2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Abstracting Linear Stochastic Systems via Knowledge Filtering

M.H.W. Engelaar[1], L. Romao[2], Y. Gao[2] , M. Lazar[1], A. Abate[2], and S. Haesaert[1]

Abstract— **In this paper, we propose a new model reduction technique for linear stochastic systems that builds upon knowledge filtering and utilizes optimal Kalman filtering techniques. This new technique will reduce the dimension of the noise disturbance and will allow any controller designed for the reduced model to be refined into a controller for the original stochastic system, while preserving any specification on the output. Although initially the reduced model will be time-varying, a method will be provided with which the reduced model can become time-invariant if it satisfies some minor technical conditions. We present our theoretical findings with an example that supports the proposed framework and illustrates how model reduction and controller refinement of stochastic systems can be achieved. We finish the paper by considering specific examples to analyze both completeness with respect to controller synthesis and model order reduction with respect to the state.**

I. Introduction

Dynamical systems are becoming more complex, and their tasks more diverse. Adding to this, the inherent uncertainty of most real-life engineering systems [6], [12], [21], makes developing correct-by-design controllers for stochastic systems, i.e., controllers which ensure the satisfaction of given tasks, an ever-expanding field of research. In the last decade multiple computational tools on correct-by-design control synthesis for stochastic systems have been developed (AMYTISS [17], FAUST^2 [20], StocHy [7] and SySCoRe [22]) that can handle complex specifications such as those expressed by temporal languages (LTL, sc-LTL, STL) [4], [8]. These tools generally suffer from the curse of dimensionality, i.e., exponential growth in computational cost whenever the state-space increases. It has been shown [13], [25] that model reduction can mitigate this effect.

The reduction of dynamical models is a mature field in control research. Often known as model order reduction, the objective is to minimize the complexity of a system while retaining some guarantee. For deterministic systems, this includes, amongst others, guarantees on performance [2], frequency domain [11], and structure [19] by utilizing, for example, balanced truncation, rational Krylov and moment matching, respectively. Less work exists that can guarantee the satisfaction of complex specifications in the time domain. Examples for deterministic systems include hierarchical control [10] and simulation relations [3]. For stochastic systems, this includes such work as (approximate) stochastic simulation relations [12], [13], stochastic simulation functions [15], and stochastic bisimulation relations [18], [24]. These notions allow higher-order (stochastic) systems to be simulated by (finite- or) lower-order systems of (approximately) the same type, all while retaining (approximate) equivalency with regard to their state or output (distribution). For an extensive list of model reduction techniques, see references within [18].

Model reduction techniques considering complex temporal specifications are also known as formal abstraction techniques due to frequent usage within formal verification and synthesis. Formal abstraction techniques mainly consists of two components. The first component is the reduction (or abstraction) procedure, which is a procedure that explains how to simplify the original dynamics, thereby obtaining a so-called (simplified) abstract model. The second component is the controller refinement algorithm, which is an algorithm that explains how a correct-by-design controller on the abstract model can be refined into a correct-by-design controller on the original dynamics.

In this paper, we will expand upon the existing literature of formal abstraction by introducing a new model reduction technique that reduces the dimension of the noise disturbance on linear stochastic systems. Similar to the previously mentioned methods, we want to retain the satisfaction of any temporal specification defined on the original system. Accordingly, we will develop a reduction procedure (abstraction procedure) and a controller refinement algorithm. The reduction will consist of two steps: firstly, removing redundant state information, referred to as *knowledge filtering*, which yields a partially observable model, and secondly, computing a reduced realization of this partially observable model via optimal Kalman filtering [1]. More precisely, the second step implements a weak Gaussian stochastic realization [23]. We will define a sound controller refinement algorithm and discuss the completeness of the whole approach.

After formalizing the problem statement in Section II, a time-varying abstraction will be obtained in Section III. In Section IV, we explain how a time-invariant abstraction can be forced, by considering some technical assumptions. Several examples will be addressed in Section V, illustrating the reduction procedure and controller refinement algorithm. It will also be shown that our method allows for model reduction with respect to the state space where previously mentioned methods are unable. This section will also illustrate a lack of completeness regarding the controller refinement, which can be attributed to the knowledge filtering in the reduction procedure.

This work is supported by the Dutch NWO Veni project CODEC (project number 18244) and Swedish Research Council International Postdoc Grant 2021-06727. [1]Department of Electrical Engineering (Control Systems Group), Eindhoven University of Technology, The Netherlands. [2]Department of Computer Science, University of Oxford, United Kingdom Emails:{m.h.w.engelaar, m.lazar, s.haesaert}@tue.nl; {licio.romao, yulong.gao, alessandro.abate}@cs.ox.ac.uk

II. Problem Setup

For a given probability measure $\mathbb{P}$ defined over Borel measurable space $(\mathbb{X}, \mathcal{B}(\mathbb{X}))$, we denote the probability of an event $A \in \mathcal{B}(\mathbb{X})$ as $\mathbb{P}(A)$. In this paper, we will work with Euclidean spaces and Borel measurability. Details of any measurability considerations are omitted, and we refer the interested reader to [5].

Linear Stochastic System. We consider a linear time-invariant stochastic system $\mathbf{M}$ given by

$$\mathbf{M}: \begin{cases} x(t+1) & = Ax(t) + Bu(t) + w(t) \\ z(t) & = Hx(t), \end{cases} \tag{1}$$

where $x \in \mathcal{X} \subseteq \mathbb{R}^n$ is the state, $u \in \mathcal{U} \subseteq \mathbb{R}^m$ is the input, $z \in \mathcal{Z} \subseteq \mathbb{R}^p$ is the (performance) output, $x(0)$ is the initial state and is the realization of a Gaussian distribution with mean μ_0 and variance Σ_0, i.e., $x(0) \sim \mathcal{N}(\mu_0, \Sigma_0)$, and disturbance $w(t) \in \mathbb{R}^n$ is a realization of an independent, identically distributed noise $w(t) \sim \mathcal{N}(0, Q_w)$. Finite executions of $\mathbf{M}$ are alternating sequences of states and inputs ending in a state, such as $\boldsymbol{\omega}_N^{\text{fin}} = x(0)u(0)x(1)u(1)\dots x(N-1)u(N-1)x(N)$, which satisfy equation (1) for some finite noise sequence $\boldsymbol{w} = w(0)w(1)w(2)\cdots, w(N-1)$, where $x(0) \sim \mathcal{N}(\mu_0, \Sigma_0)$ and $w(t) \sim \mathcal{N}(0, Q_w)$ for all $t \in \{0, 1, \cdots, N-1\}$. We denote the *history at time* N as the set of all finite executions of length N by $\mathcal{E}_N \subseteq (\mathcal{X} \times \mathcal{U})^N \times \mathcal{X}$.

In its most general setting, a controller $\mathbf{C}$ is a sequence of policies $\mathbf{C} := \mathbf{C}_0\mathbf{C}_1\mathbf{C}_2\cdots$, such that $\mathbf{C}_t : \mathcal{E}_t \to \mathcal{U}$ is a map of the available history to the set of inputs. The chosen control inputs are given by $u(t) = \mathbf{C}_t(\boldsymbol{\omega}_t^{\text{fin}})$ and the controlled stochastic system $\mathbf{C} \times \mathbf{M}$ is obtained by composing $\mathbf{C}$ with $\mathbf{M}$. We denote by $\mathcal{Z} := \mathcal{Z}^{\mathbb{N}}$ the set of all possible output trajectories associated with $\mathbf{M}$. Each execution of $\mathbf{C} \times \mathbf{M}$ will produce an output trajectory $\boldsymbol{z} = z(0)z(1)z(2)\cdots \in \mathcal{Z}$. The output trajectory $\boldsymbol{z}$ is a realization of the probability distribution induced by the controlled system $\mathbf{C} \times \mathbf{M}$ and denoted as $\boldsymbol{z} \sim \mathbb{P}_{\mathbf{C}\times\mathbf{M}}$.

Stochastic Correct-by-Design Control Synthesis. Let us consider the goal of designing a controller $\mathbf{C}$ that ensures output trajectories of the controlled system $\mathbf{C} \times \mathbf{M}$ satisfy a given specification ϕ. We assume that each specification ϕ corresponds to a Borel measurable subset of $\mathcal{Z}$, denoted by $\mathcal{Z}_\phi \in \mathcal{B}(\mathcal{Z})$. Examples of such specifications include specifications given in linear-time temporal logics [3]. Given the stochastic nature of $\mathbf{M}$, it is natural to require that the specification ϕ is satisfied by the controlled system $\mathbf{C} \times \mathbf{M}$, with probability at least p. Let us denote the satisfaction probability as $\mathbb{P}_{\mathbf{C}\times\mathbf{M}}(\mathcal{Z}_\phi)$. Then, the objective is to synthesize $\mathbf{C}$ such that $\mathbb{P}_{\mathbf{C}\times\mathbf{M}}(\mathcal{Z}_\phi) \geq p$. We refer to this as *stochastic correct-by-design control synthesis*.

Problem statement. To mitigate scaling issues such as the curse of dimensionality in stochastic correct-by-design control synthesis, we are interested in designing an abstract model for which the stochastic control synthesis problem is substantially simpler while also preserving correctness to specifications defined on the output trajectories. More precisely, our goal is to construct a *noise reduced* abstract model $\bar{\mathbf{M}}$ such that for any correct-by-design controller $\bar{\mathbf{C}}$ synthesized for the abstract model $\bar{\mathbf{M}}$, a correct-by-design controller $\mathbf{C}$ can be obtained for the original model $\mathbf{M}$ with equal satisfaction probability, i.e.,

$$\forall \bar{\mathbf{C}}\ \exists \mathbf{C} : \mathbb{P}_{\bar{\mathbf{C}}\times\bar{\mathbf{M}}}(\mathcal{Z}_\phi) = \mathbb{P}_{\mathbf{C}\times\mathbf{M}}(\mathcal{Z}_\phi). \tag{2}$$

In the remainder, we constructively solve this problem.

III. Abstraction and Control Refinement: Time-varying Abstraction

Consider a stochastic system $\mathbf{M}$ as given by (1). To solve the stochastic correct-by-design control synthesis problem in (2) while also simplifying the noise, we introduce the abstraction procedure illustrated in Fig. 1 and the controller refinement algorithm represented in Algorithm 1.

The abstraction procedure hinges on removing potential redundant information from the original model $\mathbf{M}$ without influencing the performance output $\boldsymbol{z}$. The procedure is executed in two steps. The first step filters knowledge from $\mathbf{M}$ by introducing an observation output $y(t) = Cx(t)$. The result is a new stochastic system $\mathbf{M}_{\text{Obs}}$ that is partially observable, or more specific, a partially observable Markov decision process [16]. The second step replaces the partially observable model with a fully observable equivalent model via optimal Kalman filtering [1]. We refer to this fully observable model as the abstract model $\bar{\mathbf{M}}$.

In the following, we will elucidate these steps for a time-varying abstract model and show that the controller refinement algorithm is valid. In the next section, we present some technical conditions under which a time-invariant abstract model can be obtained.

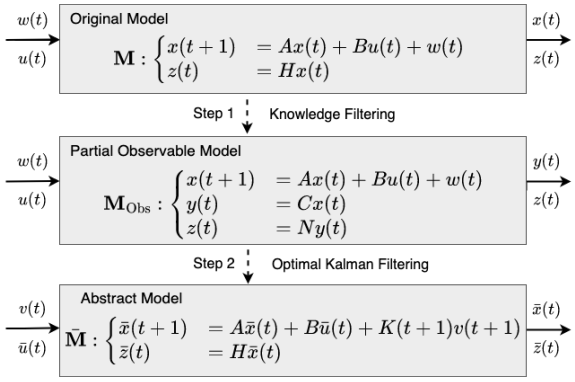

Fig. 1. The block diagram illustrates the abstraction procedure. The distribution of $v(t)$ depends on the distribution of $y(t)$. $K(t)$ is the time-varying Kalman gain obtained from the Kalman filter equations.

A. Abstract Model Construction

Following the steps of the abstraction procedure Fig. 1, we will construct the abstract model $\bar{\mathbf{M}}$. For the first step, we choose a matrix pair C and N with $C \in \mathbb{R}^{q\times n}$ and $N \in \mathbb{R}^{p\times q}$, such that $NC = H$ and $q < n$, and define the partial observable version of the original model as

$$\mathbf{M}_{\text{Obs}}: \begin{cases} x(t+1) & = Ax(t) + Bu(t) + w(t) \\ y(t) & = Cx(t) \\ z(t) & = Ny(t), \end{cases} \tag{3}$$

where $x(0) \sim \mathcal{N}(\mu_0, \Sigma_0)$, $y(t) \in \mathbb{R}^q$ is the observation output, and $w(t) \sim \mathcal{N}(0, Q_w)$. For the second step, we first introduce the needed optimal Kalman filtering techniques for estimating the state of (3) based on observations and inputs. We denote by $x_K(t|t)$ the expectation of $x(t)$, conditional on the available information at time t, that is, $x_K(t|t) = \mathbb{E}(x(t)|y(0)u(0)...u(t-1)y(t))$. Similarly, we denote by $P(t|t)$ the variance of $x(t)$, again conditional on the available information at time t, i.e., $P(t|t) = \text{Var}(x(t)|y(0)u(0)\cdots y(t))$. Quantities $x_K(t|t)$ and $P(t|t)$ are called, respectively, *a posteriori state estimate* and *a posteriori state variance*. The term a posteriori is used because all available information, including $y(t)$, is utilized in both definitions of $x_K(t|t)$ and $P(t|t)$. The *a priori* quantities $x_K(t|t-1)$ and $P(t|t-1)$ are defined similarly, but contrary to the a posteriori quantities, only consider the available information up till $u(t-1)$. As is common, these quantities can be determined as follows

$$\begin{aligned} x_K(t|t) &= x_K(t|t-1) \\ &\quad + K(t)[y(t) - Cx_K(t|t-1)], && \text{(4a)} \\ x_K(t+1|t) &= Ax_K(t|t) + Bu(t), && \text{(4b)} \\ P(t|t) &= P(t|t-1) - K(t)CP(t|t-1), && \text{(4c)} \\ P(t+1|t) &= AP(t|t)A^T + Q_w, && \text{(4d)} \\ K(t) &= P(t|t-1)C^T[CP(t|t-1)C^T]^{-1}, && \text{(4e)} \\ x_K(0|-1) &= \mu_0 \text{ and } P(0|-1) = \Sigma_0. && \text{(4f)} \end{aligned}$$

We will make the following assumption to ensure equations (4) are valid throughout this section.

Assumption 1: $C\Sigma_0 C^T \succ 0$ and $CQ_wC^T \succ 0$, i.e., both are strictly positive definite.

It is well known that the error between the a priori prediction of the output, $Cx_K(t|t-1)$, and the measured output $y(t)$ defines a Gaussian white noise sequence [23]. This noise sequence is referred to as the innovation and defined by

$$v(t) = y(t) - Cx_K(t|t-1). \tag{5}$$

The mean and variance of v can be computed directly, giving $\mu_v(t) = 0$ and $\Sigma_v(t) = CP(t|t-1)C^T$, see also [23, Theorem 14.4.2]. The innovation allows us to define a new linear stochastic system. This new system, referred to as the *a priori* innovation process, builds on the a priori quantities $\hat{x}(t) = x_K(t|t-1)$ and $\hat{P}(t) = P(t|t-1)$ and is given by

$$\hat{\mathbf{M}} : \begin{cases} \hat{x}(t+1) &= A\hat{x}(t) + Bu(t) + AK(t)v(t) \\ y(t) &= C\hat{x}(t) + v(t) \\ \hat{z}(t) &= Ny(t), \end{cases} \tag{6}$$

$$\begin{aligned} &\text{where } \hat{x}(0) = \mu_0,\ v(t) \sim \mathcal{N}(0, \Sigma_v(t)),\ \hat{P}(0) = \Sigma_0 \\ &\hat{P}(t+1) = A\hat{P}(t)A^T + Q_w - AK(t)C\hat{P}(t)A^T, \\ &K(t) = \hat{P}(t)C^T[C\hat{P}(t)C^T]^{-1},\ \Sigma_v(t) = C\hat{P}(t)C^T. \end{aligned}$$

Although this is the most commonly used version of the innovation process, we will now define an alternative one based on the a posteriori quantities $\bar{x}(t) = x_K(t|t)$ and $\bar{P}(t) = P(t|t)$. We refer to this as the *a posteriori* innovation process, and this will be our abstract model $\bar{\mathbf{M}}$, defined as

$$\bar{\mathbf{M}} : \begin{cases} \bar{x}(t+1) &= A\bar{x}(t) + Bu(t) + K(t+1)v(t+1) \\ y(t) &= C\bar{x}(t) \\ \bar{z}(t) &= Ny(t), \end{cases} \tag{7}$$

$$\begin{aligned} &\text{where } \bar{x}(0) \sim \mathcal{N}(\mu_0, \Sigma_0 - \bar{P}(0)), && \text{(8a)} \\ &v(t) \sim \mathcal{N}(0, \Sigma_v(t)),\ \Sigma_v(t) = C\hat{P}(t)C^T, && \text{(8b)} \\ &\bar{P}(t) = \hat{P}(t) - K(t)C\hat{P}(t), && \text{(8c)} \\ &\hat{P}(t+1) = A\bar{P}(t)A^T + Q_w, && \text{(8d)} \\ &K(t) = \hat{P}(t)C^T[C\hat{P}(t)C^T]^{-1}, && \text{(8e)} \\ &\bar{P}(0) = \Sigma_0 - \Sigma_0 C^T[C\Sigma_0 C^T]^{-1}C\Sigma_0. && \text{(8f)} \end{aligned}$$

In the appendix of the extended version of this paper [9], additional information is given concerning the derivation of both innovation processes. Finally, the definitive definition of the abstract model is given by

$$\bar{\mathbf{M}} : \begin{cases} \bar{x}(t+1) &= A\bar{x}(t) + B\bar{u}(t) + K(t+1)v(t+1) \\ \bar{z}(t) &= H\bar{x}(t), \end{cases} \tag{9}$$

together with the equations (8). The abstract model $\bar{\mathbf{M}}$ is a *weak Gaussian stochastic realization* of $\mathbf{M}_{\text{Obs}}$ (3) as defined in [23]. By construction, $\mathbf{M}$ and $\bar{\mathbf{M}}$ have the same state-space dimension; however, the noise affecting the latter takes value in an Euclidean space of smaller dimension, due to the knowledge filtering in step 1. More precisely, the noise input $w(t) \sim \mathcal{N}(0, Q_w)$ with $w(t) \in \mathbb{R}^n$ has been replaced with the noise input $K(t+1)v(t+1)$ with $v(t+1) \in \mathbb{R}^q$, where $q < n$. This reduction in complexity comes at the cost of having a time-varying system. In the next section, we present conditions under which the resulting $\bar{\mathbf{M}}$ is time-invariant.

B. Controller Refinement

What remains to be shown is that for any correct-by-design controller $\bar{\mathbf{C}}$ designed for the abstract model, there exists a correct-by-design controller $\mathbf{C}$ for the original model, see equation (2). We use the auxiliary output $y(t) = Cx(t)$ to define the following controller refinement Algorithm 1 – its implementation is depicted in the block diagram of Fig. 2.

Algorithm 1 Controller refinement algorithm

1: Given: $\mathbf{M}$, $\bar{\mathbf{M}}$, $\bar{\mathbf{C}}$
2: set $t := 0$ and compute $K(0) := \Sigma_0 C^T (C\Sigma_0 C^T)^{-1}$,
3: draw $x(0)$ from $\mathcal{N}(\mu_0, \Sigma_0)$,
4: compute $\bar{x}(0) = \mu_0 + K(0)(Cx(0) - C\mu_0)$,
5: **loop**
6: obtain $\bar{u}(t)$ according to $\bar{\mathbf{C}}$,
7: set $u(t) = \bar{u}(t)$, $\{ \leftarrow$ Implementing $\mathbf{C}\}$
8: draw $x(t+1)$ from $\mathbf{M}$ and get $y(t+1) = Cx(t+1)$,
9: compute $v(t+1) = y(t+1) - CA\bar{x}(t) - CB\bar{u}(t)$,
10: compute $\bar{x}(t+1) = A\bar{x}(t) + B\bar{u}(t) + K(t+1)v(t+1)$
11: take $t = t+1$.
12: **end loop**

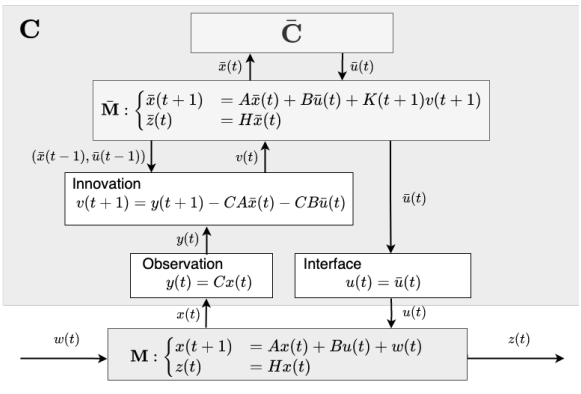

Fig. 2. A block diagram for the controller refinement (Algorithm 1)

The following theorem constitutes one of the main contributions of this paper.

Theorem 1: Consider $\mathbf{M}$ and $\bar{\mathbf{M}}$ as given by, respectively, (1) and (9) and assume that $C\Sigma_0 C^T \succ 0$ and $CQ_wC^T \succ 0$. Let ϕ be any specification described by $\mathcal{Z}_\phi \in \mathcal{B}(\mathcal{Z})$. Then $\forall \bar{\mathbf{C}}\ \exists \mathbf{C}$ such that $\mathbb{P}_{\bar{\mathbf{C}}\times\bar{\mathbf{M}}}(\mathcal{Z}_\phi) = \mathbb{P}_{\mathbf{C}\times\mathbf{M}}(\mathcal{Z}_\phi)$.

Proof: Consider a controller $\mathbf{C}$ constructed based on Algorithm 1. Using standard optimal Kalman filtering arguments, one can show that, at every time step, the realization of $v(t+1)$ in Algorithm 1 is uncorrelated with the current state $\bar{x}(t+1)$ and has distribution given by (8b). Therefore, the embedded model $\bar{\mathbf{M}}$ has the same output distribution as $\bar{\mathbf{M}}$ in (9) when both are given the same input sequence. Similarly, we claim that model $\bar{\mathbf{M}}$ in (9) and $\mathbf{M}$ have the same output distribution when given the same input sequence. The proof of this claim can be found in the appendix of the extended paper [9]. Hence, the embedded model $\bar{\mathbf{M}}$ has the same output distribution as $\mathbf{M}$ when both are given the same input sequence. This finishes the proof, as $\mathbb{P}_{\bar{\mathbf{C}}\times\bar{\mathbf{M}}}(\mathcal{Z}_\phi) = p$, now implies $\mathbb{P}_{\mathbf{C}\times\mathbf{M}}(\mathcal{Z}_\phi) = p$. □

IV. Abstraction and Control Refinement: Time-Invariant Case

In this section, we investigate sufficient conditions to obtain a time-invariant abstract model based on the abstraction procedure explained in Section III-A. From the block diagram in Fig. 2, one may deduce that a time-invariant model is derived if, amongst others, a time-invariant Kalman gain is employed.

A. Abstract Model Construction

As explained in the sequel, towards obtaining a time-invariant abstract model $\bar{\mathbf{M}}$, we need to define the following algebraic equation.

Definition 2 (Discrete Algebraic Ricatti Equation [14]): The discrete-time algebraic Ricatti equation (DARE) adapted to the model (3) is given by

$$X = AXA^T - AXC^T[CXC^T]^{-1}CXA^T + Q_w. \quad (10)$$

We say that $X \succ 0$ is a stabilizing solution to the DARE, if $A - FC$ is stable for $F = AXC^T(CXC^T)^{-1}$.
In case the variance of the initial condition (denoted by Σ_0) is a stabilizing solution to the algebraic Ricatti equation in (10), we have that $\hat{P}(t) = \Sigma_0$ in (8), i.e., the a priori state variance becomes constant. As a result the abstract model (9) will be time-invariant, which is formalized by the following lemma.

Lemma 3: Assume that $C\Sigma_0C^T \succ 0$. If $\Sigma_0 = X \succ 0$ is a stabilizing solution to (10), then the abstract model (9) is time-invariant and given by

$$\bar{\mathbf{M}}: \begin{cases} \bar{x}(t+1) & = A\bar{x}(t) + B\bar{u}(t) + Kv(t+1) \\ \bar{z}(t) & = H\bar{x}(t) \end{cases} \quad (11)$$

where $\bar{x}(0) \sim\ \mathcal{N}(\mu_0, X - P),\ \bar{v}(t) \sim \mathcal{N}(0, CXC^T)$,
$K = XC^T[CXC^T]^{-1},\ P = X - KCX.$

The main advantage of Lemma 3 is the guarantee of the abstract model (11) being time-invariant, contrary to the abstract model (9), which may be time-varying. Regrettably, most real-life engineering systems do not yield the result of Lemma 3, as, generally, Σ_0 will not solve (10). To alleviate this issue, we will consider a relaxed version that requires instead that $\Sigma_0 - X \succ 0$, with $X \succ 0$ being the stabilizing solution to (10). Accordingly, we have the following assumption for the remainder of this subsection.

Assumption 2: $CXC^T \succ 0$ and $\Sigma_0 - X \succ 0$ with $X \succ 0$ being the stabilizing solution to (10).

To obtain a time-invariant abstract model based on the above assumption, we again consider the abstraction procedure explained in Section III-A. While step 1 remains the same, step 2 will be changed slightly. An additional observation $\tilde{y} = x(0) + \tilde{w}$, where $\tilde{w} \sim \mathcal{N}(0, R)$, will be added at time $t = 0$. This will allow for modification of the a posteriori quantities of $x(0)$, $x_K(0|0)$ and $P(0|0)$, before continuing the abstraction procedure by utilizing the Kalman filter equations (4), excluding (4f). The goal is to ensure that $P(0|0) = X - XC^T[CXC^T]^{-1}CX$ implying that $P(t+1|t) = X$, $\forall t \in \{0, 1, 2, \dots\}$ in (4). This will make the a posteriori innovation process time-invariant. To accomplish this, we take $R = (X^{-1} - \Sigma_0^{-1})^{-1}$. The result will be an abstract model $\bar{\mathbf{M}}^*$, given by

$$\bar{\mathbf{M}}^*: \begin{cases} \bar{x}(t+1) & = A\bar{x}(t) + B\bar{u}(t) + Kv(t+1) \\ \bar{z}(t) & = H\bar{x}(t) \end{cases} \quad (12)$$

where $\bar{x}(0) \sim \mathcal{N}(\mu_0, \Sigma_0 - P),\ v(t) \sim \mathcal{N}(0, CXC^T)$
$K = XC^T[CXC^T]^{-1},\ P = X - KCX.$

Note that $\bar{\mathbf{M}}^*$ differs from the abstract model (11) only in the initial distribution. See the appendix of the extended paper [9] for a more detailed explanation on how to obtain $\bar{\mathbf{M}}^*$.

B. Controller Refinement

Under the conditions of Lemma 3, Algorithm 1 will again give a valid controller refinement algorithm and Theorem 1 can be rephrased as follows.

Corollary 4: Consider $\mathbf{M}$ and $\bar{\mathbf{M}}$ as given by, respectively, (1) and (11) and assume that $\Sigma_0 \succ 0$ is a stabilizing solution to (10), and $C\Sigma_0C^T \succ 0$. Let ϕ be any specification described by $\mathcal{Z}_\phi \in \mathcal{B}(\mathcal{Z})$. Then $\forall \bar{\mathbf{C}}\ \exists \mathbf{C}$ such that $\mathbb{P}_{\bar{\mathbf{C}}\times\bar{\mathbf{M}}}(\mathcal{Z}_\phi) = \mathbb{P}_{\mathbf{C}\times\mathbf{M}}(\mathcal{Z}_\phi)$.

Should instead abstract model $\bar{\mathbf{M}}^*$ be considered, Algorithm 1 needs to be slightly modified, resulting in Algorithm 2. Note that Algorithm 2 uses an auxiliary step to ensure the initialization is resolved correctly.

Algorithm 2 Controller refinement algorithm.

Given: $\mathbf{M}$, $\bar{\mathbf{M}}^*$, $\bar{\mathbf{C}}^*$
set $t := 0$ and compute $L = \Sigma_0[\Sigma_0 + R]^{-1}$,
draw $x(0)$ from $\mathcal{N}(\mu_0, \Sigma_0)$ and draw $\tilde{w}$ from $\mathcal{N}(0, R)$,
compute $\bar{\mu}_0 = \mu_0 + L(x(0) + \tilde{w} - \mu_0)$,
compute $\bar{x}(0) = \bar{\mu}_0 + K(Cx(0) - C\bar{\mu}_0)$,
loop
  obtain $\bar{u}(t)$ according to $\bar{\mathbf{C}}^*$,
  set $u(t) = \bar{u}(t)$, $\{ \leftarrow$ Implementing $\mathbf{C}\}$
  draw $x(t+1)$ from $\mathbf{M}$ and get $y(t+1) = Cx(t+1)$,
  compute $v(t+1) = y(t+1) - CA\bar{x}(t) - CB\bar{u}(t)$,
  compute $\bar{x}(t+1) = A\bar{x}(t) + B\bar{u}(t) + Kv(t+1)$
  take $t = t + 1$.
end loop

Based on Algorithm 2, we can now extend the result of Theorem 1 to the abstract model $\bar{\mathbf{M}}^*$.

Theorem 5: Consider $\mathbf{M}$ and $\bar{\mathbf{M}}^*$ as given by, respectively, (1) and (12). Let $X \succ 0$ be a stabilizing solution to (10), and assume that $\Sigma_0 - X \succ 0$ and $CXC^T \succ 0$. Let ϕ be any specification described by $\mathcal{Z}_\phi \in \mathcal{B}(\mathcal{Z})$. Then $\forall \bar{\mathbf{C}}^* \ \exists \mathbf{C}$ such that $\mathbb{P}_{\bar{\mathbf{C}}^* \times \bar{\mathbf{M}}^*}(\mathcal{Z}_\phi) = \mathbb{P}_{\mathbf{C}\times\mathbf{M}}(\mathcal{Z}_\phi)$.

Proof: The proof follows from Algorithm 2, similar to Theorem 1 only now with two initial measurements. □

Remark 1: Due to the knowledge filtering in step 1 of the abstraction procedure, in general, Theorem 1, Corollary 4 and Theorem 5 do not hold when reversing the statement, that is, the existence of $\mathbf{C}$ such that $\mathbb{P}_{\mathbf{C}\times\mathbf{M}}(\mathcal{Z}_\phi) = p$ does not imply existence of $\bar{\mathbf{C}}$ such that $\mathbb{P}_{\bar{\mathbf{C}}\times\bar{\mathbf{M}}}(\mathcal{Z}_\phi) = p$. This will be further illustrated in the following section.

V. Stochastic Correct-by-Design Control Synthesis: Examples

In this section, we will consider an example to illustrate the abstraction procedure and the controller refinement algorithm. Another example will show that model reduction with respect to the state can be achieved, under the right conditions, where previous existing methods are inadequate. Finally, we will illustrate that, by filtering knowledge, we may construct an abstract model for which synthesis of a correct-by-design controller is not possible.

Example 1: Consider the discrete-time stochastic system

$$\mathbf{M}: \begin{cases} x(t+1) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} u(t) + w(t) \\ z(t) \quad = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} x(t), \end{cases} \tag{13}$$

where $x(0) \sim \mathcal{N}(0, \Sigma_0)$ and $w \sim \mathcal{N}(0, Q_w)$ with

$$\Sigma_0 = \begin{bmatrix} 5 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{bmatrix} \text{ and } Q_w = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0.05 \end{bmatrix}.$$

Let ϕ be a temporal specification, which requires z to be within $[-1, 1]$ over the interval $[1, 100]$. We aim to design a controller $\mathbf{C}$ such that $\mathbb{P}_{\mathbf{C}\times\mathbf{M}}(\mathcal{Z}_\phi) \geq 0.95$.

Let us construct an abstract model $\bar{\mathbf{M}}_1$ utilizing information from the second and third state, that is, let $C_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and $N_1 = \begin{bmatrix} 0 & 1 \end{bmatrix}$, and notice that $[0\ 0\ 1] = N_1 C_1$, satisfying the condition $H = NC$. Let $X = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0.05 \end{bmatrix}$ be the solution to (10) associated with $\mathbf{M}$, and observe that $\Sigma_0 - X \succ 0$ and $C_1 X C_1^T \succ 0$. The abstract model is obtained from (12) and given by

$$\bar{\mathbf{M}}_1: \begin{cases} \bar{x}_1(t+1) \ = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \bar{x}_1(t) + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \bar{u}_1(t) + \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} v_1(t) \\ \bar{z}_1(t) \quad\quad = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \bar{x}_1(t) \end{cases}$$

where $\bar{x}_1(0) \sim \mathcal{N}(0, \begin{bmatrix} 4 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{bmatrix})$ and $v_1 \sim \mathcal{N}(0, \begin{bmatrix} 2 & 0 \\ 0 & 0.05 \end{bmatrix})$. Notice that this abstract model is time-invariant.

For $\bar{\mathbf{M}}_1$ to satisfy the specification, take $\bar{\mathbf{C}}_1 : \bar{u}_1(t) = \begin{bmatrix} 0 & -1 & 0 \end{bmatrix} \bar{x}_1(t)$. The result will be that $\bar{z}_1(t) = \begin{bmatrix} 0 & 1 \end{bmatrix} v_1(t+1)$, that is, $\bar{z}_1(t) \sim \mathcal{N}(0, 0.05)$. Using the cumulative distribution function of $\mathcal{N}(0, 0.05)$, we can compute that $\mathbb{P}(\bar{z}_1(t) \notin [-1, 1]) = 7.744\text{e-}6$ for all $t \in [1, 100]$. This implies that $\mathbb{P}(\bar{\boldsymbol{z}}_1 \notin \mathcal{Z}_\phi) = 7.741\text{e-}4$ and $\mathbb{P}_{\bar{\mathbf{C}}_1 \times \bar{\mathbf{M}}_1}(\mathcal{Z}_\phi) > 0.95$. To obtain controller $\mathbf{C}_1$, we utilize Algorithm 2. In Fig. 3, the result of applying Algorithm 2 is shown. □

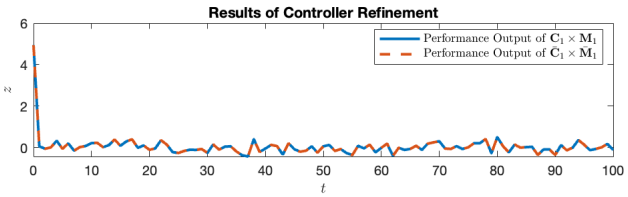

Fig. 3. The performance output of the original- and embedded abstract model over a horizon $t \in [0, 100]$, when applying Algorithm 2.

The above example illustrates that the proposed abstraction procedure yields a simplified system in regard to the noise and the controller refinement algorithm will produce a correct-by-design controller for the original model. Even though we considered a simple specification in this example, these results remain unaltered for more complex properties. Similarly, a trivial control design was used in this example, but should any other correct-by-design controller on the abstract model be used, these results remain again unaltered.

Model Reduction with respect to the State. We now investigate model reduction with respect to the state.

Example 2 (continued from Ex. 1): Assume $\Sigma_0 = X$, a stabilizing solution to (10). Inspired by Lemma 3, consider the abstract model

$$\bar{\mathbf{M}}_2: \begin{cases} \bar{x}_2(t+1) \ = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \bar{x}_2(t) + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \bar{u}_2(t) + \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} v_2(t) \\ \bar{z}_2(t) \quad\quad = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \bar{x}_2(t) \end{cases}$$

where $\bar{x}_2(0) \sim \mathcal{N}(0, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0.05 \end{bmatrix})$ and $v_2 \sim \mathcal{N}(0, \begin{bmatrix} 2 & 0 \\ 0 & 0.05 \end{bmatrix})$. Due to its structure, system $\bar{\mathbf{M}}_2$ can be reduced to

$$\bar{\mathbf{M}}_{2,r}: \begin{cases} \bar{x}_2(t+1) \ = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \bar{x}_2(t) + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \bar{u}_2(t) + v_2(t) \\ \bar{z}_2(t) \quad\quad = \begin{bmatrix} 0 & 1 \end{bmatrix} \bar{x}_2(t) \end{cases}$$

where $\bar{x}_2(0) \sim \mathcal{N}(0, \left[\begin{smallmatrix} 2 & 0 \\ 0 & 0.05 \end{smallmatrix}\right])$ and $v_2 \sim \mathcal{N}(0, \left[\begin{smallmatrix} 2 & 0 \\ 0 & 0.05 \end{smallmatrix}\right])$. Utilizing the lower dimensional system $\bar{\mathbf{M}}_{2,r}$, we obtain the correct-by-design controller $\bar{\mathbf{C}}_2 : \bar{u}_2(t) = \begin{bmatrix} -1 & 0 \end{bmatrix} \bar{x}_2(t)$, after which we use Algorithm 1 to obtain controller $\mathbf{C}_2$. □

It is important to note that the above reduction cannot be quantified by existing simulation relations such as [13], [15], [18]. This makes our method a promising new model reduction technique, but for which further research is still necessary. Notice that in Algorithm 1, a minor modification needs to be made based on the obtained reduced model. For instance, in the above example, one must remove the first element of $\bar{x}(t)$ before feeding the remainder to $\bar{\mathbf{C}}_2$.

Lack of Completeness. The proposed framework is not complete. Due to our choice of knowledge filtering, the original problem might become oversimplified to such a degree that no correct-by-design controller can be obtained for the abstract model. However, this failure to design a controller using the abstract model does not imply that the specification cannot be enforced on the original dynamics.

Example 3 (continued from Ex. 1): Consider again the linear time-invariant stochastic system (13) with constraint $\mathbb{P}_{\mathbf{C}\times\mathbf{M}}(\mathcal{Z}_\phi) \geq 0.95$. Consider now matrices $C_2 = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}$ and $N_2 = 1$, which leads to the following abstract model

$$\bar{\mathbf{M}}_3 : \begin{cases} \bar{x}_3(t+1) & = \left[\begin{smallmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right] \bar{x}_3(t) + \left[\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right] \bar{u}_3(t) + \left[\begin{smallmatrix} 0 \\ 0 \\ 1 \end{smallmatrix}\right] v_3(t) \\ \bar{z}_3(t) & = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix} \bar{x}_3(t) \end{cases}$$

where $\bar{x}_3(0) \sim \mathcal{N}(0, \left[\begin{smallmatrix} 4 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{smallmatrix}\right])$ and $v_3 \sim \mathcal{N}(0, 2.05)$.

For $\bar{\mathbf{M}}_3$, no controller $\bar{\mathbf{C}}_3$ exist such that $\mathbb{P}_{\bar{\mathbf{C}}_3\times\bar{\mathbf{M}}_3}(\mathcal{Z}_\phi) \geq 0.95$, since maximizing the probability satisfaction of the specification ϕ leads to the controller $\bar{\mathbf{C}}_3 : \bar{u}_3(t) = \begin{bmatrix} 0 & -1 & 0 \end{bmatrix} \bar{x}_3(t)$, resulting in $\bar{z}_3(t) \sim \mathcal{N}(0, 2.05)$. Using the cumulative distribution function again, we can numerically compute that $\mathbb{P}_{\bar{\mathbf{C}}_3\times\bar{\mathbf{M}}_3}(\mathcal{Z}_\phi) = 1.543\text{e-}29$. This means no controller for $\bar{\mathbf{M}}_3$ can enforce specification ϕ. However, previously, we have shown how to enforce this specification for a more complex abstract model. Hence, examples 1 and 3 clearly illustrate that while both abstract models simplify the stochastic control synthesis problem, oversimplification may prevent us from finding an adequate controller. □

VI. Conclusion

In this paper, we proposed a model reduction technique on the noise disturbance, whereby a simpler representation of the original dynamics is obtained by means of reducing state information, which we called knowledge filtering, and via optimal Kalman filtering. We introduce the abstraction procedure, which, under some technical conditions, may lead to a time-invariant abstract model. Our controller refinement algorithm is constructive and allows for the design of correct-by-design controllers on the original dynamics via correct-by-design controllers on the abstract model. We finished the paper by illustrating the abstraction procedure and the controller refinement, by showing how our reduction method can achieve model reduction on the state space, which existing methods, such as those employing simulation relations, cannot realize, and by examining the completeness of our technique.

References

[1] B. D. Anderson and J. B. Moore, *Optimal filtering*. Courier Corporation, 2012.

[2] A. C. Antoulas, *Approximation of large-scale dynamical systems*. SIAM, 2005.

[3] C. Baier and J.-P. Katoen, *Principles of model checking*. MIT press, 2008.

[4] C. Belta, B. Yordanov, and E. Gol, *Formal methods for discrete-time dynamical systems*. Springer, 2017, vol. 15.

[5] D. Bertsekas and S. E. Shreve, *Stochastic optimal control: the discrete-time case*. Athena Scientific, 1996, vol. 5.

[6] S. Brechtel, T. Gindele, and R. Dillmann, "Probabilistic decision-making under uncertainty for autonomous driving using continuous POMDPs," in *17th international IEEE conference on intelligent transportation systems (ITSC)*, 2014, pp. 392–399.

[7] N. Cauchi and A. Abate, "StocHy : Automated verification and synthesis of stochastic processes," in *Tools and Algorithms for the Construction and Analysis of Systems*, 2019, pp. 247–264.

[8] A. Donzé, "On signal temporal logic," in *Runtime Verification: 4th International Conference, RV 2013, Rennes, France, September 24-27, 2013. Proceedings 4*. Springer, 2013, pp. 382–383.

[9] M. H. W. Engelaar, L. Romao, Y. Gao, M. Lazar, A. Abate, and S. Haesaert, "Abstracting linear stochastic systems via knowledge filtering," *arXiv preprint Arxiv:2304.05770*, 2023.

[10] A. Girard and G. J. Pappas, "Hierarchical control system design using approximate simulation," *Automatica*, vol. 45, pp. 566–571, 2009.

[11] S. Gugercin, A. C. Antoulas, and C. Beattie, "H_2 model reduction for large-scale linear dynamical systems," *SIAM journal on matrix analysis and applications*, vol. 30, no. 2, pp. 609–638, 2008.

[12] S. Haesaert, N. Cauchi, and A. Abate, "Certified policy synthesis for general markov decision processes," *Performance Evaluation*, vol. 117, pp. 75–103, 2017.

[13] S. Haesaert, S. E. Z. Soudjani, and A. Abate, "Verification of general markov decision processes by approximate similarity relations and policy refinement," *SIAM Journal on Control and Optimization*, vol. 55, no. 4, pp. 2333–2367, 2017.

[14] V. Ionescu and M. Weiss, "Continuous and discrete-time riccati theory: a popov-function approach," *Linear Algebra and its Applications*, vol. 193, pp. 173–209, 1993.

[15] A. A. Julius and G. J. Pappas, "Approximations of stochastic hybrid systems," *IEEE TAC*, vol. 54, no. 6, pp. 1193–1203, 2009.

[16] V. Krishnamurthy, *Partially observed Markov decision processes*. Cambridge university press, 2016.

[17] A. Lavaei, M. Khaled, S. Soudjani, and M. Zamani, "Amytiss: Parallelized automated controller synthesis for large-scale stochastic systems," in *International Conference on Computer Aided Verification*. Springer, 2020, pp. 461–474.

[18] G. Pola, C. Manes, A. J. van der Schaft, and M. D. Di Benedetto, "Bisimulation equivalence of discrete-time stochastic linear control systems," *IEEE TAC*, vol. 63, no. 7, pp. 1897–1912, 2017.

[19] R. V. Polyuga and A. Van der Schaft, "Structure preserving model reduction of port-hamiltonian systems by moment matching at infinity," *Automatica*, vol. 46, no. 4, pp. 665–672, 2010.

[20] S. E. Z. Soudjani, C. Gevaerts, and A. Abate, "FAUST^2: Formal abstractions of uncountable-state stochastic processes," in *Tools and Algorithms for the Construction and Analysis of Systems*. Springer Berlin Heidelberg, 2015, pp. 272–286.

[21] S. Thrun, "Probabilistic robotics," *Communications of the ACM*, vol. 45, no. 3, pp. 52–57, 2002.

[22] B. Van Huijgevoort, O. Schön, S. Soudjani, and S. Haesaert, "SySCoRe: Synthesis via stochastic coupling relations," in *Proceedings of the 26th ACM International Conference on Hybrid Systems: Computation and Control*, 2023, pp. 1–11.

[23] J. H. van Schuppen, *Control and System Theory of Discrete-Time Stochastic Systems*. Springer, 2021.

[24] M. Zamani, P. M. Esfahani, R. Majumdar, A. Abate, and J. Lygeros, "Symbolic control of stochastic systems via approximately bisimilar finite abstractions," *IEEE TAC*, vol. 59, no. 12, pp. 3135–3150, 2014.

[25] M. Zamani, I. Tkachev, and A. Abate, "Towards scalable synthesis of stochastic control systems," *Discrete Event Dynamic Systems*, vol. 27, pp. 341–369, 2017.