( w \in \mathbb{W} \subset \mathbb{R}^d \) 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 \cite{Baier2008} 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 \( \mathcal{A}_i \subset \mathbb{X}, \) such that \( \bigcup_i \mathcal{A}_i = \mathbb{X} \) and \( \mathcal{A}_i \cap \mathcal{A}_j = \emptyset \) for \( i \neq j. \) Choose a representative point in each region, \( \hat{X}_i \in \mathcal{A}_i, \) and define the set of abstract states \( \hat{X} \subset \mathbb{X} \) based on these representative points that is, \( \hat{X} := \{ \hat{X}_1, \hat{X}_2, \ldots, \hat{X}_n \}, \) where \( \alpha \) is the (finite) number of regions. Furthermore, a finite set of inputs is selected from \( \mathbb{U} \) and defines \( \hat{U}. \) To define the dynamics of the abstract model, consider the operator \( \Pi : \mathbb{X} \rightarrow \hat{X} \) that maps states \( x \in \mathcal{A}_i \) to their representative points \( \hat{x}_i \in \mathcal{A}_i. \) Using \( \Pi \) to obtain a finite-state abstraction of \( M, \) we get the abstract model \( \hat{M}. \)

\[ \hat{M} : \begin{cases} \hat{x}(t + 1) = \Pi(x(t)) \\ \hat{y}(t) = C\hat{x}(t) \end{cases} \]  

with \( \hat{x} \in \hat{X}, \) \( \hat{u} \in \hat{U}, \) and \( \hat{w} \sim \mathcal{N}(0, I) \) and initialized with \( \hat{x}_0 = \Pi(x_0). \) The abstract model \( \hat{M} \) can also be written as the following LTI system

\[ \hat{M} : \begin{cases} \hat{x}(t + 1) = A\hat{x}(t) + B\hat{u}(t) + B_w \hat{w}(t) + \beta(t) \\ \hat{y}(t) = C\hat{x}(t) \end{cases} \]  

by introducing the deviation \( \beta(t) \) as in \cite{Haeusser2020}. The \( \beta(t) \)-term denotes the deviation caused by the mapping \( \Pi \) in (8) and takes values in the following bounded set \( \mathcal{B} := \bigcup \{ \hat{X}_i - x_i | x_i \in \mathcal{A}_i \}. \) At each time step \( t, \) the deviation \( \beta(t) \in \mathcal{B} \) is a function of \( \hat{X}_i, \hat{u}(t), \) 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 \((\varepsilon, \delta)\)-stochastic simulation relation given in Def. 4. Next, we show that a coupling compensator can be 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

\[ u(t) := \hat{u}(t). \]

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

\[ x^*(t) = Ax \Delta(t) + Bu \Delta w(t) - \beta(t) \]

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

The error dynamics can be used to efficiently compute the simulation relation, denoted as \( \mathcal{R}. \) In contrast to \cite{Julius2009} and \cite{Blute1997}, \cite{Desharnais2004}, which quantify the deviation between the abstract and original model either completely on \( \varepsilon \) or completely on \( \delta \) by fixing \( \mathcal{W}, \) we design a coupling compensator \( \mathcal{W}, \) with compensator value \( \gamma \) to achieve a preferred trade-off between \( \varepsilon \) and \( \delta. \) Conditioned on event \( w - \hat{w} = \gamma \) as in Def. 5 the error dynamics (11) reduce to

\[ x^*_\Delta(t) = Ax \Delta(t) + Bu \gamma \Delta w(t) - \beta(t) \]

and hold with a probability of at least \( \gamma \) 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 \( \hat{w}(t) = \hat{w}(t) - \gamma(t). \)

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 \( \mathcal{P}(\mathcal{W} \times \mathcal{W}) \) can be found in \cite{denHollander2012} 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 \( \rho(\cdot, \gamma, I) \) the respective probability density functions of \( w \sim \mathcal{N}(0, I) \) and \( \hat{w}_\gamma \sim \mathcal{N}(\gamma, I). \) As in \cite{denHollander2012}, we construct a maximal coupling \( \mathcal{W}_\gamma \) that has on its diagonal \( w - \hat{w}_\gamma = 0 \) the sub-probability distribution

\[ \rho \wedge \rho := \min(\rho, \rho), \]

where \( \min \) denotes the minimal value of the probability density function for different values of \( w. \) We can now establish a relation between deviation \( \delta \) and value \( \gamma. \)

Lemma 6 Consider two normal distributions \( \mathcal{P}_w := \mathcal{N}(0, I) \) and \( \mathcal{P}_\hat{w}_\gamma := \mathcal{N}(\gamma, I) \) 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

\[ 1 - \delta := \inf_{\gamma \in \Gamma} \text{cdf}(\frac{1}{2} |\gamma|). \]

Here, \( \text{cdf}(\cdot) \) 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 $\gamma$ and bounded disturbance $\beta$.

**Definition 7 (Controlled invariance)** A set $S$ is a (robust) controlled (positively) invariant set [Blanchini & Miani 2003] for the error dynamics given in (12) with $\gamma \in \Gamma$ and $\beta \in \mathcal{B}$, if for all states $x_s \in S$, there exists an input $\gamma \in \Gamma$, such that for any disturbance $\beta \in \mathcal{B}$ the next state satisfies $x^+ \in S$.

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 $\epsilon \geq \sup_{x_s \in S} ||Cx_s||$ and $\delta \geq \sup_{x_s \in S} 1 - 2 \epsilon \sup_{\gamma \in \Gamma } (\frac{1}{2} ||\gamma||)$

then $\hat{M}$ is $(\epsilon, \delta)$-stochastically simulated by $M$ as in Def. 4, denoted as $\hat{M} \leq^\delta \epsilon M$.

The proof is based on Lemma 6 and simulation relation $\mathcal{R} := \{(\hat{x}, x) \in \hat{X} \times X | (\hat{x}, x) \in S\}$. (16)

The inequality $\epsilon \geq \sup_{x_s \in S} ||Cx_s||$ yields

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

and therefore also implies the second condition of an $(\epsilon, \delta)$-stochastic simulation relation as in Def. 4. The full proof of Theorem 8 is given in Appendix B.

**Comparison to available methods.** As mentioned before, in Haesaert & Soudjani (2020), Julius & 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 $\epsilon$ or completely on $\delta$ by fixing $\mathcal{W}_s$. This can now be recovered by choosing a specific compensator value $\gamma$. More specifically, the deviation is completely quantified on $\epsilon$, when $\delta = 0$. This result is obtained by choosing $\gamma = 0$, and hence defining the size of $\mathcal{W}_s$. Moreover, the deviation is completely quantified on $\delta$, when $\epsilon = 0$. Similarly, the deviation is completely quantified on $\epsilon$, when $\delta$ is fully defined by the gridsize. This is obtained by choosing $\gamma(t) = -B_w^{-1}Ax(t)$ such that $x(t) = -x(t)$. Hence we recover the results in Haesaert & Soudjani (2020). Similarly, the deviation is completely quantified on $\delta$, when $\epsilon$ is fully defined by the gridsize. This is obtained by choosing $\gamma(t) = -B_q^{-1}Ax(t)$ such that $x(t) = -x(t)$. Hence we recover the results in Blute et al. (1997), Desharnais et al. (2004), Soudjani et al. (2015) that also only hold for non-degenerate systems in which $B_w$ is invertible.

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

$$S := \{(\hat{x}, x) \in \hat{X} \times X | ||x - x|| \leq \epsilon\},$$  (18)

where $||x||_D$ denotes the weighted 2-norm, that is, $||x||_D = \sqrt{x^TDx}$ with $D$ a symmetric positive-definite matrix $D = DT^T > 0$. 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 $\epsilon$ for a given bound $\delta$. This optimization problem is parameterized in $\lambda$. We say that (20) has a feasible solution for $\lambda$, $\epsilon \geq 0$, if there exist values for $\lambda$ 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), $\hat{M}$ is $(\epsilon, \delta)$-stochastically simulated by $M$.

Leveraging Theorem 9, an algorithm to search the minimal deviation $\epsilon$ can be composed as follows. The efficiency of this algorithm depends on the efficiency of the line-search algorithm for $\lambda$ (c.f. line 3) and on the optimization problem (c.f. 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 $\epsilon$-deviation requirement $\epsilon \geq \sup_{x_0 \in S} ||x^t \Delta||$ (c.f. Theorem 8) can be simplified to the following implication

$$x^t_0 \Delta x_\Delta \leq \epsilon^2 \implies x^t_0 C^T C x_\Delta \leq \epsilon^2.$$  

(21)

For this $C^T C \preceq D$, or equivalently, the $\epsilon$-deviation inequality (20b) is a sufficient condition. The input bound $\gamma \in \Gamma$ with $\gamma = F x_\Delta$ has to hold for all $x_\Delta \in S$. This reduces to

$$x^t_0 \Delta x_\Delta \leq \epsilon^2 \implies x^t_0 F^T F x_\Delta \leq \epsilon^2 \quad (22)$$

for which $F^T F \preceq \frac{\epsilon^2}{\gamma^2} D$ 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 $\gamma = F x_\Delta \in \Gamma$, 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 $\beta \in \mathcal{B}$

$$x^t_0 \Delta x_\Delta \leq \epsilon^2 \implies ((A + B_w F)x_\Delta - \beta)^T D ((A + B_w F)x_\Delta - \beta) \leq \epsilon^2.$$  

(23)

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 $\epsilon$ and $\delta$. 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 $\mathcal{X}_r \subset \mathbb{R}^{n_r}$ 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

$$ M_r: \begin{cases} x_r(t + 1) = Ax_r(t) + Bu_r(t) + B_w w_r(t) \\ y_r(t) = C_r x_r(t), \end{cases} $$

(24)

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

**Similarity quantification of $M_r$.** As in [Haesaert, Soudjani & Abate 2017], we resolve the inputs of models $M$ (7) and $M_r$ (24) by choosing interface function

$$u(t) := Ru_r(t) + Q x_r(t) + K(x(t) - Px_r(t))$$  

(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

$$x^+_r = Ax_r + Bu_r + B_w (w - w_r) + B_w w_r, \quad (26)$$

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

Unlike existing work [Haesaert, Soudjani & Abate 2017], [Haesaert, Cauchi & Abate 2017], we now use an approach similar to the one used in the previous section and substitute $w_r = w_r - \gamma_r$ for $w_r$. Subsequently, we choose $W_r$ again as the coupling that maximizes the probability of event $w - w_r = 0$. The error dynamics conditioned on this event reduce to

$$x^+_r = Ax_r + Bu_r + B_w \gamma_r + B_w w_r. \quad (27)$$

Lemma 6 still applies and can be used to compute $1 - \delta$. If $B_w = 0$ 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 $\delta$ can be modified to $\delta_r = \delta + \delta_{trunc}$, where $\delta_{trunc}$ 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 $\gamma_r$ and bounded disturbance $z = Bu_r + B_w w_r$. This is very similar to the error dynamics in (12), however, now instead of bounded disturbance $\beta$ we have $z \in Z = BU + B_w W$, with $W$ the set of the truncated disturbance $w_r$. If we now consider simulation relation $\mathcal{R}_{MOR} = \{ (x_r, x) \in \mathcal{X}_r \times \mathcal{X} \mid ||x - Px_r||_D \leq \epsilon_r \}$ (28) then we can recover the results in Theorem 8 to achieve an $(\epsilon_r, \delta_r)$-simulation relation between $M_r$ and $M$.

**Computation of deviation bounds.** Consider interface function (25) and simulation relation (28). Given bound $\delta_r$ and matrices $P, Q, R$, we can optimize bound $\epsilon_r$ 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

$$AD_r \epsilon_r \leq 0 \text{ and } AD_r \epsilon_r + BE + B_w L \frac{1}{\epsilon_r} \leq 0,$$

(29)

where $E = KD_r \epsilon_r$ and $z \in \text{vert}(Z)$. To make sure that the bound $u \in U$ 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 $M_r$.** The finite-state abstract model $M_r$ of $M_r$ (24) will now be substantially smaller than the finite-state abstraction of $M$. Given the $(\epsilon_r, \delta_r)$-simulation relation between $M_r$ and $M$, the relation between $M_r$ and $M$ can be computed by considering the relation between $M_r$ and $M_r$. 

6
More precisely, we can follow Section 4 and compute a pair $(\epsilon_{abs}, \delta_{abs})$ that guarantees that $\hat{M}_c$ is $(\epsilon_{abs}, \delta_{abs})$-stochastically simulated by $M_c$. Following Theorem 5 in Haesaert & Soudjani (2017) on transitivity of $\leq_\epsilon^\delta$, we have that if $M \leq_{\epsilon_c}^\delta \hat{M}_r$ and $M \leq_{\epsilon_{abs} + \delta_{abs}} \hat{M}_r$ both hold, the simulation relation $M \leq_{\epsilon_{abs} + \epsilon_c} \hat{M}_r$ 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 & Soudjani (2020), since given a robust satisfaction probability $\mathbb{R}_{\epsilon, \delta}(M \times \hat{C} \models \phi)$ there always exists a controller $C$ such that

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

The lower bound $\mathbb{R}_{\epsilon, \delta}$ is robust in the sense that it takes the approximation errors, $\epsilon$ and $\delta$, 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 & 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 modelled using (7) with $A = 0.9$, $B = 0.5$ and $B_w = C = 1$ and with states $x \in X = [-10, 10]$, input $u \in U = [-1, 1]$ and output $y \in \hat{Y} = X$. 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 scSTL, this can be written as $\phi_{park} = -P_2 U P_1$. Here, we have chosen the regions $P_1 = \{4.75, 6.25\}$ 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 $\epsilon$ and $\delta$ 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 seconds and a memory usage of 6.16 MB. The results are shown in Fig. 1. Quantifying all the error on $\epsilon$ (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 $\epsilon$ value, which makes reaching the desired parking spot $P_1$ very difficult. On the other hand, quantifying all the error on $\delta$ (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 $\epsilon$ and $\delta$ (c.f. the orange line) thereby achieving a higher satisfaction probability for part of the state space.

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 $x \in \hat{X} = \{(x_1, x_2)^T \in \mathbb{R}^2 \mid -2 \leq x_1 \leq 10, -8 \leq x_2 \leq 5\}$, input $u \in U = [-1, 1]^2$, output $y \in \hat{Y} = X$ and disturbance $w \sim \mathcal{N}(0, I_2)$. We wanted to synthesize a controller such that specification $\phi_{park} = \neg P_2 U P_1$, with regions $P_1 = \{(x_1, x_2)^T \in \mathbb{R}^2 \mid 4 \leq x_1 \leq 10, -4 \leq x_2 < 0\}$ and $P_2 = \{(x_1, x_2)^T \in \mathbb{R}^2 \mid 4 \leq x_1 \leq 10, 0 \leq x_2 \leq 4\}$ 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 $\epsilon$ and $\delta$ 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 seconds 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 $\epsilon$ and $\delta$ (Fig. 2b) shows a decent trade-off between quantifying the deviation completely on $\delta$ (Fig. 2a) and $\epsilon$ (Fig. 2c). 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 & 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 ($20^\circ C$) by more than $0.5^\circ C$ over a time horizon equal to 1.5 hours, i.e., $\phi_T = \bigwedge_{t=0}^5 \bigvee_{i=1}^5 P_i$ with $P_i = \{x \in \mathbb{R}^7 \mid 19.5 \leq x_i \leq 20.5\}$. We have subsequently reduced the model to a 2 dimensional system and gridded the state space. We obtained $(\epsilon, \delta, \beta) = (0.2413, 0.0161)$ and $(\epsilon_{abs}, \delta_{abs}) = (0.1087, 0)$ for a $\|\beta\| \leq 1.8 \cdot 10^{-3}$. This leads to a total deviation
have been obtained for a slightly enlarged input set in Matlab and required a memory usage of 3.06 GB with Abate et al. (2020). The computation is performed 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.

**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), FAUST2 (Soudjani et al. 2015), SReachTools (Vmod 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, FAUST2 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 mature. 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, FAUST2 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.

![Figure 2](image2.png)

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

![Figure 3](image3.png)

Fig. 3. Satisfaction probability for the BAS case study with initial state $\mathbf{x}_0 = [x_{r1}, x_{r2}]^T$. The blue and yellow regions correspond to a probability of 0 and 0.9035 respectively.

bound of $(\epsilon, \delta) = (0.35, 0.0161)$. Note that these results have been obtained for a slightly enlarged input set $u(t) \in [15, 33]$, 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.

| Method     | Run time (sec) | Max. reach probability |
|------------|----------------|------------------------|
| FAUST2     | -              | -                      |
| StocHy     | 3910.41        | $\geq 0.8 \pm 0.23$    |
| AMYTISS    | 2.9            | $\approx 0.8$          |
| SReachTools| 1.33           | $\geq 0.99$            |
| $(\epsilon, \delta)$-CC | 190.34 | $\geq 0.9035$ |

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 $(\epsilon, \delta)$-CC.

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

---

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.
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.

References

Abate, A., Blom, H., Cauchi, N., Delicaris, J., Hartmanns, A., Khaled, M., Lavaei, A., Pilch, C., Remke, A., Schupp, S. et al. (2020), ‘ARCH-COMP20 category report: Stochastic models’, EPICS Series in Computing 74, 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), pp. 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’, Proc. of 12th Annual IEEE Symposium on Logic in Computer Science pp. 149–158.

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), pp. 49–54.

Cauchi, N. & Abate, A. (2019), ‘StocHy-automated verification and synthesis of stochastic processes’, Proc. of the 22nd ACM International Conference on Hybrid Systems: Computation and Control pp. 258–259.

Girard, A. & Pappas, G. J. (2009), ‘Hierarchical control system design using approximate simulation’, Automatica 45(2), pp. 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, pp. 75–103.

Haesaert, S., Soudjani, S. (2020), ‘Robust dynamic programming for temporal logic control of stochastic systems’, IEEE Transactions on Automatic Control 66(6), pp. 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), pp. 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), pp. 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), pp. 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, pp. 263–285.

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

Lavaei, A., Khaled, M., Soudjani, S. & Zamani, M. (2020), ‘AMYTISS: Parallelized automated controller synthesis for large-scale stochastic systems’, International Conference on Computer Aided Verification pp. 461–474.

Lavaei, A., Soudjani, S. & Zamani, M. (2019), ‘Compositional construction of infinite abstractions for networks of stochastic control systems’, Automatica 107, pp. 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, pp. 100991.

Pnueli, A. (1977), ‘The Temporal Logic of programs’, 18th Annual Symposium on Foundations of Computer Science pp. 46–57.

Segala, R. & Lynch, N. (1994), ‘Probabilistic simulations for probabilistic processes’, International Conference on Concurrency Theory pp. 481–496.
A Proof of Lemma 6

First, an analytical expression for the maximal coupling of two disturbances \( w \sim \mathcal{N}(0, I) \) and \( \hat{w} \sim \mathcal{N}(\gamma, I) \) 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 equation (14). The probability density function of this maximal coupling is denoted as \( \rho_{\min}(w) = \min(\rho(w), \hat{\rho}(w)) \), with \( \Delta_{\gamma} = \int_{\mathbb{R}^d} \rho_{\min}(w)dw \) and define the coupling density function as

\[
\rho_{w}(w, \hat{w}_{\gamma}) = \rho_{\min}(w)\delta_{\hat{w}_{\gamma}}(w) + (\rho(w) - \rho_{\min}(w))(\hat{\rho}(\hat{w}_{\gamma}) - \rho_{\min}(\hat{w}_{\gamma}))/2 \quad \gamma
\]

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 density functions are Gaussian density functions of Gaussian distributions \( \rho(w) \) and \( \hat{\rho}(\hat{w}_{\gamma}) \). The latter implies that the integral evaluates to \( \Delta_{\gamma} = 2 \int_{E} \rho(w)dw \). It is trivial to see that this integral evaluates to \( \Delta_{\gamma} = 2 \left[ \text{cdf}(-\frac{1}{2}||\gamma||) \right] \).

To obtain the worst case probability as in (15) we need to take into account all possible values of \( \gamma \) as \( 1 - \delta := \inf_{\gamma \in \Gamma} \Delta_{\gamma} = \inf_{\gamma \in \Gamma} 2 \left[ \text{cdf}(-\frac{1}{2}||\gamma||) \right] \). This concludes the proof of Lemma 6.

B Proof of Theorem 8

To prove that \( \bar{M} \) is \( (\epsilon, \delta) \)-stochastically simulated by \( M \) under the conditions given in Theorem 8, the simulation relation in Def. 4 is proven point by point.

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

2. \( \epsilon \)-Accuracy. For LTI-systems \( M \) (7) and \( \bar{M} \) (9), condition (17) can be written as \( \forall (\hat{x}, x) \in \mathcal{R} \) : \( ||y - \hat{y}|| \leq \epsilon \). Hence, since \( \epsilon \geq \sup_{x \in S} ||C_{\mathcal{X}}(\Delta)\) 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 Def. 4.
Items one until three prove that \( \hat{M} \) is \((\epsilon, \delta)\)-stochastically simulated by \( M \) under the conditions given in Theorem 8.

\[ \text{C Proof of Theorem 9} \]

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 \((\epsilon, \delta)\)-stochastic simulation relation.

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

\textbf{Second inequality constraint (\( \varepsilon \)-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 \( \begin{bmatrix} D^{-1} & 0 \\ 0 & I \end{bmatrix} \) yields constraint (20b). Hence, if constraint (20b) is satisfied, the inequality \( C^T C \preceq D \) holds and the bound on \( \epsilon \) also holds.

\textbf{Third inequality constraint (input bound):} Similarly, the implication (22) holds if \( F^T F \preceq \varepsilon^2 D \) 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 \( L = FD_{\text{inv}} \). Hence, if constraint (20c) is satisfied, the inequality \( F^T F \preceq \varepsilon^2 D \) holds and the input bound also holds.

\textbf{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 et al. 1994, p. 23) and Schur complement (with \( D > 0 \)) and conclude that the implication in (23) holds for any \( \beta \in B \) if there exists \( \lambda \geq 0 \) such that for any \( \beta \in B \)

\[
\begin{bmatrix}
\lambda D & 0 & (A + B \omega F)^T D \\
0 & (1-\lambda) I^2 & -\beta^T D \\
D(A + B \omega F) & -D\beta & D
\end{bmatrix} \succeq 0
\]

holds. Performing a congruence transformation with non-singular matrix \( \begin{bmatrix} D_{\text{inv}} & 0 & 0 \\ 0 & \frac{1}{\lambda} I & 0 \\ 0 & 0 & D^{-1} \end{bmatrix} \) yields

\[
\begin{bmatrix}
\lambda D_{\text{inv}} & 0 & 0 \\
0 & \frac{1}{\lambda} D_{\text{inv}} + A + B \omega L & -\beta^T D_{\text{inv}} \\
0 & (1-\lambda) \frac{1}{\lambda} & -\beta^T D_{\text{inv}} + (L^T B \omega)^T D_{\text{inv}}
\end{bmatrix} \succeq 0,
\]

with \( D_{\text{inv}} = D^{-1} \) and \( L = FD_{\text{inv}} \). It is computationally impossible to verify this matrix inequality point by point for any \( \beta \in B \). However, if \( B \) is a polytope, which we represent as \( B = \{ \beta = bz, \bar{1}^T z \leq 1, z \geq 0 \} \) with \( b \) consisting of the \( q \) vectors \( \beta_l \) and \( \bar{1} = [1 \ 1 \ ... \ 1]^T \). Then we only have to consider the \( q \) vertices of \( B \) and we conclude that the implication holds for any \( \beta \in B \) 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 \((\epsilon, \delta)\)-stochastically simulated by \( M \).