Computing finite abstractions with robustness margins via local reachable set over-approximation

Yinan Li[†,*], **Jun Liu**[†,*], **Necmiye Ozay**[‡]

[†] *Department of Automatic Control and System Engineering*
University of Sheffield, Sheffield, S1 3JD, UK
[*] *Current affiliation: Department of Applied Mathematics*
University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
(e-mails: mmchong.yinan@gmail.com; j.liu@uwaterloo.ca)
[‡] *Department of Electrical Engineering and Computer Science*
University of Michigan, Ann Arbor, MI 48109, USA
(e-mail: necmiye@umich.edu).

Abstract: This paper proposes a method to compute finite abstractions that can be used for synthesizing robust hybrid control strategies for nonlinear systems. Most existing methods for computing finite abstractions utilize some global, analytical function to provide bounds on the reachable sets of nonlinear systems, which can be conservative and lead to spurious transitions in the abstract systems. This problem is even more pronounced in the presence of imperfect measurements and modelling uncertainties, where control synthesis can easily become infeasible due to added spurious transitions. To mitigate this problem, we propose to compute finite abstractions with robustness margins by over-approximating the local reachable sets of nonlinear systems. We do so by linearizing the nonlinear dynamics into linear affine systems and keeping track of the linearization error. It is shown that this approach provides tighter approximations and several numerical examples are used to illustrate of effectiveness of the proposed methods.

Keywords: Nonlinear systems, temporal logic, control synthesis, reachable set computation.

1. INTRODUCTION

Construction of finite abstractions for nonlinear systems is a critical step when applying abstraction-based approaches to hybrid control synthesis (Alur et al., 2000). Such approaches have gained popularity over the past few years for their ability to handle control problems for complex dynamical systems from high-level, rigorous specifications (see, e.g., piecewise affine systems (Kloetzer and Belta, 2008; Yordanov et al., 2012), polynomial and nonlinear switched systems (Ozay et al., 2013; Liu et al., 2013).The underlying principle of such approaches is to search for a controller in a finite abstraction of the original continuous system, leveraging formal synthesis techniques developed in computer science. As a result, the fidelity of finite abstractions has a significant influence on the result of control synthesis.

Symbolic models that are approximately similar or bisimilar to continuous-time nonlinear systems have been proposed and studied extensively (Pola et al., 2008; Girard et al., 2010; Zamani et al., 2012; Tabuada, 2009), which provide concrete means for computing finite approximate models often based on state-space discretization. For example, the symbolic models proposed in Pola et al. (2008) and Girard et al. (2010) are based on approximate bisimulation relations, which require incremental input-to-state stability (Angeli, 2002) of the original system. The work by Zamani et al. (2012) later relaxes the stability requirement and constructs symbolic models that are essentially approximately alternatingly similar to the original system. Such symbolic models are nondeterministic and the computation of transitions relies on a global, analytical function provided by the incremental forward completeness of dynamics (Zamani et al., 2012).

When dynamical systems are affected by imperfections such as measurement errors, delays, and disturbances, synthesis of robust control strategies becomes important. Motivated by this, the work by Liu and Ozay (2014) introduces a notion of finite abstractions that are equipped with additional robustness margins to account for imperfections in measurements and/or models. These margins also lead to added nondeterminism in the abstractions.

To increase the fidelity of the nondeterministic finite abstractions, one needs to reduce the number of spurious transitions in the abstractions. One way to do so is to compute tighter approximations of the local reachable sets for nonlinear systems. While local reachable set computation has been used for nonlinear system analysis and verification (see, e.g., Althoff (2010); Althoff and Krogh (2014)), we use it here to compute finite abstractions for robust control synthesis. More specifically, we linearize the nonlinear dynamics and keep track of the linearization errors. Robustness margins are incorporated in the set of initial conditions used for computing local reachable sets. This allows us to use margins that are state-dependent and take into account variations in local dynamics. One major advantage of the proposed approach is that it provides much less conservative abstractions, compared with existing approaches.

Notation: let $\mathbb{Z}$ be the set of integers and $\mathbb{N}$ be the set of all nonnegative integers; $\mathbb{R}$ represents the set of all real numbers; $\mathbb{R}_{\geq 0}$ and $\mathbb{R}_{>0}$ are the sets of all nonnegative and all positive real numbers, respectively; $\mathbb{R}^n$ denotes the n-dimensional Euclidean space; $\mathbb{Z}^n$ denotes the n-dimensional integer lattice (the set of vectors in $\mathbb{R}^n$ whose components are all integers); given a vector $x = (x_1, \cdots, x_n)$ in $\mathbb{R}^n$, let $|x| = (|x_1|, \cdots, |x_n|)$, i.e., the vector obtained by taking entrywise absolute value of x; given two vectors $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$, $x \leq y$ means $x_i \leq y_i$ for all $i \in \{1, \cdots, n\}$ ($x < y$, $x > y$, and $x \geq y$ are similarly defined) and $x \circ y$ indicates the entrywise product, i.e., $x \circ y := (x_1 y_1, \cdots, x_n y_n)$; a vector $x \in \mathbb{R}^n$ is said to be positive if $x > 0 \in \mathbb{R}^n$ and nonnegative if $x \geq 0 \in \mathbb{R}^n$; let $\mathbb{R}^n_{>0}$ and $\mathbb{R}^n_{\geq 0}$ denote the set of positive and non-negative vectors in $\mathbb{R}^n$; given vectors $\delta \in \mathbb{R}^n_{\geq 0}$ and $x \in \mathbb{R}^n$, define $B_\delta(x) := \{x' \in \mathbb{R}^n : |x' - x| \leq \delta\}$, a hyper-rectangular box centred at x; $\mathscr{B}_\delta(0)$ is written as $\mathscr{B}_\delta$ for short; given $\eta \in \mathbb{R}^n_{\geq 0}$, define $[\mathbb{R}^n]_\eta := \{\eta \circ k \in \mathbb{R}^n : k \in \mathbb{Z}^n\}$ to be a hyper-rectangular grid with granularity parameter η; given a set $S \subseteq \mathbb{R}^n$ and a vector $\eta \in \mathbb{R}^n_{\geq 0}$, define $[S]_\eta := S \cap [\mathbb{R}^n]_\eta$ to be the set of all grid points in S; given two sets $X \subseteq \mathbb{R}^n$ and $Y \subseteq \mathbb{R}^n$, $X \oplus Y$ denotes their Minkowski addition defined as $X \oplus Y := \{x + y \mid x \in X, y \in Y\}$; given a function f, $\mathrm{dom}(f)$ denotes its domain.

2. PROBLEM FORMULATION

2.1 Continuous-time control system

We consider a continuous-time control system described by a tuple $\mathscr{T} := (X, X_0, U, f, \Pi, L)$, whose execution is governed by the ordinary differential equation with inputs

$$\dot{x}(t) = f(x(t), u(t)), \tag{1}$$

where $t \in \mathbb{R}_{\geq 0}$, $x(t) \in X \subseteq \mathbb{R}^n$ is the system state, $x(0) \in X_0 \subseteq \mathbb{R}^n$ is the initial state, and $u(t) \in U \subseteq \mathbb{R}^m$ is the control input. A measurable locally essentially bounded function defined on $[0, \tau]$ taking values in U is called a *control signal* of duration τ. Let $\mathscr{U}$ be the set of all control signals with arbitrary but finite duration. The vector field $f : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ is a continuous function that fulfills the basic conditions (see, e.g., Khalil (2002)) for existence and uniqueness of solutions: given $x_0 \in X$, $T \in \mathbb{R}_{\geq 0}$, and a control signal $\mathbf{u}$ of duration T, there exists a unique solution, denoted by $\xi(t, x_0, \mathbf{u})$, that satisfies (1) for $t \in [0, T]$ and the initial condition $x(0) = x_0$. The labeling function $L : X \to 2^\Pi$ is function that maps a state of $\mathscr{T}$ to a set of propositions in Π that hold true at this state.

2.2 LTL control synthesis problem

The desired system behaviors for $\mathscr{T}$ are specified using linear temporal logic (LTL). LTL is able to express a combination of safety, reachability, invariance properties. It is built upon a set of atomic propositions Π, logical operators $\neg$ (negation), $\wedge$ (conjunction) and temporal operators $\bigcirc$ (next), $\mathbf{U}$ (until). An LTL formula φ is formed by connecting a finite set of atomic propositions with these operators. In this paper, we use a stutter-invariant fragment of LTL (denoted by $\mathrm{LTL}_{\backslash \bigcirc}$), which excludes operation $\bigcirc$. The syntax of $\mathrm{LTL}_{\backslash \bigcirc}$ can be found in Clarke et al. (2000). We also assume that all $\mathrm{LTL}_{\backslash \bigcirc}$ formulas have been transformed into negation normal form (Clarke et al., 2000, p. 132), by adding the operator $\mathbf{R}$ (release) and replacing any negations of atomic propositions with new atomic propositions. The continuous-time and discrete-time semantics of LTL can be found, e.g., in LiuO14.

Assume the system state x_k is measured at time t_k with $t_0 = 0$, $0 \leq t_k < t_{k+1}$, $k \in \mathbb{N}$. A *continuous control strategy* is defined as a function $\sigma : x_0, \cdots, x_i \to \mathbf{u}_i$ that generates a control signal $\mathbf{u}_i \in \mathscr{U}$ for the horizon $[t_i, t_{i+1})$ according to the history of states $x_0, \cdots, x_i$.

We are now ready to formulate the main control synthesis problem this paper aims to address.

Continuous Synthesis Problem: Given a continuous-time control system $\mathscr{T}$ and an $\mathrm{LTL}_{\backslash \bigcirc}$ specification φ, find a nonempty set of initial states X_0 and a control strategy σ such that the resulting solutions of $\mathscr{T}$ satisfy φ. The specification φ is said to be *realizable* for $\mathscr{T}$ if such X_0 exists.

3. FINITE ABSTRACTIONS WITH ROBUSTNESS MARGINS

This section is devoted to formally defining a notion of abstractions useful for solving robust control synthesis problems and proving their correctness and robustness guarantees when solving the continuous synthesis problem by discrete synthesis using these abstractions.

3.1 Finite abstractions with robustness margins

In Liu and Ozay (2014), the authors introduced a notion of finite abstractions with additional robustness margins that can effectively handle a range of robustness related issues in control synthesis, including modelling uncertainty, measurement errors, and jitter or delays in control signals.

This paper aims to improve its computational procedure in two aspects. First, we define the finite abstractions with a varying (state-dependent) robustness margins while Liu and Ozay (2014) use fixed margins which are often conservatively chosen to cope with the worst case. Second, we construct transitions by way of local reachable set computation while the results in Liu and Ozay (2014) rely on a global analytical bound that can lead to spurious transitions being added due to variation in local dynamics.

To this end, we shall formally define the notion of finite abstractions with robustness margins using reachable set.

Definition 1. Given a control signal $\mathbf{u} \in \mathscr{U}$ of duration τ and a set of initial states X_0, the *reachable set* for system (1) at time τ under this control signal $\mathbf{u}$ is defined by

$$\mathscr{R}_{\mathbf{u}, X_0}(\tau) := \{\xi(\tau, x_0, \mathbf{u}) \mid x_0 \in X_0\}.$$

The *reachable tube* for system (1) over the interval $[0, \tau]$ is the union of all reachable sets during this time interval, which is

$$\mathscr{R}_{\mathbf{u}, X_0}([0, \tau]) := \bigcup_{t \in [0, \tau]} \{\xi(t, x_0, \mathbf{u}) \mid x_0 \in X_0\}.$$

With a fixed $u \in U$ and $\tau \in \mathbb{R}_{>0}$, $\mathscr{R}_{u, X_0}(\tau)$ and $\mathscr{R}_{u, X_0}([0, \tau])$ are interpreted as u being a constant control signal on $[0, \tau]$.

We are now ready to define finite abstractions with robustness margins using reachable set.

Definition 2. Given $\delta \in \mathbb{R}^n_{>0}$ and functions $\Gamma_i : X \to \mathbb{R}^n_{\geq 0}$, $i = 1, 2$, a finite transition system

$$\hat{\mathscr{T}} := (\hat{\mathscr{Q}}, \hat{\mathscr{Q}}_0, \hat{\mathscr{A}}, \to_{\hat{\mathscr{T}}}, \hat{\Pi}, \hat{L})$$

is said to be a $(\Gamma_1, \Gamma_2, \delta)$-*abstraction* of the continuous-time control system $\mathscr{T} = (X, X_0, U, f, \Pi, L)$, denoted by $\mathscr{T} \preceq_{(\Gamma_1, \Gamma_2, \delta)} \hat{\mathscr{T}}$, if there exists an abstraction map $\Omega : X \to \hat{\mathscr{Q}}$ such that

- $\hat{\mathscr{Q}}$ is a finite subset of X;

- $\hat{\mathcal{Q}}_0 = \bigcup_{x \in X_0} \{\Omega(x)\}$;
- $\hat{\mathcal{A}}$ is a finite subset of $\mathcal{U}$;
- $(\hat{q}, \hat{\mathbf{u}}, \hat{q}') \in \rightarrow_{\hat{\mathcal{T}}}$ if, under $\hat{\mathbf{u}} \in \hat{\mathcal{A}}$ with duration τ, $\hat{q}$ and $\hat{q}'$ satisfy

$$\left(\Omega^{-1}(\hat{q}') \oplus \mathcal{B}_{\Gamma_2(\hat{q}')}\right) \cap \mathcal{R}_{\hat{\mathbf{u}}, \Omega^{-1}(\hat{q}) \oplus \mathcal{B}_{\Gamma_1(\hat{q})}}(\tau) \neq \varnothing;$$

- $\hat{L} : \hat{\mathcal{Q}} \rightarrow 2^{\hat{\Pi}}$ is defined by $\hat{L}(\hat{q}) = \cap_{x \in \mathcal{B}_\delta(\hat{q}) \cap X} L(x)$, $\hat{\Pi} = \Pi$.

The parameter δ is used to guarantee that specifications are satisfied even if the controller is synthesized using a finite abstraction with approximation errors. The functions $\Gamma_{1,2}$ provide additional robustness margins that varies with respect to local dynamics to account for imperfections such as system delay, measurement or modelling errors, at the price of increasing the nondeterminism in the abstraction.

Example 1. A common and practical type of imperfections involves delays and measurement errors (e.g., noise or quantization). Consider the system $\mathcal{T}$ with a continuous control strategy σ subjects to a measurement delay $h(t) \in [0, \Delta]$, $\Delta \in \mathbb{R}_{\geq 0}$, and an error $e(t)$ with $|e(t)| \leq \varepsilon \in \mathbb{R}_{\geq 0}^n$, the system dynamics becomes

$$\begin{cases} \dot{x}(t) = f(x(t), \mathbf{u}_i), \mathbf{u}_i = \sigma(\hat{x}(t_0), \cdots, \hat{x}(t_i)), \\ \hat{x}(t_i) = x(t_i - h(t_i)) + e(t_i). \end{cases} \quad (2)$$

where $\hat{x}$ denotes the measurement of system states, $t \in [t_i, t_{i+1})$, $t_0 = 0$, $t_i < t_{i+1}$, $i \in \mathbb{N}$ and $\tau_i = t_{i+1} - t_i$ is the time duration of $\mathbf{u}_i$.

3.2 Discrete synthesis problem

An $\text{LTL}_{\backslash \bigcirc}$ formula can be interpreted over paths of $\hat{\mathcal{T}}$. A *path* of $\hat{\mathcal{T}}$ is a sequence of states $\hat{\rho} = \hat{q}_0 \hat{q}_1 \hat{q}_2 \cdots$ under the the corresponding action $\hat{a}_i \in \hat{\mathcal{A}}$ at each state $\hat{q}_i \in \hat{\mathcal{Q}}$ while satisfying $(\hat{q}_i, \hat{a}_i, \hat{q}_{i+1}) \in \rightarrow_{\hat{\mathcal{T}}}$, $i \in \mathbb{N}$.

Similar to continuous control strategy, a *discrete control strategy* for $\hat{\mathcal{T}}$ is a function $\hat{\sigma} : \hat{q}_0, \cdots, \hat{q}_i \rightarrow \hat{a}_i$ that maps the history path to a control action. Then we formulate the discrete synthesis problem as follows.

Discrete Synthesis Problem Given a finite transition system $\hat{\mathcal{T}}$ and an $\text{LTL}_{\backslash \bigcirc}$ specification φ, find a nonempty set of initial states $\hat{X}_0$ and a control strategy $\hat{\sigma}$ such that any resulting path satisfies φ. If such $\hat{X}_0$ exists, then φ is said to be realizable for $\hat{\mathcal{T}}$.

3.3 Correctness and robustness guarantees

In general, the existence of a discrete control strategy $\hat{\sigma}$ that solves the discrete synthesis problem with an $\text{LTL}_{\backslash \bigcirc}$ specification φ does not guarantee that a control strategy exists for the continuous synthesis problem with the same specification.

As indicated in Definition 2, $\hat{\mathcal{T}}$ requires the same propositions of $\mathcal{T}$ to hold within a neighbourhood of radius δ, which is more restrictive. This is because the discrete strategy only guarantees that a sequence of sampled states satisfy a given specification and the parameter δ accounts for the possible mismatches of the inter-sample states. In addition, the robustness margin functions Γ_i ($i = 1, 2$) are chosen to account for possible imperfections.

To formally reason about the correctness and robustness guarantees of solving the continuous synthesis problem by

discrete synthesis using finite abstractions with robustness margins, the following theorem gives a sufficient condition for the realizability of the continuous synthesis problem by the realizability of the discrete synthesis problem.

Theorem 1. Given a continuous-time control system $\mathcal{T}$, its $(\Gamma_1, \Gamma_2, \delta)$-abstraction $\hat{\mathcal{T}}$, and an $\text{LTL}_{\backslash \bigcirc}$ formula φ,

(i) (correctness) φ being realizable for $\hat{\mathcal{T}}$ implies that φ is realizable for $\mathcal{T}$, provided that, for all $(\hat{q}, \hat{\mathbf{u}}, \hat{q}') \in \rightarrow_{\hat{\mathcal{T}}}$,

$$\mathcal{R}_{\hat{\mathbf{u}}, \Omega^{-1}(\hat{q}) \oplus \mathcal{B}_{\Gamma_1(\hat{q})}}(\text{dom}(\hat{\mathbf{u}})) \subseteq \mathcal{B}_\delta(\hat{q}). \quad (3)$$

In particular, if $\hat{\mathcal{T}}$ satisfies φ with $\hat{\sigma}$ and $\hat{\mathcal{Q}}_0$, then φ is realizable for $\mathcal{T}$ using $X_0 = \cup_{q \in \hat{\mathcal{Q}}_0} \Omega^{-1}(q)$ and $\sigma(x_0, \cdots, x_i) = \hat{\sigma}(\Omega(x_0), \cdots, \Omega(x_i))$ where $x_0, \cdots, x_i$ is the sequence of measured states.

(ii) (robustness) if the system is subjected to measurement delays and errors defined in (2), then the same statement holds true, provided additionally that the robustness margins Γ_i ($i = 1, 2$) satisfy that, for all $\hat{\mathbf{v}} \in \hat{\mathcal{A}}$ and $\hat{q} \in \hat{\mathcal{Q}}$, $\Gamma_2(\hat{q}) \geq \varepsilon$ and

$$\mathcal{R}_{\hat{\mathbf{v}}, \Omega^{-1}(\hat{q}) \oplus \mathcal{B}_\varepsilon}([0, \Delta]) \subseteq \Omega^{-1}(\hat{q}) \oplus \mathcal{B}_{\Gamma_1(\hat{q})}. \quad (4)$$

The proof for Theorem 1 (as well as subsequent proofs) is omitted for space constraints and can be found in the extended version (Li et al., 2015).

4. REACHABLE SET OVER-APPROXIMATION BASED ON LINEARIZATION AND ERROR ESTIMATION

A key step in constructing finite abstractions with robustness margins defined in the previous section is to compute the reachable sets for nonlinear systems. In practice, exact reachable sets of nonlinear systems are difficult to obtain and thus their approximations are usually computed. For example, reachable set over-approximation is implicitly required by the abstraction procedures in Pola et al. (2008); Zamani et al. (2012); Liu and Ozay (2014), where analytical bounds, usually obtained by Lyapunov-like functions, are used to roughly estimate the evolution of trajectories. A more precise computation of reachable sets has the potential to significantly reduce the spurious transitions in the abstraction.

In this section, we present a linearization-based method for the computation of reachable sets for nonlinear systems. For simplicity, we only consider constant control signals, which suffice for the computation of finite abstractions by discretization-based methods to be discussed in Section 5.

4.1 Reachable set computation for linear systems

Consider a class of affine control systems of the form

$$\dot{x}(t) = Ax(t) + b + u(t) \quad (5)$$

where $b \in \mathbb{R}^n$ is a constant vector, $x(t) \in X$ is the state, $u(t) \in U$ is the control signal, and $U \subseteq \mathbb{R}^m$ is a compact convex set.

Similar to Definition 1, given an initial set of states $X_0 \subseteq X$, we denote by $\mathcal{R}_{X_0}^L(\tau)$ the set of states that are reachable at time $\tau \in \mathbb{R}_{\geq 0}$ under U, which is defined by

$$\mathcal{R}_{X_0}^L(\tau) := \{x(\tau) \in X | \dot{x}(t) = Ax(t) + b + u(t), \forall t \in [0, \tau],$$
$$u(t) \in U, x(0) \in X_0\}.$$

The reachable tube over the interval $[0, \tau]$ is defined by

$$\mathcal{R}_{X_0}^L([0, \tau]) := \bigcup_{t \in [0, \tau]} \mathcal{R}_{X_0}^L(t).$$

Since the control input $u(t)$ is chosen arbitrarily from the set U, both the reachable set and tube are difficult to be computed exactly. For linear control systems, their convex over-approximations are used instead (see, e.g., Lemmas 1 and 2 in Guernic and Girard (2010)). The convex hull of two convex sets, which is defined by

$$\mathrm{CH}(\mathscr{X}, \mathscr{Y}) = \{\lambda x + (1 - \lambda) y \mid x \in \mathscr{X}, y \in \mathscr{Y}, \lambda \in [0, 1]\},$$

is used to compute the reachable tube. For the linear affine control systems, we give the following proposition to over-approximate the reachable sets and tubes.

Proposition 2. For a linear affine control system (5), given a compact convex set $X_0 \subseteq X$ and a time $\tau \in \mathbb{R}_{\geq 0}$, let

$$Y(\tau) = e^{A\tau} X_0 \oplus \{G(A, \tau) b\} \oplus \tau U \oplus \mathscr{B}_{\beta_\tau},$$
$$Y([0, \tau]) = \mathrm{CH}(X_0, Y(\tau) \oplus \mathscr{B}_{\alpha_\tau + \gamma_\tau}), \qquad (6)$$

where

$$\alpha_\tau = (e^{\tau \|A\|} - 1 - \tau \|A\|) \max_{x \in X_0} \|x\| \mathbf{1},$$
$$\beta_\tau = (e^{\tau \|A\|} - 1 - \tau \|A\|) \|A\|^{-1} \max_{u \in U} \|u\| \mathbf{1}, \qquad (7)$$
$$\gamma_\tau = (e^{\tau \|A\|} - 1 - \tau \|A\|) \|A\|^{-1} \|b\| \mathbf{1},$$

with $\|\cdot\|$ as the infinity norm, $\mathbf{1} \in \mathbb{R}^n$ representing the vector of ones, i.e., each element of it equals to 1, and $G(A, \tau) := \int_0^\tau e^{A(\tau - t)} dt$.

Then

$$\mathscr{R}_{X_0}^L(\tau) \subseteq Y(\tau),$$
$$\mathscr{R}_{X_0}^L([0, \tau]) \subseteq Y([0, \tau]).$$

Remark 1. Proposition 2 differs from (Guernic and Girard, 2010) in considering affine systems. Defining $v(t) := b + u(t), v(t) \in V = \{b\} \oplus U$, the method in (Guernic and Girard, 2010) can also be applied. Yet when $u(t)$ is small compared to b, the size of $Y(\tau)$ computed by proposition 2 is smaller because of a smaller bloating parameter β_τ.

4.2 Reachable set computation for nonlinear systems

Reachable set over-approximation for nonlinear systems obtained by a global analytical function can be conservative. To obtain a relatively tighter over-approximation of the one-step reachable set of nonlinear systems, we can write the nonlinear system dynamics as the sum of its linearization in a local area and an approximation error term.

More specifically, for a nonlinear system (1) under a constant control input $u \in \mathscr{U}$, the dynamics around a center point $x^* \in X$ can be approximated by its first-order Taylor expansion with a Lagrangian remainder:

$$\dot{x}(t) = A_{x^*}(x(t) - x^*) + f(x^*, u) + d_{x^*}(t), \qquad (8)$$

where $A_{x^*} = \partial f / \partial x|_{x^*}$, and $d_{x^*}(t) = (d_1(t), \cdots, d_n(t)) \in \mathbb{R}^n$ is the approximation error with

$$d_i(t) = \frac{1}{2} (x(t) - x^*)^T H_i(z_i(t))(x(t) - x^*),$$

$$H_i(z_i(t)) = \left. \frac{\partial^2 f_i}{\partial x^2} \right|_{z_i(t)},$$

and $z_i(t) \in \mathscr{B}_{|x(t) - x^*|}(x^*)$.

If the system trajectory does not exceed a predefined linearization area $\mathscr{B}_r(x^*)$, where $r \in \mathbb{R}_{>0}^n$, then $d_{x^*}(t)$ belongs to a convex set $\mathscr{D}_{x^*}(r)$ given by

$$\mathscr{D}_{x^*}(r) = \{d = (d_1, \ldots, d_n) \mid d_i = \frac{1}{2} x^T H_i(z_i) x,$$
$$x \in \mathscr{B}_r, z_i \in \mathscr{B}_r(x^*)\}. \qquad (9)$$

Defining $\tilde{x}(t) := x(t) - x^*$, (8) is in the form of (5). Thus, the reachable set and tube of the nonlinear control system (1) can be computed using Proposition 2 locally.

4.3 Reachable set computation using zonotopes

Since set operations, such as linear transformation, addition and multiplication, are used extensively in the computation of reachable sets, a proper set representation can help expedite the computational process. To this end, zonotope representation is attractive for its efficiency in the aforementioned set operations (see, e.g., Girard (2005); Girard et al. (2006); Althoff and Krogh (2014)).

Definition 3. A *zonotope* is a set represented as

$$\mathscr{Z} := \left\{ x \in \mathbb{R}^n \mid x = c + \sum_{i=1}^{l} \lambda_i g^{(i)}, \lambda_i \in [-1, 1] \right\},$$

where $c, g^{(i)} (i = 1, 2, \ldots, l) \in \mathbb{R}^n$ are called the central vector and generators, respectively; l is the number of generators. It is often denoted as $\mathscr{Z} = (c, g^{(1)}, \ldots, g^{(l)})$.

The addition of two zonotopes $\mathscr{Z}_1 = (c_1, g_1^{(1)}, \ldots, g_1^{(l_1)})$ and $\mathscr{Z}_2 = (c_2, g_2^{(1)}, \ldots, g_2^{(l_2)})$ and the multiplication of a zonotope with a matrix $M \in \mathbb{R}^{n \times n}$ can be easily derived as

$$\mathscr{Z}_1 \oplus \mathscr{Z}_2 = (c_1 + c_2, g_1^{(1)}, \ldots, g_1^{(l_1)}, g_2^{(1)}, \ldots, g_2^{(l_2)}),$$
$$M\mathscr{Z}_1 = (Mc_1, Mg_1^{(1)}, \ldots, Mg_1^{(l_1)}).$$

For a zonotope with l generators in $\mathbb{R}^n$, l/n is called the *order* of the zonotope.

Example 2. The set $\mathscr{B}_r$ with $r = (r_1, \cdots, r_n), r_i \in \mathbb{R}_{>0}$ can be written in the form of zonotope as

$$\mathscr{Z}_{\mathscr{B}_r} = (0, g_r^{(1)}, g_r^{(2)}, \cdots, g_r^{(n)}), \qquad (10)$$

where $g_r^{(i)} \in \mathbb{R}^n$ is a vector with all the elements being zero except that the ith element is r_i, $i = 1, 2, \cdots, n$.

The approximation error $\mathscr{D}_{x^*}(r)$ as in (9) can be over-approximated using the quadratic map (Althoff and Krogh, 2014). Instead of computing $H_i(z_i)$ for every $z_i \in \mathscr{B}_r(x^*)$, we enclose it by an interval matrix $\overline{H}_i(x^*)$. Denote by $\overline{h}_{ij}$ the element of the ith row and jth column of $\overline{H}_i(x^*)$, then $\overline{h}_{ij} = [h_{ij}^l, h_{ij}^u]$, where h_{ij}^l and h_{ij}^u is the minimum and maximum values of $\overline{h}_{ij}$ in the linearization area respectively. Using $\mathscr{Z}_{\mathscr{B}_r}$ defined in (10), we can compute an over-approximation of $\mathscr{D}_{x^*}(r)$ by

$$\mathscr{D}_{x^*}(r) \subseteq \overline{\mathscr{D}}_{x^*}(r) := \mathrm{quad}(\overline{H}_i(x^*), \mathscr{Z}_{\mathscr{B}_r}), \qquad (11)$$

where $\mathrm{quad}(\cdot, \cdot)$ is the quadratic map defined in Althoff and Krogh (2014).

The convex hull operation of two zonotopes can be over-approximated by (see Girard (2005); Althoff (2010) for more details)

$$\overline{\mathrm{CH}}(\mathscr{Z}_1, \mathscr{Z}_2) = \frac{1}{2}(c_1 + c_2, g_1^{(1)} + g_2^{(1)}, \cdots, g_1^{(l)} + g_2^{(l)},$$
$$c_1 - c_2, g_1^{(1)} - g_2^{(1)}, \cdots, g_1^{(l)} - g_2^{(l)}).$$

To sum up, we give the following proposition, which aims to over-approximate the local reachable sets of nonlinear systems using zonotopes.

Proposition 3. Given a nonlinear control system $\mathscr{T}$, the function $\Gamma_1 : X \to \mathbb{R}_{\geq 0}^n$, an abstraction map $\Omega : X \to \hat{\mathscr{Q}}$ and a finite

set of constant control actions $\hat{\mathscr{A}}$, for any $\hat{q} \in \hat{\mathscr{Q}}$ and $\hat{\mathbf{u}} \in \hat{\mathscr{A}}$ with $\hat{\mathbf{u}}(t) = \hat{u} \in U, \forall t \in [0, \tau]$, denote

$$X_{\hat{q}} = \Omega^{-1}(\hat{q}) \oplus \mathscr{B}_{\Gamma_1(\hat{q})}, \quad \tilde{X}_{\hat{q}} = \{-\hat{q}\} \oplus X_{\hat{q}}. \quad (12)$$

The reachable set and tube $\mathscr{R}_{\hat{u},X_{\hat{q}}}(\tau)$ and $\mathscr{R}_{\hat{u},X_{\hat{q}}}([0,\tau])$ can be over-approximated by the sets $\overline{\mathscr{R}}_{\hat{u},X_{\hat{q}}}(\tau)$ and $\overline{\mathscr{R}}_{\hat{u},X_{\hat{q}}}([0,\tau])$, respectively, which are computed by

$$\overline{\mathscr{R}}_{\hat{u},X_{\hat{q}}}(\tau) = \{\hat{q}\} \oplus \tilde{Y}(\tau), \quad (13)$$

and

$$\overline{\mathscr{R}}_{\hat{u},X_{\hat{q}}}([0,\tau]) = \{\hat{q}\} \oplus \overline{\mathrm{CH}}(\tilde{X}_{\hat{q}}, \tilde{Y}(\tau) \oplus \mathscr{B}_{\alpha_\tau + \gamma_\tau}), \quad (14)$$

where

$$\tilde{Y}(\tau) = e^{A_{\hat{q}}\tau} \tilde{X}_{\hat{q}} \oplus G(A_{\hat{q}}, \tau) f(\hat{q}, u) \oplus \tau \mathscr{D}_{\hat{q}}(r) \oplus \mathscr{B}_{\beta_\tau},$$

and $\alpha_\tau, \beta_\tau, \gamma_\tau, G(A_{\hat{q}}, \tau)$ are defined as in Proposition 2.

5. COMPUTATION OF ABSTRACTION BY DISCRETIZATION AND ZONOTOPE REPRESENTATION

In this section, we discuss how to construct finite abstractions with robustness margins by grid-based discretization.

5.1 Grid-based discretization

Consider uniform parameters $\eta \in \mathbb{R}_{>0}^n$, $\mu \in \mathbb{R}_{>0}^m$ and a fixed sampling time $\tau_s \in \mathbb{R}_{>0}$. Let $\hat{\mathscr{Q}} = [X]_\eta$ be the set of states in $\hat{\mathscr{T}}$. In this case, $\Omega^{-1}(\hat{q}) \oplus \mathscr{B}_{\Gamma_i(\hat{q})} = \mathscr{B}_{\eta/2 + \Gamma_i(\hat{q})}(\hat{q})$ $(i = 1, 2)$. Using zonotopes with order 1, $X_{\hat{q}}, \tilde{X}_{\hat{q}}$ in (12) become

$$X_{\hat{q}} = (\hat{q}, g_\eta^{(1)}, g_\eta^{(2)}, \cdots, g_\eta^{(n)}),$$
$$\tilde{X}_{\hat{q}} = (0, g_\eta^{(1)}, g_\eta^{(2)}, \cdots, g_\eta^{(n)}),$$

where $g_\eta^{(i)} \in \mathbb{R}^n$ is a vector with all the elements are zero except the ith element being $\eta/2 + \Gamma_1(\hat{q})$, $i = 1, 2, \cdots, n$.

The set of control actions $\hat{\mathscr{A}}$ only contains the control signals that take values in $[U]_\mu$ and the time duration are integral multiples of τ_s. Since the computation of reachable sets and tubes are only valid within the linearization area $\mathscr{B}_r(\hat{q})$, the time duration and the value of the control signals should be determined to make sure that the transitions only take place inside it. Furthermore, in order to satisfy Theorem 1, this area should belong to $\mathscr{B}_\delta(\hat{q})$; in other words, $r \leq \delta$.

5.2 Algorithm for computing transitions

The algorithm for computing transitions is designed to collect all the valid transitions under a grid-based discretization according to Theorem 1 (details can be found in Li et al. (2015)). The main steps are devoted to solving the key problem of determining the valid control signal duration $\tau = k\tau_s, k \in \mathbb{N}$ (if it exists) for each element in $[U]_\mu$ and state in $\hat{\mathscr{Q}}$.

Similar to a lazy control strategy, which means that the control action is kept to be the same for as long as possible, we choose $\tau = \tau_{\max}$, where $\tau_{\max}$ is the maximum time of a control signal under which the system remains within a pre-defined linearization area. A practical consideration for this is that a short time duration can potentially introduce spurious self-transitions that do not exist in the original continuous system.

Out of simplicity in implementation, we use $\hat{\tau}_{\max} = p^* \tau_s, p^* \in \mathbb{N}$ as an under-approximation of $\tau_{\max}$, and approach it iteratively using a lower bound a and an upper bound b $(a, b \in \mathbb{N}$

and $a \leq b)$. The initial guess equals to the upper bound b. If the reachable set is fully inside the linearization area, which means $p^* \geq b$, the bounds shift to $[b, b + (b - a)]$; if the reachable set has already move outside the region, the bounds shrink to $[a, \lfloor \frac{a+b}{2} \rfloor]$. Considering the situation that reachable sets shrinks around the equilibria, i.e., $\tau_{\max} = \infty$, we set an upper limit $N \in \mathbb{N}$ for p.

6. COMPARISON WITH LYAPUNOV-BASED APPROXIMATION

We analyze the performance of the controllers synthesized using finite abstractions with robustness margins by two examples: the pendulum system (Pola et al., 2008)) and the automatic cruise control (Liu and Ozay, 2014).

6.1 Pendulum

The pendulum model considered here is

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} x_2 \\ -\dfrac{g}{l} \sin x_1 - \dfrac{k}{m} x_2 + u \end{bmatrix},$$
$$g = 9.8, l = 5, m = 0.5, k = 3,$$

where $u \in U = [-1, 0], x \in X = [-0.5, 0] \times [-0.2, 0.2]$; u is the normalized control torque; x_1, x_2 represent the angle (rad) and the angular rate (rad/sec), respectively. The angle is measured from the perpendicular line to the current ball position. The positive direction is counter clockwise. The constants g, l, m, k denote the gravity acceleration, rod length, mass, and friction coefficient, respectively.

The specification is given by an $\text{LTL}_{\backslash \bigcirc}$ formula $\varphi = \Box \varphi_s \wedge \Diamond \Box \varphi_t$ with $\varphi_s = X$ and $\varphi_t = [-0.3, -0.2] \times [-0.05, 0.05]$. In our simulation, the abstraction parameters are $\tau_s = 0.01s$, $r = [0.04; 0.04]$, $\eta = [0.02; 0.02]$, $\mu = 0.01$. As shown in Fig. 1 (left), the controlled system trajectory satisfies the given specification.

On the other hand, we fail to generate a controller using the abstraction based on Lyapunov-like method, as a result of its greater conservatism. We compare the number of transitions included by different reachable set computation methods. With the same partition, applying the control torque $u = -0.81$ at the state $x_1 = -0.3$, $x_2 = 0.1$, the number of post states computed by our method is 4 while it is 49 using the Lyapunov-based method. As shown in Fig. 1, the one-step reachable set computed using our method is smaller than that using the Lyapunov-based method.

6.2 Automatic cruise control

Consider the longitudinal dynamics of automatic cruise control $\dot{v} = u - c_0 - c_1 v^2$, where $v \in [20, 30]$, $u \in [-1.5, 1]$, $c_0 = 0.1$, and $c_1 = 0.00016$.

To design a controller satisfying the specification $\varphi = \Box(v \leq 30) \wedge \Diamond \Box(v \in [22, 24])$, we set $\tau_s = 0.3s$, $r = 0.6$, $\eta = 0.1$, $\mu = 0.2$. In the simulations, the system is subjected to a maximum delay $d = 0.01s$ and a measurement error bound $\varepsilon = 0.1m/s$. We construct three different abstractions: i) one without robustness margins; ii) one with uniform robustness margins (as defined in Liu and Ozay (2014)); iii) one with varying robustness margins (as defined in this paper). Fig. 2 presents the simulation results of the cruise control system, under controllers
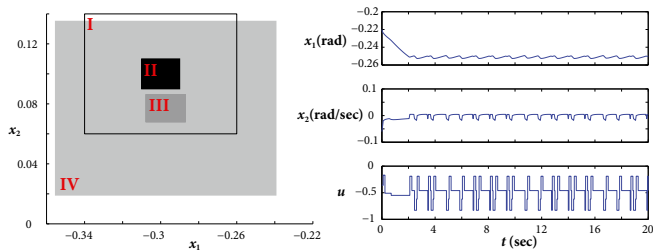
Fig. 1. Left: The trajectories of the controlled pendulum system states and the corresponding control signal. Right: Comparison of one-step reachable sets generated by two methods: region I indicates the linearization region $\mathscr{B}_r(\hat{q})$; region II is the initial set of states; region III is an over-approximation of the reachable set obtained by the proposed linearization-based method; region IV is an over-approximation of the reachable set obtained by an analytical bound using Lyapunov-based methods.

synthesized using the first and the third abstractions. As observed from Fig. 2 (left), the speed jumps out of the target range as the time lapses because the first abstraction cannot counteract delays or measurement errors, while the result from the third abstraction shown on the right of Fig. 2 is satisfactory. To compare the second and the third abstractions, we look at their transitions around the state $v = 21.4$m/s under the control input $u = 0.15$. The second abstraction has 30 transitions, whereas the third one has only 20. In fact, due to its greater conservatism, the second abstraction is not able to generate a controller during control synthesis.
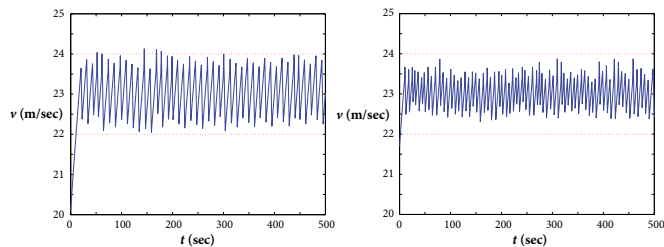

Fig. 2. Controlled state evolution synthesized from an abstraction with (right) and without (left) robustness margins.

7. CONCLUSION

In this paper, we considered the problem of constructing finite abstractions for nonlinear systems that are suitable for synthesizing robust controllers. A notion of finite abstractions with robustness margins that vary with respect to the local dynamics was formally defined. One main contribution of our work was to apply local reachable sets computation techniques in computing finite transitions, which led to reduced degree of nondeterminism in the abstractions. The local reachable sets are computed by linearization and approximation error estimation. As illustrated by numerical examples, the abstractions generated by the proposed method contain fewer spurious transitions than those obtained from Lyapunov-based methods and therefore are more likely to render the control synthesis problem realizable. Future work will combine the abstraction procedures presented in this paper, which take into account local dynamics, with automated

refinement procedures to mitigate potential state explosion problems.

REFERENCES

Althoff, M. and Krogh, B.H. (2014). Reachability analysis of nonlinear differential-algebraic systems. *IEEE Trans. Automat. Control*, 59(2), 371–383.

Althoff, M. (2010). *Reachability Analysis and its Application to the Safety Assessment of Autonomous Cars*. Ph.D. thesis, Technische Universität München.

Alur, R., Henzinger, T.A., Lafferriere, G., and Pappas, G.J. (2000). Discrete abstractions of hybrid systems. In *Proc. IEEE*, volume 88, 971–984.

Angeli, D. (2002). A Lyapunov approach to incremental stability properties. *IEEE Trans. Automat. Control*, 47(3), 410–421.

Clarke, E.M., Grumberg, O., and Peled, D.A. (2000). *Model Checking*. The MIT Press.

Girard, A. (2005). Reachability of uncertain linear systems using zonotopes. In *Proc. of HSCC*, 291–305.

Girard, A., Guernic, C.L., and Maler, O. (2006). Efficient computation of reachable sets of linear time-invariant systems with inputs. In *Proc. of HSCC*, 257–271.

Girard, A., Pola, G., and Tabuada, P. (2010). Approximately bisimilar symbolic models for incrementally stable switched systems. *IEEE Trans. Automat. Control*, 55(1), 116–126.

Guernic, C.L. and Girard, A. (2010). Reachability analysis of linear systems using support functions. *Nonlinear Analysis: Hybrid Systems*, 4(2), 250–262.

Khalil, H.K. (2002). *Nonlinear Systems*. Prentice Hall.

Kloetzer, M. and Belta, C. (2008). A fully automated framework for control of linear systems from temporal logic specifications. *IEEE Trans. Automat. Control*, 53(1), 287–297.

Li, Y., Liu, J., and Ozay, N. (2015). Computing finite abstractions with robustness margins via local reachable set over-approximation. *arXiv:1507.06248 [cs.SY]*. URL http://arxiv.org/abs/1507.06248.

Liu, J. and Ozay, N. (2014). Abstraction, discretization, and robustness in temporal logic control of dynamical systems. In *Proc. of HSCC*, 293–302.

Liu, J., Ozay, N., Topcu, U., and Murray, R.M. (2013). Synthesis of reactive switching protocols from temporal logic specifications. *IEEE Trans. Automat. Control*, 58(7), 1771–1785.

Ozay, N., Liu, J., Prabhakar, P., and Murray, R.M. (2013). Computing augmented finite transition systems to synthesize switching protocols for polynomial switched systems. In *Proc. of ACC*, 6237–6244.

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

Tabuada, P. (2009). *Verification and Control of Hybrid Systems - A Symbolic Approach*. Springer.

Yordanov, B., Tůmová, J., Černá, I., Barnat, J., and Belta, C. (2012). Temporal logic control of discrete-time piecewise affine systems. *IEEE Trans. on Automatic Control*, 57(6), 1491–1504.

Zamani, M., Pola, G., Jr., M.M., and Tabuada, P. (2012). Symbolic models for nonlinear control systems without stability assumptions. *IEEE Trans. Automat. Control*, 57(7), 1804–1809.