Abstraction Based Supervisory Controller Synthesis for High Order Monotone Continuous Systems

Thomas Moor[1] and Jörg Raisch[2]

[1] Research School of Information Sciences and Engineering
Australian National University, Canberra
[2] Lehrstuhl für Systemtheorie technischer Prozesse
Otto-von-Guericke Universität Magdeburg, and
Systems and Control Theory Group
Max-Planck-Institut für Dynamik komplexer technischer Systeme
Magdeburg, Germany

Abstract. Abstraction based approaches to hybrid control systems synthesis have so far been mostly limited to problems with low-order linear continuous dynamics. In this paper, results from the theory of monotone dynamical systems are used to efficiently compute discrete abstractions for a class of nonlinear models. Furthermore, a situation is investigated where the high-dimensional plant state converges to a low-dimensional manifold; in the proposed approach the computational effort is governed by the dimension of the low-order manifold without neglecting the high-order dynamics. Results are applied to synthesize a discrete event controller for the automatic start-up of a nonlinear distillation column model of order 42.

1 Introduction

The control of a physical, biological or chemical process by a digital computer program often leads to heterogeneous systems that include both continuous and discrete event dynamics. Such systems are referred to as *hybrid control systems* and, in general, exhibit highly complex behaviours. From an engineering perspective, the systematic design of hybrid systems to meet given performance specifications is of particular interest; e.g. (Asarin et al., 2000b, Cury et al., 1998, Davoren and Nerode, 2000, Koutsoukos et al., 2000, Lunze et al., 1997, Lygeros et al., 1999, Zhivoglyadov and Middleton, 1999). When investigating suitable methodologies for particular design objectives and system classes, the development of synthesis procedures that are both efficient and reliable represents a major challenge. The demand for reliability results from safety critical applications, such as air traffic control or the control of chemical processes. As it is only for extremely restrictive conditions that hybrid controller synthesis problems can be solved directly on the basis of a hybrid plant model, a common approach is to resort to approximation based methods; e.g. (Cury et al., 1998, Koutsoukos et al., 2000, Lichtenberg et al., 1999a, Lunze et al., 1997, Moor and Raisch, 1999b, Philips et al., 1999, Raisch and O'Young, 1998). In this context, reliability becomes a nontrivial issue: does a controller which has been synthesized for a particular approximation also achieve the design objectives for the original problem? Roughly speaking, an affirmative answer can be given under the condition that the approximation accounts for all signals on

S. Engell, G. Frehse, E. Schnieder (Eds.): Modelling, Analysis and Design of Hybrid Systems, LNCIS 279, pp. 247−265, 2002.

which the original plant can possibly evolve. An approximation that exhibits this crucial *behavioural inclusion property* is referred to as an *abstraction.*

This paper specifically addresses the synthesis of discrete event controllers for continuous plants with discrete external signals. For this class of synthesis problems we have developed an abstraction scheme of particular convenience, namely *l-complete approximation*. While for all parameter values $l \in \mathbb{N}_0$ the behavioural inclusion property is fulfilled, it can be seen that increasing l corresponds to improving the approximation accuracy. The latter is an essential feature as it allows to systematically adjust the approximation accuracy to the application at hand. By construction, any l-complete approximation can be realized by a finite automaton. Hence, the hybrid synthesis problem is transformed into a purely discrete problem, which can subsequently be solved using methods from DES theory. Some further detail on l-complete approximation in the context of supervisory controller synthesis is given in Sect. 2; for a self contained development of the topic the reader is referred to (Moor and Raisch, 1999b, Moor et al., 2002, Raisch and O'Young, 1998). Our work on abstraction based supervisory control and related topics in hybrid control theory was partly funded by *Deutsche Forschungsgemeinschaft* under the KONDISK-scheme (research grants Ra 516/3-1, Fr 598/6-1, Fr 598/6-2, and Fr 598/6-3). This support is gratefully acknowledged. Beside our core contribution to abstraction based supervisory control (Lichtenberg et al., 1999a, Moor, 1998, Moor, 2000, Moor and Raisch, 1999b, Moor et al., 1998, Moor et al., 2002, Raisch, 1998, Raisch, 2000a, Raisch, 2000b, Raisch and O'Young, 1997, Raisch and O'Young, 1998), we have also addressed hierarchical (Moor et al., 2001b, Raisch et al., 2001, Raisch and Itigin, 2000, Raisch et al., 2000) and modular (Moor et al., 2001a, Moor and Raisch, 2000) extensions to our approach. We have discussed computational procedures for linear dynamics under time-driven and event-driven sampling (Franke et al., 2000, Moor and Raisch, 1999a, Raisch and O'Young, 1997) and applied our results in a number of case studies (Klein et al., 2000, Klein et al., 1998, Klein et al., 1999, Klein and Raisch, 1998, Raisch et al., 1998).

In principle, the computational procedure to generate l-complete approximations is straightforward. There are, however, two major problems that have limited applications to a class of plant models that appears small when compared to the generality of the theoretical framework provided by (Moor and Raisch, 1999b): (i) quantization cells have to be tracked under the progress of time and intersected with other quantization cells. Clearly, this is a difficult problem if the right hand side of the differential or difference equation is nonlinear in the continuous state variable. (ii) Computational effort "explodes" with growing state dimension. Hence, applications have been restricted to fairly low-dimensional plant models. From a more general perspective, both limitations are closely related to the absence of efficient procedures for high-order and/or nonlinear reachability analysis and, in principle, also apply to other approximation based synthesis methods. In this contribution, we derive conditions for high order nonlinear systems that allow efficient computation of l-complete approximations without sacrificing reliability in the subsequent controller design.

The paper is organized as follows: in Sect. 2, we briefly summarize the considered controller synthesis problem and the basic procedure for l-complete approximation. In Sect. 3, we introduce the notion of monotone dynamical systems and show why it is extremely helpful for computing discrete abstractions for a certain class of nonlinear systems. In Sect. 4, we explore a situation that allows treatment of high-dimensional systems. Finally, in Sect. 5, we apply our results to synthesize a DES controller for the start-up of a distillation column that is described by a nonlinear model of order 42.

2 Abstraction Based Supervisory Control

In earlier work (Moor and Raisch, 1999b, Moor et al., 2002, Raisch and O'Young, 1997, Raisch and O'Young, 1998), we combine techniques from J.C. WILLEMS' behavioural systems theory (Willems, 1989, Willems, 1991) and P.J. RAMADGE and W.M. WONHAM's supervisory control theory (Ramadge and Wonham, 1987, Ramadge and Wonham, 1989) to address the problem of supervisory controller synthesis for a fairly general class of hybrid systems and to establish an abstraction based solution procedure. The purpose of this section is to briefly summarize the consequences of (Moor and Raisch, 1999b, Moor et al., 2002) for the more specific case of sampled continuous systems with discrete-valued inputs and outputs; it is this class of plants that we will develop efficient abstraction procedures for in the following sections. While we need to provide an unambiguous framework for the abstraction step, technical aspects of the controller synthesis step are omitted and only an informal outline is given. For a detailed discussion, the reader is referred to (Moor and Raisch, 1999b, Moor et al., 2002).

Plant model. Consider the plant

$$x(k+1) = F(x(k),\, u(k)) \qquad \text{and} \qquad y(k) \in G(x(k))\,, \tag{1}$$

where

- the *input signal* $u\colon \mathbb{N}_0 \to U$ is a sequence of input symbols from the finite input alphabet U, $|U| \in \mathbb{N}$; [1]
- the *state trajectory* $x\colon \mathbb{N}_0 \to \mathbb{R}^n$ is a sequence of real-valued states;
- the *state transition map* $F\colon \mathbb{R}^n \times U \to \mathbb{R}^n$ uniquely determines the successor state from the current state and the current input symbol;
- the *measurement map* $G\colon \mathbb{R}^n \to 2^Y \setminus \{\emptyset\}$ models a quantized measurement of the continuous state; it is not required to be deterministic.
- the *output signal* $y\colon \mathbb{N}_0 \to Y$ is a sequence of measurement symbols from the finite output alphabet Y, $|Y| \in \mathbb{N}$.

[1] We denote the positive integers $\mathbb{N}$ and the non-negative integers $\mathbb{N}_0$. We use $|A| \in \mathbb{N}$ to indicate that A is a nonempty finite set.

This class of plant models includes a scenario of particular application relevance, namely sampled continuous dynamics with a discrete-valued input switching between a finite number of operation modes and a discrete-valued output being generated by measurement quantisation. Assuming a constant sampling period $\Delta > 0$, the state transition map is given by

$$F(\xi, \mu) := \Phi^{\mu}_{\Delta}(\xi)\,, \tag{2}$$

where for each $\mu \in U$ the map $\Phi^{\mu}_{t}\colon \mathbb{R}^n \to \mathbb{R}^n$, $t \in \mathbb{R}^+_0$, denotes the flow induced by a vector field $f_\mu\colon \mathbb{R}^n \to \mathbb{R}^n$; i.e. $z(t) = \Phi^{\mu}_{t}(z_0)$ solves the ODE

$$\dot{z}(t) = f_\mu(z(t)) \tag{3}$$

for the initial condition $z(0) = z_0$, and we assume unique existence of such a solution on the entire time axis. Note that if we were concerned with the system behaviour between given sampling instants, we could adopt our set-up to the case of event-driven sampling. In the latter case, the occurrence of events is entirely determined by the system (e.g., by elements of the continuous state vector z crossing certain thresholds) instead of being restricted to a fixed time grid. For linear dynamics, this case has been addressed in (Franke et al., 2000, Moor, 1998, Moor and Raisch, 1999a).

By allowing the measurement map G to be nondeterministic, the quantization cells

$$G^{-1}(\nu_j) \subseteq \mathbb{R}^n, \quad \nu_j \in Y, \quad j = 1, \ldots |Y|,$$

may cover (instead of partition) the continuous state space. This models the practically important case where measurement information is, to a certain extent, ambiguous.

Supervisory control. From the perspective of a potential controller, the system exhibits a discrete event behaviour: at the k-th sampling instant, the supervisor applies an input symbol $u(k) \in U$ and then waits for the next measurement symbol $y(k+1) \in Y$. Naturally, for the problem of controller synthesis, this *external behaviour* plays a key role. We formally define the external behaviour $\mathfrak{B}$ induced by (1) as

$$\mathfrak{B} := \{(u,\, y)\colon \mathbb{N}_0 \to U \times Y \mid \exists\, x\colon \mathbb{N}_0 \to \mathbb{R}^n : \text{Eq. (1) holds for all } k \in \mathbb{N}_0 \,\}\,; \tag{4}$$

i.e. $\mathfrak{B}$ denotes the set of all pairs of input and output signals on which the plant model (1) can possibly evolve. This definition is consistent with J.C. WILLEMS' behavioural systems theory, where a dynamical system is characterized by the set of trajectories that are compatible with the phenomenon it models.

Following the concepts of RAMADGE and WONHAM's supervisory control theory for DESs, the task of a supervisor is to restrict the plant behaviour $\mathfrak{B} \subseteq (U \times Y)^{\mathbb{N}_0}$ such that the closed loop is guaranteed to exhibit only acceptable signals. This specification can be formally represented by the set of acceptable external signals,

denoted $\mathfrak{B}_{\rm spec} \subseteq (U \times Y)^{\mathbb{N}_0}$. Similar to the plant, the supervisor is characterized by a behaviour $\mathfrak{B}_{\rm sup} \subseteq (U \times Y)^{\mathbb{N}_0}$, which denotes the set of external signals it can evolve on. The closed-loop behaviour is the intersection $\mathfrak{B}_{\rm cl} = \mathfrak{B} \cap \mathfrak{B}_{\rm sup}$, i.e. only those pairs of input and output signals "survive closing the loop" that are consistent with both plant and controller dynamics. The supervisor $\mathfrak{B}_{\rm sup}$ is said to *enforce the specification* $\mathfrak{B}_{\rm spec}$ if $\mathfrak{B}_{\rm cl} \subseteq \mathfrak{B}_{\rm spec}$. However, when interconnecting plant and supervisor one needs to ensure that the supervisor respects the input-output structure of the plant; i.e. the supervisor may enable or disable certain input events at any time but no restrictions must be imposed on the plant outputs. If the latter condition holds, $\mathfrak{B}_{\rm sup}$ is said to be *admissible* w.r.t. $\mathfrak{B}$; see (Moor and Raisch, 1999b) for a formal definition of admissibility. The problem of supervisory controller synthesis can then be stated as follows:

Given a plant behaviour $\mathfrak{B}$ and a specification $\mathfrak{B}_{\rm spec}$, a supervisor $\mathfrak{B}_{\rm sup}$ is said to be a solution to the supervisory control problem $(\mathfrak{B},\ \mathfrak{B}_{\rm spec})$ if (i) $\mathfrak{B}_{\rm sup}$ is admissible w.r.t. $\mathfrak{B}$, and (ii) $\mathfrak{B}_{\rm sup}$ enforces the specification.

Discrete abstractions. Suppose both $\mathfrak{B}$ and $\mathfrak{B}_{\rm spec}$ were realized by finite automata. Not surprisingly, the controller synthesis problem could then be treated by a slightly modified version of known methods from DES theory; e.g. (Ramadge and Wonham, 1989). For this case, efficient procedures are known which either compute a finite automaton realization of a solution $\mathfrak{B}_{\rm sup}$ or find that no such solution exists. However, the plant (1) is defined on the continuous state space $\mathbb{R}^n$, and a finite automaton realization of $\mathfrak{B}$ can only exist if $\mathbb{R}^n$ can be decomposed by a finite partition into sets of states that are indistinguishable under all external signals. This is a very restrictive condition and, in general, we can *not* assume that $\mathfrak{B}$ is realizable by a finite automaton. A method to overcome this problem is to first construct a finite automaton that *approximates* the hybrid plant and then to solve the synthesis problem for the approximation. Various variants of this approach have been discussed, e.g., in (Cury et al., 1998, Koutsoukos et al., 2000, Lunze et al., 1997, Philips et al., 1999, Raisch and O'Young, 1997, Raisch and O'Young, 1998). In (Moor and Raisch, 1999b, Moor et al., 2002), we justify this approximation based approach by providing a sufficient condition for a solution obtained at the approximation level to remain valid for the actual hybrid plant:

Consider a plant approximation $\mathfrak{B}_{\rm ca} \subseteq (U \times Y)^{\mathbb{N}_0}$, a specification $\mathfrak{B}_{\rm spec}$, and a solution $\mathfrak{B}_{\rm sup}$ of the supervisory control problem $(\mathfrak{B}_{\rm ca},\ \mathfrak{B}_{\rm spec})$. Assume that each behaviour $\mathfrak{B}_{\rm ca}$, $\mathfrak{B}_{\rm spec}$, $\mathfrak{B}_{\rm sup}$ is realized by a finite automaton. If $\mathfrak{B}_{\rm ca} \supseteq \mathfrak{B}$, then $\mathfrak{B}_{\rm sup}$ also solves $(\mathfrak{B},\ \mathfrak{B}_{\rm spec})$, where $\mathfrak{B}$ denotes the external behaviour of the plant model (1)*. See (Moor and Raisch, 1999b), Theorem 25, and (Moor et al., 2002), Sect. 6.*

Note that the nontriviality of this result is due to the requirement that any solution $\mathfrak{B}_{\rm sup}$ respects the input output structure of $\mathfrak{B}$. A plant approximation $\mathfrak{B}_{\rm ca}$ is said to

be a *discrete abstraction* of $\mathfrak{B}$, if (i) the behavioural inclusion $\mathfrak{B}_{\mathrm{ca}} \supseteq \mathfrak{B}$ is fulfilled, and (ii) $\mathfrak{B}_{\mathrm{ca}}$ is realizable by a finite automaton. The supervisory controller synthesis problem has thus been reduced to the construction of a discrete abstraction $\mathfrak{B}_{\mathrm{ca}} \supseteq \mathfrak{B}$ that is sufficiently accurate such that $(\mathfrak{B}_{\mathrm{ca}},\, \mathfrak{B}_{\mathrm{spec}})$ is solvable.

l-Complete approximation. In the case of time invariant systems, a particularly suitable discrete abstraction is the so called *strongest l-complete approximation* $\mathfrak{B}_l \supseteq \mathfrak{B}$, where $l \in \mathbb{N}$ is a parameter. Formally, $\mathfrak{B}_l$ can be characterized by

$$\mathfrak{B}_l := \{(u,y)\colon \mathbb{N}_0 \to U \times Y |\ (u,y)\big|_{[k,k+l]} \in \mathfrak{B}\big|_{[0,l]}\ \forall\, k \in \mathbb{N}_0\}\,, \tag{5}$$

where the restriction operator $(\,\cdot\,)|_{[k,k+l]}\colon (U \times Y)^{\mathbb{N}_0} \to (U \times Y)^{(l+1)}$ picks the finite string ranging from the k-th to the $(k+l)$-th pair of external events and discards its absolute location on the time axis:

$$(u,y)|_{[k,k+l]} := [\,(u(k),y(k)),\, \ldots\, (u(k+l),y(k+l))\,] \in (U \times Y)^{(l+1)}\,. \tag{6}$$

It can be naturally extended to sets of signals:

$$\mathfrak{B}|_{[0,l]} := \{(u,y)\big|_{[0,l]} \in (U \times Y)^{(l+1)} \mid (u,y) \in \mathfrak{B}\}\,. \tag{7}$$

Note that $\mathfrak{B}|_{[0,l]}$ is a finite set as both U and Y are finite. The most relevant features of the strongest l-complete approximation $\mathfrak{B}_l$ are that (i) accuracy is monotone in l, i.e. $\mathfrak{B}_l \supseteq \mathfrak{B}_{l+1} \supseteq \mathfrak{B}$, and that (ii) a finite realization can be easily derived from the restricted plant behaviour $\mathfrak{B}|_{[0,l]}$; see (Moor and Raisch, 1999b), Corollary 11. Hence, there is no need to evaluate (5) in order to construct $\mathfrak{B}_l$. All that remains to be done is the computation of $\mathfrak{B}|_{[0,l]}$ and we recall the following iterative procedure from (Moor and Raisch, 1999b):

Theorem 1. *Let $\mathfrak{B} \subseteq (U \times Y)^{\mathbb{N}_0}$ denote the external behaviour of* (1)*. For $(u,\, y) \in (U \times Y)^{\mathbb{N}_0}$ and $l \in \mathbb{N}_0$, iteratively define the sets of states $\mathcal{X}((u,y)|_{[0,l]}) \subseteq \mathbb{R}^n$ that are compatible with the strings $(u,y)|_{[0,l]}$:*

$$\mathcal{X}((u,y)\big|_{[0,0]}) := G^{-1}(y(0))\,, \tag{8a}$$

$$\mathcal{X}((u,y)\big|_{[0,\lambda+1]}) := F(\mathcal{X}((u,y)\big|_{[0,\lambda]}),\, u(\lambda)) \cap G^{-1}(y(\lambda+1))\,, \tag{8b}$$

for $\lambda = 0, \ldots l-1$. Then,

$$(u,y)\big|_{[0,l]} \in \mathfrak{B}\big|_{[0,l]} \quad\Longleftrightarrow\quad \mathcal{X}((u,y)|_{[0,l]}) \neq \emptyset\,. \tag{9}$$

According to the above theorem, $\mathfrak{B}|_{[0,l]}$ can be established via a finite iteration of images under F and intersections with the quantization cells G^{-1}. Then, the methods presented in (Moor and Raisch, 1999b, Moor et al., 2002) allow the construction of a discrete abstraction of the hybrid plant and finally the synthesis of a supervisory controller.

While this approach has been successfully applied to a number of examples, there are two major limitations from a practical point of view. First, for nonlinear continuous dynamics, images of sets of states under F can, in general, not be computed efficiently. Roughly speaking, one is often left with the simulation of an exhaustive number of initial conditions $\xi_0 = x(0)$; it is then naively assumed that $\mathcal{X}((u,y)|_{[0,l]}) = \emptyset$ whenever no $\xi_0 \in \mathcal{X}((u,y)|_{[0,l]})$ can be found. Clearly, this implies the risk of omitting a particular string from $\mathfrak{B}|_{[0,l]}$, hence from $\mathfrak{B}_{\mathrm{ca}} = \mathfrak{B}_l$, therefore violating the requirement $\mathfrak{B}_{\mathrm{ca}} \supseteq \mathfrak{B}$. Second, for high dimensional continuous dynamics, a reasonably accurate quantization leads to computationally intractable output alphabets Y. In the following two sections, we identify a broad class of hybrid systems where the above iterative procedure can be refined in order to gain substantial computational efficiency.

3 Discrete Abstractions for Monotone Systems

For *monotone dynamical systems* (see (Smith, 1995) for a comprehensive treatment of the subject), it is possible to efficiently estimate the sets of compatible states $\mathcal{X}((u,y)|_{[0,l]})$ and to derive a discrete abstraction from those estimates. In general, monotonicity is defined with respect to an arbitrary partial order. In this paper, we consider the specific partial order $\preccurlyeq$ which, for $a, b \in \mathbb{R}^n$, is defined by

$$a \preccurlyeq b \quad :\Longleftrightarrow \quad \forall\, i \in \{1, \ldots n\} :\ a_i \leq b_i. \tag{10}$$

Hence, $a \preccurlyeq b$ if and only if $b - a$ lies in the nonnegative convex cone $\mathbb{R}^n_+ := \{\xi \in \mathbb{R} | \xi \geq 0\}^n$.

Definition 1. The map $g : \mathbb{R}^q \to \mathbb{R}^n$ is called *order preserving* if $a \preccurlyeq b$ implies $g(a) \preccurlyeq g(b)$.

Note that a map is order preserving if all its partial derivatives are nonnegative. The image of a *box*

$$Q(a,b) := \{c |\ a \preccurlyeq c \preccurlyeq b\} \tag{11}$$

under an order preserving map g can be efficiently over-approximated via the images of a and b, i.e. $g(Q(a,b)) \subseteq Q(g(a), g(b))$. It is this property that allows efficient approximation of monotone systems.

In the following, we consider dynamical systems

$$\dot{z}(t) = f(z(t)) \tag{12}$$

and assume that, for any initial condition $z(0) = z_0$, there exists a unique solution $\Phi_t(z_0)$ for all $t \geq 0$. The dynamical system (12) is called *monotone*, if ordered states remain ordered under the progress of time:

Definition 2. The dynamical system (12) is *monotone*, if the flow $\Phi_t \colon \mathbb{R}^n \to \mathbb{R}^n$ induced by the vector field $f \colon \mathbb{R}^n \to \mathbb{R}^n$ is order preserving for all $t \geq 0$.

A monotonicity test can be stated in terms of the off-diagonal entries of the Jacobian of f:

Theorem 2. *(see e.g. (Smith, 1995)) The dynamical system $\dot{z} = f(z)$ is monotone if*

$$\frac{\partial f_i}{\partial z_j} \geq 0 \quad \forall i \neq j\,. \tag{13}$$

As an example, consider a linear system $\dot{z}(t) = A\,z(t)$. If all eigenvalues of A lie in $\mathbb{R}$, then there exists a real linear transformation that transforms A in its Jordan normal form. Clearly, the transformed system is monotone by Theorem 2. For further illustration, Fig. 1 shows two state trajectories $z(t)$ and $\hat{z}(t)$ of the monotone system $\dot{z}(t) = \left(\begin{smallmatrix} -1 & 1 \\ 0 & -1 \end{smallmatrix}\right) z(t)$. For the respective initial conditions $z(0) = (0,\, -1.2)^\intercal$ and $\hat{z}(0) = (0.2,\, -1)^\intercal$ we have $z(0) \preccurlyeq \hat{z}(0)$, and hence, by monotonicity, $z(t) \preccurlyeq \hat{z}(t)$ for all $t \geq 0$. This is confirmed by Fig. 1, which also clarifies that monotonicity of a dynamical system must not be confused with monotonicity of individual components of state trajectories: in the example, $z_1(t)$ and $\hat{z}_1(t)$ clearly fail to be monotonously increasing (or decreasing) as functions of t.

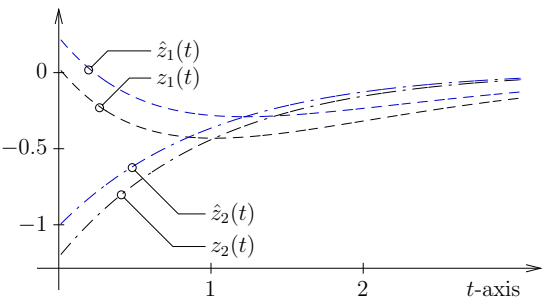

Fig. 1. State trajectories of a linear monotone system.

In consequence, for monotone systems, there is no need to integrate a huge number of states. Instead, the temporal evolution of a box $Q(\zeta_a, \zeta_b)$ can be over-approximated by evaluating the flow for the two points ζ_a, ζ_b only: $\Phi_t(Q(\zeta_a, \zeta_b)) \subseteq Q(\Phi_t(\zeta_a), \Phi_t(\zeta_b))$. Clearly, this is independent of the state dimension.

We now turn to the discrete abstraction of the hybrid plant model (1), with sampled continuous dynamics (3). Obviously, during each sampling interval, the continuous dynamics depends on a fixed control symbol $\mu \in U$. Under the assumption that the continuous system (3) is monotone for each $\mu \in U$, it immediately follows that the transition function $F(\,\cdot\,,\,\mu)$ defined in (2) is order preserving. We further assume that measurement symbols ν_j, $j = 1, \ldots, p$, correspond to bounded boxes in $\mathbb{R}^n$, i.e.

$$G^{-1}(\nu_j) = Q(a_j, b_j), \quad a_j, b_j \in \mathbb{R}^n,\ a_j \preccurlyeq b_j\,. \tag{14}$$

Obviously, a finite number of bounded boxes (14) can not cover the entire $\mathbb{R}^n$. Hence, we need an additional *out of range symbol* $\ddagger$ with

$$G^{-1}(\ddagger) = \mathbb{R}^n \setminus \bigcup_{1\le j\le p} G^{-1}(\nu_j)\,, \quad \text{to give} \quad Y = \{\nu_1, \ldots, \nu_p\} \cup \{\ddagger\}\,. \tag{15}$$

Based on the iteration (8a), (8b), we are now in a position to provide easily computable *conservative estimates* $\hat{\mathcal{X}}((u,y)|_{[0,l]}) \subseteq \mathbb{R}^n$ for the sets of compatible states. Using

$$\hat{F}(Q(a,b),\,\mu) := Q(F(a,\mu), F(b,\mu))$$

as an over-approximation of the continuous evolution of a box $Q(a,b)$ under the order preserving flow Φ^{μ}_{Δ}, we define:

- if $y(0) = \nu_j \neq \ddagger$ for some j, let

$$\hat{\mathcal{X}}((u,y)\big|_{[0,0]}) := G^{-1}(\nu_j)\,; \tag{16}$$

- if $y(0) = \ddagger$, let

$$\hat{\mathcal{X}}((u,y)\big|_{[0,0]}) := \mathbb{R}^n\,. \tag{17}$$

And, for $\lambda = 0, \ldots l-1$:

- if $y(\lambda+1) \neq \ddagger$ and $\hat{\mathcal{X}}((u,y)\big|_{[0,\lambda]}) \neq \mathbb{R}^n$, let

$$\hat{\mathcal{X}}((u,y)\big|_{[0,\lambda+1]}) := \hat{F}(\hat{\mathcal{X}}((u,y)\big|_{[0,\lambda]}),\, u(\lambda)) \cap G^{-1}(y(\lambda+1))\,; \tag{18}$$

- if $y(\lambda+1) \neq \ddagger$ and $\hat{\mathcal{X}}((u,y)\big|_{[0,\lambda]}) = \mathbb{R}^n$, let

$$\hat{\mathcal{X}}((u,y)\big|_{[0,\lambda+1]}) := G^{-1}(y(\lambda+1))\,; \tag{19}$$

- if $y(\lambda+1) = \ddagger$ and $\hat{\mathcal{X}}((u,y)\big|_{[0,\lambda]}) \neq \mathbb{R}^n$
  and $\hat{F}(\hat{\mathcal{X}}((u,y)\big|_{[0,\lambda]}),\, u(\lambda)) \not\subseteq \cup_{1\le j\le p} G^{-1}(\nu_j)$, let

$$\hat{\mathcal{X}}((u,y)\big|_{[0,\lambda+1]}) := \hat{F}(\hat{\mathcal{X}}((u,y)\big|_{[0,\lambda]}),\, u(\lambda))\,; \tag{20}$$

- if $y(\lambda+1) = \ddagger$ and $\hat{\mathcal{X}}((u,y)\big|_{[0,\lambda]}) \neq \mathbb{R}^n$
  and $\hat{F}(\hat{\mathcal{X}}((u,y)\big|_{[0,\lambda]}),\, u(\lambda)) \subseteq \cup_{1\le j\le p} G^{-1}(\nu_j)$, let

$$\hat{\mathcal{X}}((u,y)\big|_{[0,\lambda+1]}) := \emptyset\,; \tag{21}$$

- if $y(\lambda+1) = \ddagger$ and $\hat{\mathcal{X}}((u,y)\big|_{[0,\lambda]}) = \mathbb{R}^n$, let

$$\hat{\mathcal{X}}((u,y)\big|_{[0,\lambda+1]}) := \mathbb{R}^n\,. \tag{22}$$

Note that (16)–(22) iteratively define the sets $\hat{\mathcal{X}}((u,y)|_{[0,l]})$ for all external signals $(u,y) \in (U \times Y)^{\mathbb{N}_0}$ and for all $l \in \mathbb{N}_0$: (16) and (17) define $\hat{\mathcal{X}}((u,y)|_{[0,0]})$ while (18)–(22) systematically define $\hat{\mathcal{X}}((u,y)|_{[0,\lambda+1]})$ in terms of $\hat{\mathcal{X}}((u,y)|_{[0,\lambda]})$. Note also that $\hat{F}$ is only applied to bounded boxes. By construction, the sets $\hat{\mathcal{X}}((u,y)|_{[0,l]})$ are guaranteed to be supersets of the sets of compatible states $\mathcal{X}((u,y)|_{[0,l]})$. Formally:

Proposition 1. *Assume that for each $\mu \in U$ the state transition map $F(\,\cdot\,,\mu)$ is order preserving and the output map G is defined by* (14)–(15)*. Then, for all external signals $(u,y) \in (U \times Y)^{\mathbb{N}_0}$ and for all $l \in \mathbb{N}_0$ the following inclusion holds:*

$$\hat{\mathcal{X}}((u,y)\big|_{[0,l]}) \supseteq \mathcal{X}((u,y)\big|_{[0,l]})\,. \tag{23}$$

Proof. Pick an arbitrary external signal $(u,y) \in (U \times Y)^{\mathbb{N}_0}$. For $l = 0$ the claim follows immediately from (16) and (17). For $l \neq 0$, the proof is by induction w.r.t. $\lambda = 0, \ldots l-1$: we assume $\hat{\mathcal{X}}((u,y)|_{[0,\lambda]}) \supseteq \mathcal{X}((u,y)|_{[0,\lambda]})$ and show in each of the cases corresponding to (18)–(22) that $\hat{\mathcal{X}}((u,y)|_{[0,\lambda+1]}) \supseteq \mathcal{X}((u,y)|_{[0,\lambda+1]})$. First, observe that for the cases (19) and (22) the inclusion

$$\hat{\mathcal{X}}((u,y)|_{[0,\lambda+1]}) \supseteq \mathcal{X}((u,y)|_{[0,\lambda+1]})$$

follows immediately. For the remaining cases, note that, by monotonicity,

$$\hat{F}(Q(a,b),\mu) \supseteq F(Q(a,b),\mu)$$

holds for any $a,\ b \in \mathbb{R}^n$, $\mu \in U$. Hence,

$$\hat{F}(\hat{\mathcal{X}}((u,y)|_{[0,\lambda]},u(\lambda)) \supseteq F(\mathcal{X}((u,y)|_{[0,\lambda]},u(\lambda)).$$

For the case (18) one obtains

$$\hat{\mathcal{X}}((u,y)|_{[0,\lambda+1]}) \supseteq F(\mathcal{X}((u,y)|_{[0,\lambda]}),\ u(\lambda)) \cap G^{-1}(y(\lambda+1)) = \mathcal{X}((u,y)|_{[0,\lambda+1]}).$$

The same argument resolves case (20). Only case (21) remains. From condition $\hat{F}(\hat{\mathcal{X}}((u,y)|_{[0,\lambda]}),\ u(\lambda)) \subseteq \cup_{1\leq j\leq p} G^{-1}(\nu_j)$ one obtains

$$F(\mathcal{X}((u,y)|_{[0,\lambda]}),\ u(\lambda)) \subseteq \cup_{1\leq j\leq p} G^{-1}(\nu_j).$$

Together with (15), this implies $F(\mathcal{X}((u,y)|_{[0,\lambda]}),\ u(\lambda)) \cap G^{-1}(\ddagger) = \emptyset$, and, hence,

$$\mathcal{X}((u,y)|_{[0,\lambda+1]}) = \emptyset = \hat{\mathcal{X}}((u,y)|_{[0,\lambda+1]}).$$

Remark 1. The assumption of quantization boxes instead of more general (bounded) quantization sets does not imply any loss of generality: in the latter case, we would simply replace $G^{-1}(\ldots)$ by $Q(\inf G^{-1}(\ldots), \sup G^{-1}(\ldots))$ in the above iteration (16)–(22).

As an immediate consequence of Proposition 1, we obtain a finite abstraction $\mathfrak{B}_{\mathrm{ca}}$.

Corollary 1. *Under the same hypothesis as in Proposition 1, the following inclusions hold:*

$$\hat{\mathfrak{B}}\big|_{[0,l]} := \left\{(u,y)\big|_{[0,l]} \mid \hat{\mathcal{X}}((u,y)\big|_{[0,l]}) \neq \emptyset\right\} \supseteq \mathfrak{B}\big|_{[0,l]}\,, \tag{24}$$

$$\mathfrak{B}_{\mathrm{ca}} := \{(u,y)|\ (u,y)\big|_{[k,k+l]} \in \hat{\mathfrak{B}}\big|_{[0,l]}\ \forall\, k \in \mathbb{N}_0\} \supseteq \mathfrak{B}_l \supseteq \mathfrak{B}\,. \tag{25}$$

A finite realization of $\mathfrak{B}_{\mathrm{ca}}$ can now be constructed in the same manner as for $\mathfrak{B}_l$, see (Moor et al., 2002, Moor and Raisch, 1999b), – we merely have to replace $\mathfrak{B}\big|_{[0,l]}$ by $\hat{\mathfrak{B}}\big|_{[0,l]}$. This completes the discrete abstraction procedure for monotone dynamical systems. Note that we do not assume linearity; our results are therefore applicable to nonlinear monotone dynamics.

4 Handling High-Order Dynamics

Many complex technical processes, although intrinsically high-dimensional, converge to a low-dimensional manifold within a short time. Distillation columns are a well-known example: a first principles modelling approach leads to a large number of ODEs describing the temporal evolution of concentrations on each tray of the column. When a column is operated, however, these concentrations stop to be arbitrary and form a concentration profile that can be described by very few parameters.

This particular structure can be exploited in the following way: instead of quantizing the high-dimensional plant state space, only a well defined neighbourhood of the relevant part of the respective manifold is covered by quantization cells and hence provides measurement information; the "rest" of the state space returns the out of range symbol "‡". For a formal treatment of this idea, let

$$h_\mu : \mathbb{R}^q \to \mathbb{R}^n,\ q < n, \tag{26}$$

represent a continuously differentiable parametrization of a q-dimensional manifold $\mathcal{M}_\mu$ in $\mathbb{R}^n$, i.e. $\mathcal{M}_\mu = h_\mu(\mathbb{R}^q)$. Naturally, both the manifold and its parametrization may depend on the control symbol μ. Assume h_μ to be order preserving and $\mathcal{M}_\mu$ to be attractive, i.e.

$$\lim_{t\to\infty} \operatorname{dist}(\mathcal{M}_\mu,\, \Phi_t^\mu(z_0)) = 0\,, \tag{27}$$

for all initial conditions $z_0 \in \mathbb{R}^n$, where

$$\operatorname{dist}(X,\zeta) := \inf\{\|\zeta - \xi\| \mid \xi \in X\} \tag{28}$$

denotes the distance of a point $\zeta \in \mathbb{R}^n$ to a set $X \subseteq \mathbb{R}^n$ w.r.t. some norm $\|\cdot\|$. Let the bounded subset $P \subset \mathbb{R}^q$ represent the relevant operating range on $\mathcal{M}_\mu$ and, for a given $\delta > 0$,

$$\mathcal{V}_\delta(h_\mu(P)) := \{\zeta \mid \operatorname{dist}(h_\mu(P),\zeta) < \delta\} \tag{29}$$

the neighbourhood of $h_\mu(P)$ that is to be covered by quantization cells.

We give an explicit formula for quantisation cells covering $\mathcal{V}_\delta(h_\mu(P))$ for the case where the operators dist$(\,\cdot\,)$ and $\mathcal{V}_\delta(\,\cdot\,)$ refer to the so called weighted infinity norm; i.e. $\|\,\cdot\,\| := \|\,\cdot\,\|_\infty^\beta$ with $\|\xi\|_\infty^\beta := \max_i |\beta_i \xi_i|$ for the weighting vector $\beta = (\beta_1, \ldots \beta_n)^\intercal$. Subject to the constraints $\beta_i > 0$, $\sum \beta_i/n = 1$, the weights β may be chosen arbitrarily but are assumed to be fixed for the scope of this paper. Note that the closure of a neighbourhood of a bounded box w.r.t. $\|\,\cdot\,\|_\infty^\beta$ is again a bounded box:

$$\overline{\mathcal{V}}_\delta(Q(a,b)) = Q(a - \delta\beta^{-1}, b + \delta\beta^{-1})\,, \tag{30}$$

where $\beta^{-1} := (\beta_1^{-1}, \ldots \beta_n^{-1})^\intercal$, and $\overline{\mathcal{V}}_\delta(X)$ denotes the closure of $\mathcal{V}_\delta(X)$. The *diameter* of a box w.r.t. $\|\,\cdot\,\|_\infty^\beta$ is defined by

$$\operatorname{diam}(Q(a,b)) := \sup\{\|\xi - \zeta\|_\infty^\beta \mid \xi, \zeta \in Q(a,b)\} = \|a - b\|_\infty^\beta\,. \tag{31}$$

Given a finite a number of (q-dimensional) boxes covering P – they are referred to as *parameter cells* – we define the (n-dimensional) measurement quantisation cells by

$$P \subseteq \bigcup_{1 \le j \le p_\mu} Q(a_j, b_j) \;=:\; \hat{P} \subset \mathbb{R}^q\,, \quad a_j, b_j \in \mathbb{R}^q\,, \tag{32}$$

$$G^{-1}(\nu_j^\mu) := Q(h_\mu(a_j) - \delta\beta^{-1}, h_\mu(b_j) + \delta\beta^{-1}) \subset \mathbb{R}^n\,. \tag{33}$$

This is illustrated in Fig. 2, where, for simplicity, dependence on μ has been omitted and all β_i are equal. Then, as required, the quantisation cells cover $\mathcal{V}_\delta(h_\mu(P))$. Furthermore, referring to a Lipschitz constant of h_μ, the diameter of the parameter cells can be chosen such that the measurement quantisation cells meet a given accuracy requirement, i.e. the measurement cells do not exceed a given maximum diameter. Formally, this can be stated as follows:

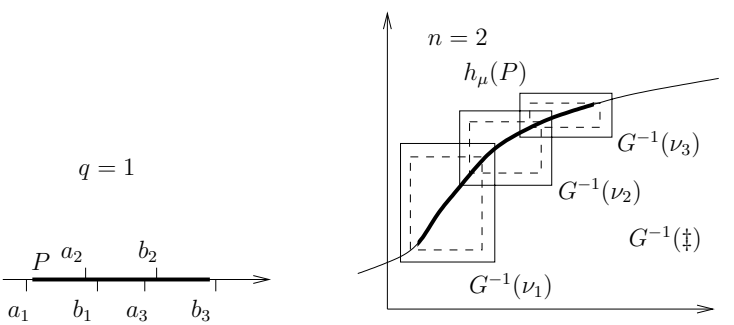

Fig. 2. Quantization of neighbourhood of $h_\mu(P)$.

Proposition 2. *Given the order preserving and continuously differentiable map* $h_\mu : \mathbb{R}^q \to \mathbb{R}^n$*, let* $L > 0$ *denote a Lipschitz constant w.r.t.* $\|\cdot\|_\infty^\beta$ *for* h_μ *on the domain* $\hat{P} \subset \mathbb{R}^q$*. Then* $\operatorname{diam}(G^{-1}(\nu_j^\mu)) \leq L \operatorname{diam}(Q(a_j, b_j)) + 2\delta$*. Let* γ *denote the maximum diameter of the parameter cells in the finite cover* (32)*. Then*

$$\overline{\mathcal{V}}_{\delta+\gamma L}(h_\mu(\hat{P})) \quad \supseteq \quad \bigcup_{1\leq j\leq p_\mu} G^{-1}(\nu_j^\mu) \quad \supseteq \quad \mathcal{V}_\delta(h_\mu(P))\,. \tag{34}$$

Proof. The existence of a Lipschitz constant L is ensured by continuous differentiability of h_μ and boundedness of $\hat{P}$. As an immediate consequence, observe $\operatorname{diam}(\, Q(h_\mu(a_j),\, h_\mu(b_j))\,) \leq L \operatorname{diam}(Q(a_j, b_j))$. By the triangle inequality, we obtain

$$\operatorname{diam}(G^{-1}(\nu_j^\mu)) \leq L \operatorname{diam}(Q(a_j, b_j)) + 2\delta.$$

To show the first of the two inclusions in (34), pick an arbitrary point

$$\xi \in \cup_{1\leq j\leq p_\mu} G^{-1}(\nu_j^\mu)$$

and an integer j such that $\xi \in \overline{\mathcal{V}}_\delta(\, Q(h_\mu(a_j),\, h_\mu(b_j))\,)$. Hence, there exists a point $\zeta \in Q(h_\mu(a_j),\, h_\mu(b_j))$ with $\|\xi - \zeta\|_\infty^\beta \leq \delta$. Obviously, $Q(h_\mu(a_j),\, h_\mu(b_j))$ has a nonempty intersection with $h_\mu(\hat{P})$, and therefore

$$\operatorname{dist}(h_\mu(\hat{P}),\, \zeta) \leq \operatorname{diam}(\, Q(h_\mu(a_j),\, h_\mu(b_j))\,) \leq \gamma L.$$

This implies $\operatorname{dist}(h_\mu(P),\, \xi) \leq \delta + \gamma L$. Hence, $\xi \in \overline{\mathcal{V}}_{\delta+L\gamma}(h_\mu(P))$, completing the proof of the first inclusion in (34). To show the second inclusion, take any $\zeta \in \mathcal{V}_\delta(h_\mu(P))$. Then there exists a $p \in P$, $\xi := h_\mu(p)$, such that $\|\xi - \zeta\|_\infty^\beta < \delta$. By (32), we can find a j such that $p \in Q(a_j, b_j)$. As h_μ is order preserving, this implies $\xi = h_\mu(p) \in Q(h_\mu(a_j),\, h_\mu(b_j))$. Hence, $\zeta \in \mathcal{V}_\delta(Q(h_\mu(a_j),\, h_\mu(b_j))$, and, by (30), $\zeta \in G^{-1}(\nu_j^\mu)$. This proves the second inclusion in (34).

The part of $\mathbb{R}^n$ not covered by any of the cells $G^{-1}(\nu_j^\mu)$, $j = 1, \ldots p_\mu$, $\mu \in U$, again returns the out of range symbol ‡, i.e.

$$G^{-1}(‡) := \mathbb{R}^n \setminus \bigcup_{1\leq j\leq p_\mu,\ \mu\in U} G^{-1}(\nu_j^\mu)\,, \tag{35}$$

such that the set of measurement symbols is given by

$$Y := \bigcup_{\mu\in U} \{\nu_1^\mu, \ldots, \nu_{p_\mu}^\mu\} \cup \{‡\}\,. \tag{36}$$

This concludes the construction of a measurement quantization based on lower dimensional attractive manifolds. The reduction of the number of required quantization cells is quite significant. If, for example, one was to cover a bounded subset of $\mathbb{R}^n$ by cells not exceeding a certain diameter $\varrho > 0$, the number of required cells

would be of the order $\mathcal{O}(1/\varrho^n)$. By the above method, only $\mathcal{O}(|U|/\varrho^q)$ cells are necessary to cover the corresponding portion of the manifolds $\mathcal{M}_\mu$, $\mu \in U$.

A discrete abstraction can again be obtained via Theorem 1 or, assuming monotonicity of the system dynamics, by Corollary 1, and a supervisor that is synthesized for the abstraction is guaranteed to enforce the specification for the original hybrid plant. While we have significantly reduced the number of cells, the dimension of each individual cell $G^{-1}(\nu_j^\mu)$ is not affected and the propagation over time of each such cell is with respect to the full-dimensional dynamics. As indicated, the manifold $\mathcal{M}_\mu$ may very well depend on the input symbol μ and Theorem 1 (or Corollary 1) still ensures the crucial inclusion $\mathfrak{B}_{\mathrm{ca}} \supseteq \mathfrak{B}$. Note that neither Theorem 1 nor Corollary 1 refer to the attractiveness of $\mathcal{M}_\mu$ and therefore the respective statements remain true even if $\mathcal{M}_\mu$ fails to be attractive. From the construction of the measurement quantization, however, the discrete abstraction $\mathfrak{B}_{\mathrm{ca}}$ can only be expected to be reasonably accurate if changes in the input signal only occur when the state trajectory evolves within $\mathcal{V}_\delta(h_\mu(P))$. If the state trajectory does *not* approach $\mathcal{V}_\delta(h_\mu(P))$, the resulting abstraction will not purvey sufficient information on the underlying plant dynamics and we can not expect that a nontrivial specification can be enforced for the abstraction.

Given a continuous system (3), a constructive proof for the existence of an attractive manifold $\mathcal{M}_\mu$, in general, is a nontrivial problem. However, in contrast to hybrid controller synthesis, non-linear stability analysis refers exclusively to continuous dynamics and has been discussed in depth for many application relevant ODEs. In Sect. 5, we give an example of a chemical process that demonstrates how our hyrid controller synthesis framework benefits from a rich knowledge base regarding the non-linear process dynamics. A class of hybrid control problems for which an attractive manifold $\mathcal{M}_\mu$ is readily known to exist occurs in hierarchical control architectures, in which a continuous plant is subject to a number of alternative *low-level* continuous controllers; see (Moor et al., 2001b). In this configuration, a *high-level* discrete input symbol $\nu \in U$ implements the activation of the respective low-level controller. In particular, for each μ the system (3) represents a continuous closed-loop model, which in many applications is required to exhibit stable state components by any resonable design objective. Again, the enforcement of such low-level design objectives refers to continuous dynamics only and for the solution of these control problems one can draw from the literature on non-linear control.

5 Start-Up of a Distillation Column

We consider a distillation column in pilot plant scale which is operated at the Institut für Systemdynamik und Regelungstechnik in Stuttgart. It is about 10 m high, and consists of 40 bubble cap trays (consecutively numbered by $i = 2, \ldots, 41$ from bottom to top), a reboiler ($i = 1$) and a condenser ($i = 42$), see Fig. 3. Feed is supplied on tray 21. Our application example is the separation of methanol and propanol.

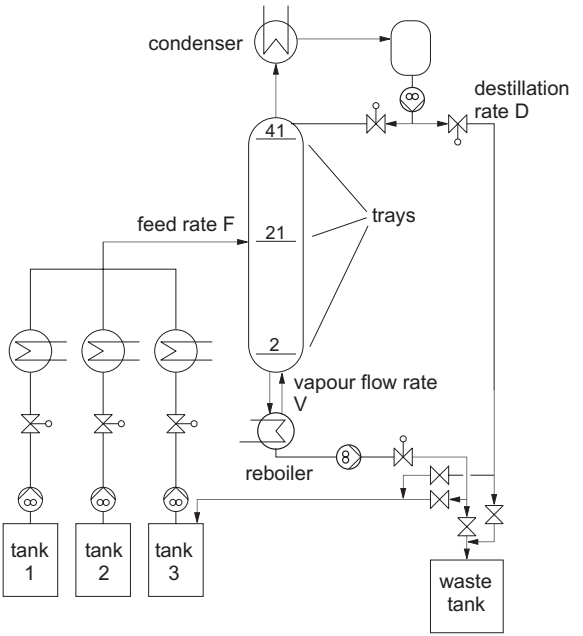

Fig. 3. Distillation column

The following steps can be distinguished during conventional column start-up: initially, the column trays are partially filled with liquid mixture from the previous experimental run. Further feed is added, and the column is heated up until boiling point conditions are established in the whole column. During this start-up step, the column is operated at total reflux and reboil. At the end of this step, a single concentration front is established. The position of this front depends on the initial concentration and varies from experiment to experiment. In a second step, the feed F, and the control inputs (distillate and vapour flow rate, D and V) are adjusted to their desired steady state values, and the initial front splits into two fronts. Then, in a third step, the two fronts move *very* slowly towards their steady state. We try to speed up the third step of the start-up procedure by introducing a suitable supervisory control strategy. The starting point for our approximation based controller synthesis is a continuous distillation column plant model which incorporates the following assumptions, which are well justified during the third step of the start-up: constant molar overflows, constant molar liquid holdups, negligible vapour holdups, total condenser, constant relative volatilities, a tray efficiency of one. Therefore, the model is based on material balances only and consists of one nonlinear first-order ODE for each tray, the reboiler, and the condenser (Klein et al., 1999):

$$n_L^i \dot{x}_i = F_L^{i+1} x_{i+1} - F_L^i x_i + F_V^{i-1} y_{i-1} - F_V^i y_i + \begin{cases} F x^F & \text{if } i = 21\,, \\ 0 & \text{else,} \end{cases} \tag{37a}$$

$$y_i = x_i \frac{\alpha}{1 + x_i(\alpha - 1)}\,, \tag{37b}$$

where x_i and y_i are the methanol mole fractions in the liquid and in the vapour on the i-th tray ($i = 2, \ldots, 41$), in the condenser ($i = 42$) and the reboiler ($i = 1$); $\alpha = 2.867$ is the relative volatility; $x^F = 0.32$ is the methanol mole fraction in the feed; F_L^i denotes the liquid molar flow rate, F_V^i the vapour flow rate and n_L^i the molar liquid holdup. Numerical values for the latter are given in Table 1. The table also states how F_L^i and F_V^i depend on F, D and V (feed, distillate and vapour flow rate).

Table 1. Flow rates and liquid holdups

	i	F_L^{i+1}	F_L^i	F_V^{i-1}	F_V^i	n_L^i [mol]
condenser	42	0	V	V	0	1.922
stripping	22-41	$V - D$	$V - D$	V	V	1.922
feed tray	21	$V - D$	$F + V - D$	V	V	1.922
rectifying	2-20	$F + V - D$	$F + V - D$	V	V	1.922
reboiler	1	$F + V - D$	$F - D$	0	V	135

The feed flow rate is considered to be constant at $F = 220.0$ mol/h, while D and V are control inputs. For any constant D and V, the system (37a), (37b) has an attractive equilibrium $x^*(D, V)$, which, for the nominal inputs $D_0 = 70.4$ mol/h and $V_0 = 188.2$ mol/h, corresponds to the desired operating point $x_0^* := x^*(D_0, V_0)$ of the distillation column. To speed up the process of approaching x_0^*, we look for a controller that switches between a finite number of constant input values. Considering only values $V > 0$, $D > 0$ such that $F + V - D \geq 0$, monotonicity of (37a), (37b) follows from the criterion given in Theorem 2.

The construction of lower dimensional manifolds $\mathcal{M}_\mu$, which is vital for approximation based discrete control, is based on *wave propagation theory* (Kienle, 2000); it considers particular concentration profiles as waves and discusses their propagation in time and space. Each wave is of the form

$$x_i = p_1 + \frac{p_2 - p_1}{1 + e^{\varrho(i-s)}}\,, \tag{38}$$

where p_1 and p_2 are the asymptotic values of the methanol mole fraction at the bottom and at the top of the wave, s is the so called wave position (point of inflexion) and ϱ is the slope at s. The aspect of wave propagation theory most relevant to our discussion is that during the third startup step, the concentration profile can be represented by two waves of the type (38), one each in the stripping ($1 \leq i \leq 21$) and the rectifying section ($21 < i \leq 42$). Their slopes can be approximated reasonably well by the slopes corresponding to the equilibrium $x^*(D, V)$. For the nominal inputs D_0 and V_0, the slopes turn out to be $\varrho_s = 0.465$ and $\varrho_r = 0.572$ for the stripping section and the rectifying section, respectively. Neglecting the effect of different inputs to

the slopes, the lower dimensional manifold under construction becomes independent of the input symbol. If we further assume constant methanol mole fractions in the reboiler and condenser, $x_1 = 0$ and $x_{42} = 1$, the asymptotic values in (38) are uniquely determined by the feed concentration x_{21} and the wave positions $\hat{s}_s$ and $\hat{s}_r$ for the stripping and rectifying section, respectively. [2] Consequently, the wave fronts of interest are parametrized by a map $h\colon \mathbb{R}^3 \to \mathbb{R}^{42}$ mapping parameter triples $(x_{21},\, \hat{s}_s,\, \hat{s}_r)$ to concentration profiles in the high dimensional state space. The i-th component h_i of h evaluates to

$$h_i(x_{21},\, \hat{s}_s,\, \hat{s}_r) := x_{21}\,[\,(1-e^{(i-1)\varrho_s})\,(1+e^{(\hat{s}_s-1)\varrho_s})\,] \times [\,(1-e^{20\,\varrho_s})\,(1+e^{(i-22+\hat{s}_s)\varrho_s})\,]^{-1} \quad (39)$$

for $1 \le i \le 21$, and

$$h_i(x_{21},\, \hat{s}_s,\, \hat{s}_r) := [\,x_{21}\,(e^{21\varrho_r} - e^{(i-63+\hat{s}_r)\varrho_r}) + (1-x_{21})\,(e^{(\hat{s}_r-21)\varrho_r} - e^{(i-21)\varrho_r}) + e^{(i-42+\hat{s}_r)\varrho_r} - 1\,] \times [\,(e^{21\varrho_r}-1)\,(e^{(i-63+\hat{s}_r)\varrho_r}+1)\,]^{-1} \quad (40)$$

for $22 \le i \le 42$. Note that all partial derivatives of h are non-negative. Hence, h is order preserving. This completes the construction of $\mathcal{M} \equiv \mathcal{M}_\mu := h(\mathbb{R}^3)$.

We now specify the operating range of the supervisor. For our particular setting, the equilibrium x_0^* corresponds to the parameter triple $x_{21} \approx 0.318$, $\hat{s}_s \approx 10.7$, $\hat{s}_r \approx 28.7$. The bounded box of parameters $P = [0.300,\, 0.340] \times [4.0,\, 20.0] \times [23.0,\, 37.0]$ is considered a reasonably large operation range, which we partition by $p = 139$ parameter cells $Q(a_j, b_j)$, $1 \le j \le p$. The high dimensional measurement quantization cells are then constructed by (33) with $\delta = 0.002$. Input symbols $U = \{\mu_1, \ldots \mu_9\}$ are chosen according to Table 2; see (Klein et al., 1999) for a detailed motivation of the particular numerical values.

Table 2. Control symbols

symbol	μ_1	μ_2	μ_3	μ_4	μ_5
D [mol/h]	35.8070	59.3318	82.8566	46.8782	70.4030
V [mol/h]	188.2433	158.6412	129.0391	217.8455	188.2433
symbol	μ_6	μ_7	μ_8	μ_9	
D [mol/h]	93.9278	57.9494	81.4742	104.999	
V [mol/h]	158.6412	247.4476	217.8455	188.2433	

[2] We use the substitutions $22 - s \to \hat{s}_s$ and $63 - s \to \hat{s}_r$ for the wave positions in order to end up with an order preserving map h.

For each input symbol $\mu \in U$, the system (37a), (37b) exhibits a unique solution and hence induces a flow Φ_t^μ. With the choice of a particular sampling interval ($\Delta = 10$ min), a hybrid plant model according to Sec. 2 is completely determined.

As a specification, we require the supervisor to drive any initial state within $X_0 = \mathcal{V}_\delta(h(P))$ into the target region $X_f = \overline{\mathcal{V}}_\delta(h(P_f))$ within no more than 20 min, where $P_f = [0.316,\ 0.320] \times [8.5,\ 11.5] \times [27.5,\ 31.0] \subset P$. Choosing one of the quantization cells equal to X_f, this specification can be formalized by the behaviour $\mathfrak{B}_{\mathrm{spec}}\{(u,y)|\ y(k) = \nu_f\ \forall\ k \geq 2\}$, where $G^{-1}(\nu_f) = X_f$ for some $\nu_f \in Y$. Controller synthesis is then successfully carried out based on the estimate sets $\hat{\mathcal{X}}((u,y)|_{[0,l]})$ for $l = 2$. A simulation of the closed loop (consisting of 42nd order continuous plant model and DES controller) is shown in Fig. 4. For each sampling instant, one concentration profile is plotted, the arrows indicate forward evolution in time and the intervals per tray indicate the target region X_f. As the sampling intervals in the closed-loop configuration are chosen to be 10 min, the target region is seen to be reached within 20 min. In contrast, Fig. 5 shows an open-loop simulation for the nominal input V_0 and D_0. Here, one profile every 5 h is plotted, and it takes an overall time of 20 h to reach the target region.

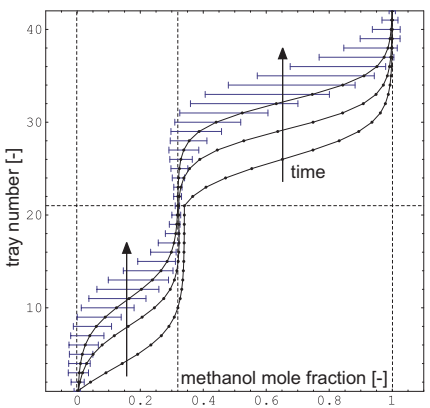

Fig. 4. Closed-loop (Δ=10min)

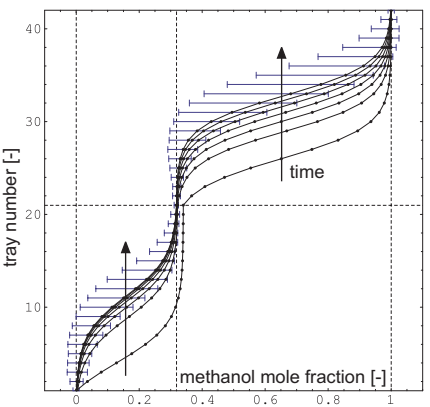

Fig. 5. Open-loop (Δ=5h)

Remark 2. The properties employed for the construction of $\mathcal{M}$ are well motivated by wave propagation theory and also have been validated by simulations and experiments. It follows from the successful completion of the controller synthesis procedure, that our discrete abstraction is accurate enough for the particular purpose. While the insight from the process engineering perspective has been an essential guidance, it is important to note that the reliability of our controller does not depend on the various claims and assumptions regarding the process model: the only relevant requirement is the inclusion $\mathfrak{B}_{\mathrm{ca}} \supseteq \mathfrak{B}$, and this follows purely from the monotonicity of f as discussed in Sect. 3, see Corollary 1.

On a decent workstation, the overall time required for the computation of both the discrete approximation and the supervisory controller is about 10 min. This is a significant performance increase when compared with earlier work (Klein et al., 2000, Klein et al., 1998, Klein et al., 1999) on the very same scenario, but based on exhaustive simulation: there, computations took many hours. Note also the different quality of reliability: while our new approach guarantees the approximation to be conservative, exhaustive simulation may – in principle – overlook critical states.

6 Conclusions

In this paper, we have shown how a general method for the abstraction based synthesis of discrete event controllers can be applied to a class of nonlinear high-order continuous systems, characterised by a monotonicity condition and an attractive low-dimensional manifold. In the presence of strict reliability requirements, abstraction based controller synthesis methods have been mostly restricted to low-order linear plant models and in this sense our contribution constitutes a considerable extension to the range of potential applications. Using monotonicity, the temporal evolution of quantization cells can be conveniently over-approximated even for nonlinear dynamics. This allows for the economical construction of a discrete abstraction for the nonlinear plant dynamics under investigation. Under the assumption that the plant state approaches a low-dimensional manifold, we construct an abstraction that in terms of computational effort depends only on the dimension of the attractive manifold rather than the full order of the plant dynamics. Note that both of our conditions lie completely within the domain of continuous dynamics: whether or not a plant is monotone and whether or not it exhibits an attractive manifold can be assessed by means of the classical theories. One might argue that our conditions are too restrictive for our results to be of practical relevance. This is not true, and we present a real-world example to support our claim to the contrary: based on a 42nd order nonlinear model of a pilot plant scale distillation column, we synthesize a discrete controller that speeds up the column start-up procedure. A comparison with earlier work underlines the achieved computational benefits.

Acknowledgement. We'd like to thank D. Flockerzi for valuable discussions on monotone dynamical systems and A. Kienle, A. Itigin, and E. Klein for their help with the the distillation column scenario.