Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnline CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 54-5 (2021) 115–120

Simulation Relations for Abstraction-based Robust Control of Hybrid Dynamical Systems

Pavithra Prabhakar * **Jun Liu** **

* *Kansas State University, Manhattan, KS 66503 USA (e-mail: pprabhakar@ksu.edu).*

** *University of Waterloo, Waterloo, Ontario N2L 3G1 Canada (e-mail: j.liu@waterloo.ca)*

Abstract: The paper addresses the problem of robust control of hybrid dynamical systems with respect to linear-time properties. First, three notions of robust controllers are formulated, that capture imperfect measurements, actuation errors and delays, and uncertain dynamics, respectively. Under mild assumptions of uniform continuity on the transition relation, robust controller synthesis problem with respect to uncertain dynamics is shown to be more general than those with respect to measurement errors, actuation errors and delays. Hence, the paper focuses on the latter notion of robust controllers. Next, foundations for abstraction-based robust controller synthesis are explored, and uniformly continuous alternating simulation relations are shown to preserve the existence of robust controllers with respect to uncertain dynamics.

Keywords: Hybrid Systems, Robustness, Simulations, Bisimulations, Abstractions

1. INTRODUCTION

Modern embedded software systems consist of complex software that control safety-critical physical systems as in autonomous vehicles, smart grids and smart buildings. Given the safety criticality of these embedded software systems, formal synthesis has emerged as a rigorous methodology for automatically designing correct-by-construction controllers for complex dynamical systems representing physical systems. A synthesis algorithm takes as input a mathematical model of the physical system (plant) and a formal specification of correctness, and outputs a controller such that the closed-loop system satisfies the specification. Formal synthesis is a well-studied problem in the area of formal methods with the focus mainly on discrete finite-state systems, wherein automata-theoretic methods are used to compute controllers for objectives ranging from safety to general linear-time properties specified using logics such as Linear Temporal Logics or automata-based formalisms such as Büchi automata Grädel et al. (2002); Baier and Katoen (2008). Correct-by-construction synthesis for dynamical systems has gained momentum in recent years, which consists of an abstraction-based approach. First, an abstraction of the dynamical system $\dot{x}(t) = f(x(t), u(t))$ is constructed, typically, as a finite-state game, and an abstract controller is synthesized for the finite-state game using automata-theoretic methods. A concrete controller $u(t)$ is then extracted from the abstract controller. This approach has been investigated extensively with applications to robot path planning Wongpiromsarn et al. (2011); Belta et al. (2017); Rungger and Zamani (2016); DeCastro and Kress-Gazit (2013).

In this paper, we consider a robust version of the controller synthesis problem, wherein, we desire to synthesize a controller $u(t)$ such that the closed loop system satisfies the given specification even in the presence of state measurement errors/sensor noise, actuation errors and delays, as well as uncertain dynamics, which are practical issues that arise in an embedded control system. The objectives of this paper are two fold. First, we intend to formulate the different notions of robustness required to capture the deviations introduced in the controller design and implementation process in the general setting of metric transition systems that can capture "hybrid dynamical systems" resulting from the interaction of complex continuous physical systems and digital controllers. Secondly, the design of software-controlled physical systems is computationally complex, and can lead to undecidability for relatively simple classes of system dynamics Henzinger et al. (1995). Hence, it is crucial to incorporate abstraction-based design. However, existing literature on *robust* controller synthesis using an abstraction-based approach is limited (See Section 1.1 for a discussion of some of the related work on robust controller synthesis). Our objective is to develop the foundations for the abstraction-based design of robust controllers by understanding the relation between a given concrete system and an abstract system such that robust controllers are preserved. Pre-orders such as alternating simulations and bisimulations Alur et al. (1998) provide the foundations for abstraction-based design and analysis of systems. More precisely, if there is an alternating simulation from $\mathcal{T}_1$ to $\mathcal{T}_2$, then the existence of a controller for $\mathcal{T}_2$ implies the existence of a controller for $\mathcal{T}_1$. Here, $\mathcal{T}_2$, the simulating system is interpreted as the abstract/simplified system on which the controller synthesis is performed. Our objective is to define pre-orders that, in addition to

⋆ Pavithra Prabhakar was partially supported by NSF CAREER Award No. 1552668 and ONR YIP Award No. N000141712577.

10.1016/j.ifacol.2021.08.484

the preservation of controllers, guarantee the preservation of *robustness* of the controllers. Our focus in not on the algorithmic aspects of abstractions, but on the foundations for the design of abstraction algorithms, namely, to understand the relation between the given dynamical system (concrete system) and the abstract system that preserves the existence of robust controllers. The proofs in the paper have been eliminated due to lack of space.

1.1 Related Work

Robustness plays a central role in control design, because imperfections are ubiquitous in the modelling, sensing, computation, communication, and actuation aspects of practical control systems. For this reason, robust control has become a standard topic in control theory Dullerud and Paganini (2013); Zhou and Doyle (1998). In the context of embedded and cyber-physical systems, how to design robust control software has been identified as one of the major challenges Henzinger (2008). For limited class of systems modelled as finite-state systems or timed automata, decision procedures for synthesizing robust controllers have been studied Bloem et al. (2014); Sankur et al. (2013); Topcu et al. (2012); Majumdar et al. (2011). In this paper, we are interested in the robust controller synthesis problem for a general class of systems that include switched and hybrid systems.

One of the promising approaches for effective design of control software for switched and hybrid systems is through abstraction-based methods and using notions such as approximate alternating simulations. Belta et al. (2017); Kloetzer and Belta (2008); Pola and Tabuada (2009); Rungger and Zamani (2016); Tabuada et al. (2002); Tabuada (2009); Nilsson et al. (2017); Reissig et al. (2017); Zamani et al. (2012). We note that earlier work on approximate alternating simulations Pola and Tabuada (2009); Zamani et al. (2012) did not directly address robustness issues as pointed out in Liu and Ozay (2014); Reissig et al. (2017). We also note that a different quantitative robustness notion (similar to input-output gain) is proposed in Tarraf et al. (2008) and abstractions that preserve such robustness notions have also been introduced in Tarraf (2012); Rungger and Tabuada (2014). These results are complementary to the results of this paper, because we focus on robustness of controllers satisfying linear time properties.

2. PRELIMINARIES

In this section, we introduce formally some preliminary concepts related to transition systems and controllers.

Given a set A, we use A^* to denote the set of finite sequences over A, that is, all sequences $w = a_0 a_1 \dots a_k$, where $a_i \in A$ for all $0 \leq i \leq k$. The i-the element of the sequence w, namely, a_i is denoted by $w(i)$, and the last element of w, a_k, is denoted by $last(w)$. We use $|w|$ to denote the length of sequence w, namely, k. We use $A \cdot B$ to denote the set of all finite sequences ab, where $a \in A$ and $b \in B$.

2.1 Metric Transition Systems.

We will consider transition systems enriched with metric on both the state space as well as the action space, that can capture perturbations on the states, inputs, and sampling times. The actions can be used to model both the control inputs as well as time delays in a dynamical system. The correct behaviors of a system are specified as properties on observable states and inputs and hence, we introduce both state labels and action labels.

Definition. A *metric transition system* is a tuple $\mathcal{T} = (\mathcal{Q}, d^{\mathcal{Q}}, \mathcal{A}, d^{\mathcal{A}}, \longrightarrow, \Pi^{\mathcal{Q}}, \Pi^{\mathcal{A}}, \mathcal{L}^{\mathcal{Q}}, \mathcal{L}^{\mathcal{A}})$, where

- $\mathcal{Q}$ is a set of states;
- $d^{\mathcal{Q}} : \mathcal{Q} \times \mathcal{Q} \to \mathbb{R}^{\infty}_{+}$ is a (pseudo)-metric on $\mathcal{Q}$;
- $\mathcal{A}$ is a set of actions;
- $d^{\mathcal{A}} : \mathcal{A} \times \mathcal{A} \to \mathbb{R}^{\infty}_{+}$ is a (pseudo)-metric on $\mathcal{A}$;
- $\longrightarrow \subseteq \mathcal{Q} \times \mathcal{A} \times \mathcal{Q}$ is a transition relation;
- $\Pi^{\mathcal{Q}}$ is a set of state labels;
- $\Pi^{\mathcal{A}}$ is a set of action labels;
- $\mathcal{L}^{\mathcal{Q}} : \mathcal{Q} \to 2^{\Pi^{\mathcal{Q}}}$ is a state labelling function; and
- $\mathcal{L}^{\mathcal{A}} : \mathcal{A} \to 2^{\Pi^{\mathcal{A}}}$ is an action labelling function.

We will often refer to a metric transition system as just a system or a transition system. A transition $(q, a, q') \in \longrightarrow$ states that a system in state q upon taking action a reaches the state q'; the action a can capture control inputs and/or time elapse. We will also denote a transition $(q, a, q') \in \longrightarrow$ as $q \xrightarrow{a} q'$. The sets $\Pi^{\mathcal{Q}}$ and $\Pi^{\mathcal{A}}$ consist of state and action labels, respectively, that are interpreted as the observable part/feature of the state/action. We specify the correctness of a controlled system using these observations. We will often use subscripts to refer to the components of a transition system, for instance, $\mathcal{Q}_{\mathcal{T}}$ will refer to the states of $\mathcal{T}$ and $\mathcal{L}^{\mathcal{Q}}_{\mathcal{T}}$ will refer to the state labelling function of $\mathcal{T}$. When it is clear from the context, we will drop the subscript.

An *execution* of $\mathcal{T}$ is an alternating sequence of (finite or infinite) states and actions that correspond to a sequence of transitions, that is, of the form $\rho = q_0 a_0 q_1 a_1 q_2 a_2 \dots$, where $(q_i, a_i, q_{i+1}) \in \longrightarrow$ for all $i \geq 0$. We will also represent it as $\rho = q_0 \xrightarrow{a_0} q_1 \xrightarrow{a_1} q_2 \dots$. We refer to the sequence of states appearing in an execution as a path, that is, the *path* associated with the execution ρ above is $Path(\rho) = q_0 q_1 q_2 \dots$. We refer to the sequence of state and action labels of an execution as a trace; it is the observable behavior the system. The *trace* of the execution ρ is defined by

$$Trace(\rho) = \mathcal{L}^{\mathcal{Q}}(q_0)\mathcal{L}^{\mathcal{A}}(a_0)\mathcal{L}^{\mathcal{Q}}(q_1)\mathcal{L}^{\mathcal{A}}(a_1)\mathcal{L}^{\mathcal{Q}}(q_2)\dots.$$

The executions, paths and traces can be finite or infinite.

We define the states that can be reached from a state q by applying an action a, using the predicate $Post_{\mathcal{T}}(q, a)$ as follows:

$$Post_{\mathcal{T}}(q, a) = \{q' | (q, a, q') \in \longrightarrow_{\mathcal{T}}\}$$

We say that an action a is *enabled* at a state q if $Post_{\mathcal{T}}(q, a) \neq \emptyset$, that is, there is a q' such that $(q, a, q') \in \longrightarrow$. We denote the set of all actions that are enabled at q by $Enable_{\mathcal{T}}(q)$.

A *strategy* for a transition system $\mathcal{T}$ is a partial function $\mu{:}(\mathcal{Q}\cdot\mathcal{A})^*\mathcal{Q} \to \mathcal{A}$, such that the the action $\mu(q_0a_0q_1a_1\dots a_{n-1}q_n)$ is enabled at q_n. A *μ-controlled execution* of a transition system $\mathcal{T}$ is an execution of $\mathcal{T}$, where for each $i \geq 0$, the action a_i is chosen according to the control strategy μ. That is, $\rho = q_0a_0q_1a_1q_2a_2\dots$, is a μ-controlled execution of $\mathcal{T}$ if $\mu(q_0a_0q_1\dots a_{i-1}q_i) = a_i$ for all i. μ-controlled paths and traces will be paths and traces corresponding to μ-controlled executions. We say that a strategy μ is *complete* for q if $\mu(q_0a_0q_1a_1\dots a_{n-1}q_n)$ is defined for every μ-controlled finite execution $q_0a_0q_1a_1q_2a_2\dots a_{n-1}q_n$, where $q_0 = q$. Hence, the system does not get stuck if it is following a certain strategy because of the controller action not being defined. We will assume that all strategies are complete with respect to the state under consideration and hence, will not explicitly state it.

Given a set X, let X^ω denote all the infinite sequences over X. A *property* over X is a subset of X^ω. In general, the control problem is to construct a strategy μ, given a system $\mathcal{T}$ and a property $\mathcal{P}$ over $2^{\Pi^{\mathcal{Q}}\times\Pi^{\mathcal{A}}}$, such that all the μ-controlled traces of $\mathcal{T}$ are in $\mathcal{P}$.

Definition.[Winning strategy under Ideal assumptions] Given a transition system $\mathcal{T}$, a state q_0 and a property $\mathcal{P}$, a strategy μ is a *winning* strategy for $\mathcal{T}, q_0$ and $\mathcal{P}$, if the traces of all μ-controlled executions of $\mathcal{T}$ starting at q_0 are in $\mathcal{P}$.

Problem.[Control problem under ideal assumptions] Given a transition system $\mathcal{T}$, a state q_0 and a property $\mathcal{P}$, construct a winning strategy μ for $\mathcal{T}, q_0$ and $\mathcal{P}$.

The above control problem is formulated under the ideal assumption that there are no sensing/actuation errors, delays or uncertain dynamics. In Section 3, we formulate control problems which incorporate these imperfections.

2.2 Switched Systems

A *switched system* $\mathcal{S} = \{f_m\}_{m\in M}$, where M is a finite set of modes, and for each m, $f_m : \mathbb{R}^n \to \mathbb{R}^n$ defines the dynamics associated with mode m. A function $x : [0,T] \to \mathbb{R}^n$ is said to be a *solution* of dynamics f_m if

$$\frac{dx}{dt}(t') = f_m(x(t')), \quad \forall t' \in [0,T]. \tag{1}$$

We say that x is an execution starting from $x(0)$.

We can represent the switched system $\mathcal{S}$ as a metric transition system. Let $\mathcal{L}^{\mathcal{Q}} : \mathbb{R}^n \to 2^{\Pi^{\mathcal{Q}}}$ and $\mathcal{L}^{\mathcal{A}} : \mathbb{R}^{d+1} \to 2^{\Pi^{\mathcal{A}}}$ be given labelling functions. The corresponding metric transition system $\mathcal{T}_{\mathcal{S}} = (\mathcal{Q}, d^{\mathcal{Q}}, \mathcal{A}, d^{\mathcal{A}}, \longrightarrow, \Pi^{\mathcal{Q}}, \Pi^{\mathcal{A}}, \mathcal{L}^{\mathcal{Q}}, \mathcal{L}^{\mathcal{A}})$, where:

- $\mathcal{Q} = \mathbb{R}^n$ is the set of states;
- $d^{\mathcal{Q}}$ is the Euclidean distance on $\mathcal{Q}$;
- $\mathcal{A} = \mathbb{R}_+ \times M$ is the set of actions;
- $d^{\mathcal{A}}$ is a metric on $\mathcal{A}$ defined as $d^{\mathcal{A}}((t_1,m_1),(t_2,m_2)) = |t_1 - t_2|$ if $m_1 = m_2$, and ∞ otherwise; and
- $\longrightarrow \subseteq \mathcal{Q}\times\mathcal{A}\times\mathcal{Q}$ is the transition relation that is defined by

  $(q,(t,m),q') \in \longrightarrow$ if there exists a solution $x : [0,t] \to \mathbb{R}^n$ of f_m such that $x(0) = q$, and $x(t) = q'$.

A switching control is a piecewise constant signal $\sigma : [0,\infty) \to M$, where for any t, $\sigma(t)$ specifies the mode in which the system operates at time t. A periodic switching control with period τ is a switching control σ such that $\sigma(t)$ is constant in the interval $[i\tau,(i+1)\tau)$ for every i. A switching control σ with period τ can be captured by a strategy μ such that $\mu(q_0a_0q_1a_1\dots a_{i-1}q_i) = (\tau,\sigma(i\tau))$.

3. ROBUST CONTROLLER SYNTHESIS PROBLEMS

We defined the control problem under ideal assumptions where we seek a strategy such that the traces of the executions conformant with the strategy satisfy a given property. However, a practical implementation of the strategy will not satisfy the assumptions under which the strategy guarantees the property. In this section, we propose several notions of robust strategies that are intended to capture controllers that are robust to sensor/actuator noise, computation/communication delays and uncertain dynamics. More precisely, we define three notions of robust strategies:

- $1,\delta$*-robust strategies*: Strategies robust to δ-(state) measurement errors.
- $2,\delta$*-robust strategies*: Strategies robust to δ-action errors, that can capture strategies robust to δ-actuation errors as well as strategies robust to δ-delays.
- $3,\delta$*-robust strategies*: Strategies robust to δ-uncertainty in the dynamics.

Our main result is that under certain constraints on the transition relation, 3-robust strategies are stronger than 1 and 2-robust strategies in that if there is $3,\delta$-robust winning strategy for a system, then there is a $1,\delta_1$ and a $2,\delta_2$-robust winning strategy for some δ_1 and δ_2. Next we formulate control problems which incorporate these imperfections.

3.1 Control problem with measurement errors

The objective is to synthesize a controller that is robust to state measurement errors up to a bound δ. More precisely, we are interested in synthesizing a control strategy that suggests the next action based on the observed state sequence $\hat{\rho} = \hat{q}_0a_0\hat{q}_1a_1\dots a_{k-1}\hat{q}_k$ instead of an actual execution $\rho = q_0a_0q_1a_1\dots a_{k-1}q_k$, where the sensor measurement errors are bounded by δ, that is, $d^{\mathcal{Q}}(\hat{q}_i,q_i) \leq \delta$ for all i.

Definition. Given a system $\mathcal{T}$, a strategy μ and $\delta \geq 0$, a sequence $\hat{\rho} = \hat{q}_0a_0\hat{q}_1a_1\dots a_{k-1}\hat{q}_k$ is said to be *μ-observable* under δ measurement errors in $\mathcal{T}, q_0$, if there is an execution $\rho = q_0a_0q_1\dots a_{k-1}q_k$ of $\mathcal{T}$ such that $d^{\mathcal{Q}}(\hat{q}_i,q_i) \leq \delta$ and $\mu(\hat{q}_0a_0\hat{q}_1a_1\dots a_{i-1}\hat{q}_i) = a_i$ for all $0 \leq i < k$. We call ρ a witness for $\hat{\rho}$.

Definition. Given a system $\mathcal{T}$, a strategy μ and $\delta \geq 0$, an execution $\rho = q_0a_0q_1a_1\dots$ of $\mathcal{T}$ is said to be *δ-measurement error μ-conformant* if there is a sequence $\hat{\rho} = \hat{q}_0a_0\hat{q}_1a_1\dots$ such that $d^{\mathcal{Q}}(\hat{q}_i,q_i) \leq \delta$ and $\mu(\hat{q}_0a_0\hat{q}_1a_1\dots a_{i-1}\hat{q}_i) = a_i$ for all $i \geq 0$.

Definition.[Strategy robust to sensor measurement errors] Given a system $\mathcal{T}$, a state q_0 and a property $\mathcal{P}$, a strategy μ is said to be a $1,\delta$-robustly winning for $\mathcal{T}, q$ and $\mathcal{P}$ if

- for all $\hat{\rho}$ that is μ-observable under δ-measurement errors in $\mathcal{T}, q_0$, $\mu(\hat{\rho})$ is defined and enabled at all states in $B_\delta(last(\hat{\rho}))$;
- the trace of every δ-measurement error μ-conformant execution ρ of $\mathcal{T}$ from q_0 is in $\mathcal{P}$.

The robust control problem with respect to measurement errors seeks a controller that is robustly winning with respect to sensor measurement errors.

Problem.[Control problem with measurement errors] Given a transition system $\mathcal{T}$, a state q_0, $\delta \geq 0$, and a property $\mathcal{P}$, construct a $1,\delta$-robust winning strategy μ for $\mathcal{T}, q_0$ and $\mathcal{P}$.

3.2 Control problem with actuation errors and delays

Next, we consider the problem of controller synthesis under actuation errors and delays. In our framework, the control input and delays are both captured using actions, hence, we formulate a controller synthesis problem under perturbations to actions, wherein a small perturbation of the action is applied to the plant instead of the action suggested/computed by the controller.

Definition. Given a system $\mathcal{T}$, a strategy μ and $\delta \geq 0$, a sequence $\hat{\rho} = q_0\hat{a}_0q_1\hat{a}_1\dots\hat{a}_{k-1}q_k$ is said to be *μ-observable* under δ action errors in $\mathcal{T}$, if there is an execution $q_0a_0q_1\dots a_{k-1}q_k$ of $\mathcal{T}$ such that $d^{\mathcal{A}}(\hat{a}_i, a_i) \leq \delta$ and $\mu(q_0\hat{a}_0q_1\hat{a}_1\dots\hat{a}_{i-1}q_i) = \hat{a}_i$ for all $0 \leq i < k$.

Definition. Given a system $\mathcal{T}$, a strategy μ and $\delta \geq 0$, an execution $\rho = q_0a_0q_1a_1\dots$ of $\mathcal{T}$ is said to be *δ-action error μ-conformant* if there is a sequence $\hat{\rho} = q_0\hat{a}_0q_1\hat{a}_1\dots$ such that $d^{\mathcal{A}}(\hat{a}_i, a_i) \leq \delta$ and $\mu(q_0\hat{a}_0q_1\hat{a}_1\dots\hat{a}_{i-1}q_i) = \hat{a}_i$ for all $i \geq 0$.

Definition.[Strategy robust to actuation errors and delays] Given a system $\mathcal{T}$, a state q_0 and a property $\mathcal{P}$, a strategy μ is said to be a $2,\delta$-robustly winning for $\mathcal{T}, q_0$ and $\mathcal{P}$ if

- for all $\hat{\rho}$ from q_0 that is μ-observable under δ-action errors in $\mathcal{T}$, $\mu(\hat{\rho})$ is defined and $B_\delta(\mu(\hat{\rho})) \subseteq Enable_{\mathcal{T}}(last(\hat{\rho}))$;
- the trace of every δ-action error μ-conformant execution ρ of $\mathcal{T}$ from q_0 is in $\mathcal{P}$.

The control problem with action errors seeks a a winning strategy that is robust to action errors.

Problem.[Control problem with action errors] Given a transition system $\mathcal{T}$, a state q_0, $\delta \geq 0$, and a property $\mathcal{P}$, construct a $2,\delta$-robust winning strategy μ for $\mathcal{T}, q_0$ and $\mathcal{P}$.

Remark. Note that actuation errors and delays can be captured by appropriately defining the metric on the action space $\mathbb{R}_+ \times \mathcal{U}$ of a dynamical system. More precisely, considering $d^{\mathcal{A}}((t_1, a_1), (t_2, a_2)) = |t_1 - t_2|$ if $a_1 = a_2$ and ∞ otherwise, captures time delays, while considering $d^{\mathcal{A}}((t_1, a_1), (t_2, a_2)) = \|a_1 - a_2\|$ if $t_1 = t_2$ and ∞, otherwise, will capture input perturbations, that is, actuator noise. If we want to consider both delays and actuator noise simultaneously, we could consider the metric, where $d^{\mathcal{A}}((t_1, a_1), (t_2, a_2)) = \max\{|t_1 - t_2|, \|a_1 - a_2\|\}$.

3.3 Control problem with uncertain dynamics

Our final notion of robustness intends to capture robustness with respect to measurement errors and action errors. We consider strategies that are robust to perturbations in the dynamics which are modelled in our framework using transitions in a metric transition system.

Definition.[δ-perturbed metric transition system] Given a metric transition system $\mathcal{T} = (\mathcal{Q}, d^{\mathcal{Q}}, \mathcal{A}, d^{\mathcal{A}}, \longrightarrow, \Pi^{\mathcal{Q}}, \Pi^{\mathcal{A}}, \mathcal{L}^{\mathcal{Q}}, \mathcal{L}^{\mathcal{A}})$ and a number $\delta \geq 0$, define the δ-perturbation of $\mathcal{T}$, denoted by $\mathcal{T}_\delta$, as $\mathcal{T}_\delta = (\mathcal{Q}, d^{\mathcal{Q}}, \mathcal{A}, d^{\mathcal{A}}, \longrightarrow_\delta, \Pi^{\mathcal{Q}}, \Pi^{\mathcal{A}}, \mathcal{L}^{\mathcal{Q}}, \mathcal{L}^{\mathcal{A}})$, where $\longrightarrow_\delta \{(q_1, a, q_2) : \exists(q_1, a', q_2') \in \longrightarrow$ s.t. $d^{\mathcal{Q}}(q_1, q_1') \leq \delta, d^{\mathcal{A}}(a, a') \leq \delta\}$.

Definition. Given an execution $\rho = q_0a_0q_1a_1\dots$, $B_\delta(\rho) = \{\rho' \mid \rho' = q_0'a_0'q_1'a_1'\dots, \forall i, d^{\mathcal{Q}}(q_i, q_i') \leq \delta, d^{\mathcal{A}}(a_i, a_i') \leq \delta\}$.

Definition. Given a system $\mathcal{T}$, state q_0 and property $\mathcal{P}$, a control strategy μ is said to be a $3,\delta$-robustly winning strategy for $\mathcal{T}, q_0$ and $\mathcal{P}$, if $Trace(\rho')$ is in $\mathcal{P}$ for every $\rho' \in B_\delta(\rho)$ for some μ-controlled execution ρ of $\mathcal{T}_\delta$ from q_0.

The control problem with uncertain dynamics seeks a a $3,\delta$-winning strategy.

Problem.[Control problem with uncertain dynamics] Given a transition system $\mathcal{T}$, a state q_0, $\delta \geq 0$, and a property $\mathcal{P}$, construct a $3,\delta$-robust winning strategy μ for $\mathcal{T}, q_0$ and $\mathcal{P}$.

4. RELATION BETWEEN ROBUST CONTROL PROBLEMS

In Section 3, we defined three robust controller synthesis problems, and establish the relationship between the three problems. We show that the control problems with measurement errors and action errors can be transformed to the control problem with uncertain dynamics.

4.1 Transformation from control problem with measurement errors to that with uncertain dynamics

The broad intuition is that the measurement error can be embedded into the uncertainty in the dynamics if the behaviors from the actual state and the measured state are close.

Definition. We say that $\mathcal{T}$ is *uniformly continuous with respect to states*, if for any $\varepsilon > 0$, there exists some $\gamma > 0$

such that for all states q_0, q_1, if $d^{\mathcal{Q}}(q_0, q_1) \leq \gamma$, then for each $(q_0, a, q_0') \in \longrightarrow$, there exists $(q_1, a, q_1') \in \longrightarrow$ such that $d^{\mathcal{Q}}(q_0', q_1') \leq \varepsilon$.

Theorem. Let $\mathcal{T}$ be a metric transition system that is uniformly continuous with respect to states, q_0 be a state of $\mathcal{T}$ and $\delta > 0$. If μ is a $3, \delta$-robust winning strategy for $\mathcal{T}, q_0'$ and $\mathcal{P}$ for every $q_0' \in B_\delta(q_0)$, then there exists a $\delta' > 0$ and a strategy μ' such that μ' is a $1, \delta'$-robust winning strategy for $\mathcal{T}, q_0$ and $\mathcal{P}$.

4.2 Transformation from control problem with action errors to that with uncertain dynamics

Again, the broad intuition is that the action errors can be embedded into the uncertainty in the dynamics if behavior of the system in reaction to the actual action and perturbed action are close.

Definition. We say that $\mathcal{T}$ is *uniformly continuous with respect to actions*, if for any $\varepsilon > 0$, there exists some $\gamma > 0$ such that for all actions a_0, a_1, if $d^{\mathcal{A}}(a_0, a_1) \leq \gamma$, then for each $(q_0, a_0, q_0') \in \longrightarrow$, there exists $(q_0, a_1, q_1') \in \longrightarrow$ such that $d^{\mathcal{Q}}(q_0', q_1') \leq \varepsilon$.

Theorem. Let $\mathcal{T}$ be a metric transition system that is uniformly continuous with respect to actions, q_0 be a state of $\mathcal{T}$ and $\delta > 0$. If μ is a $3, \delta$-robust winning strategy for $\mathcal{T}, q_0$ and $\mathcal{P}$, then there exists a $\delta' > 0$ and a strategy μ' such that μ' is a $1, \delta'$-robust winning strategy for $\mathcal{T}, q_0$ and $\mathcal{P}$.

Remark. In fact, the proof of Theorem 4.1 only requires perturbations on the target states in the definition of $\mathcal{T}_\delta$, and similarly, the proof of Theorem 4.2 only requires perturbations on the actions in the definition of $\mathcal{T}_\delta$.

Remark. Note that the computation of δ' corresponding to δ in Theorems 4.1 and 4.2 relies on being able to compute the γ corresponding to $\epsilon = \delta$ in Definitions 4.1 and 4.2. If we replace uniform continuity with Lipschitz continuity, we can get an explicit relation between ϵ and γ. Further, note that the strategy μ' is essentially the same as μ, hence, $1, \delta'$ and $2, \delta'$ strategies can be computed given a $3, \delta$ strategy.

5. PRE-ORDERS PRESERVING ROBUST CONTROLLERS

The objective of this section is to investigate pre-orders on transition systems that "preserve" the robust controllers. Theorems 4.1 and 4.2 suggest that a 1-robust and a 2-robust strategy can be constructed from a 3-robust strategy if certain parameters of the uniform continuity of the transition system can be computed as explained in Remark 4.2. Hence, we focus on synthesis of $3, \delta$-robust winning strategies, that is, the control problem with respect to uncertain dynamics.

Abstractions are key toward scalable verification and synthesis; the foundations of abstractions lie in understanding relation between systems that preserve property satisfaction and existence of controllers. We explore notions similar to simulations that preserve the existence of robust controllers.

Definition. Given two metric transition systems $\mathcal{T}_1 = (\mathcal{Q}_1, d_1^{\mathcal{Q}}, \mathcal{A}_1, d_1^{\mathcal{A}}, \longrightarrow_1, \Pi_1^{\mathcal{Q}}, \Pi_1^{\mathcal{A}}, \mathcal{L}_1^{\mathcal{Q}}, \mathcal{L}_1^{\mathcal{A}})$, and $\mathcal{T}_2 = (\mathcal{Q}_2, d_2^{\mathcal{Q}}, \mathcal{A}_2, d_2^{\mathcal{A}}, \longrightarrow_2, \Pi_2^{\mathcal{Q}}, \Pi_2^{\mathcal{A}}, \mathcal{L}_2^{\mathcal{Q}}, \mathcal{L}_2^{\mathcal{A}})$, a pair of relations $\mathcal{R} = (\mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{A}})$, where $\mathcal{R}_{\mathcal{Q}} \subseteq \mathcal{Q}_1 \times \mathcal{Q}_2$ and $\mathcal{R}_{\mathcal{A}} \subseteq \mathcal{A}_1 \times \mathcal{A}_2$, is said to be an *alternating simulation relation* from $\mathcal{T}_1$ to $\mathcal{T}_2$, denoted, $\mathcal{T}_1 \preceq_{\mathcal{R}} \mathcal{T}_2$, if the following conditions are satisfied:

(i) for all $(q_1, q_2) \in \mathcal{R}_{\mathcal{Q}}$, $\mathcal{L}_1^{\mathcal{Q}}(q_1) = \mathcal{L}_2^{\mathcal{Q}}(q_2)$;
(ii) for all $(a_1, a_2) \in \mathcal{R}_{\mathcal{A}}$, $\mathcal{L}_1^{\mathcal{A}}(a_1) = \mathcal{L}_2^{\mathcal{A}}(a_2)$; and
(iii) for all $(q_1, q_2) \in \mathcal{R}_{\mathcal{Q}}$, for all $a_2 \in Enable_{\mathcal{T}_2}(q_2)$, there exists $a_1 \in Enable_{\mathcal{T}_1}(q_1)$ such that $(a_1, a_2) \in \mathcal{R}_{\mathcal{A}}$, and for every $q_1' \in Post_{\mathcal{T}_1}(q_1, a_1)$, there exists $q_2' \in Post_{\mathcal{T}_2}(q_2, a_2)$ with $(q_1', q_2') \in \mathcal{R}_{\mathcal{Q}}$.

The following definition captures when two executions are related by an alternating simulation relation.

Definition. Given metric transition systems $\mathcal{T}_1$ and $\mathcal{T}_2$, an alternating simulation relation $\mathcal{R} = (\mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{A}})$ from $\mathcal{T}_1$ to $\mathcal{T}_2$ and two executions $\rho = q_0 a_0 q_1 a_1 \ldots$ and $\rho' = q_0' a_0' q_1' a_1' \ldots$ from $\mathcal{T}_1$ and $\mathcal{T}_2$, respectively, we say that ρ and ρ' are related by $\mathcal{R}$, denoted $\mathcal{R}(\rho, \rho')$, if $|\rho| = |\rho'|$, and $\mathcal{R}_{\mathcal{Q}}(q_i, q_i')$ and $\mathcal{R}_{\mathcal{A}}(a_i, a_i')$ for all $i \geq 0$.

Alternating simulation guarantees that if states q_1 and q_2 are related by $\mathcal{R}_{\mathcal{A}}$, then a winning strategy from q_2 for a property $\mathcal{P}$ guarantees the existence of a winning strategy from q_1. However, a robust winning strategy from q_2 does not necessarily translate to a robust winning strategy from q_1. Hence, we explore pre-orders that can enforce preservation of robust controllers. We define the notion of a uniformly continuous alternating simulation relation inspired by the definition of uniformly continuous simulations in Prabhakar et al. (2017). First, we define a uniform continuity of a relation.

Definition. A relation $X \subseteq A \times A$ on a metric space (A, d) is said to be *uniformly continuous* if for every $\epsilon > 0$, there exists a $\delta > 0$, such that for all $(a_1, a_2) \in X$ and $a_1' \in B_\delta(a_1)$, there exists $a_2' \in B_\epsilon(a_2)$ with $(a_1', a_2') \in X$.

A uniformly continuous alternating simulation relation from $\mathcal{T}_1$ to $\mathcal{T}_2$ is an alternating simulation relation, such that the corresponding relations on the states and actions are uniformly continuous.

Definition. An alternating simulation relation $\mathcal{R} = (\mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{A}})$ from $\mathcal{T}_1$ to $\mathcal{T}_2$ is said to be *uniformly continuous* if both $\mathcal{R}_{\mathcal{Q}}$ and $\mathcal{R}_{\mathcal{A}}$ are uniformly continuous relations.

The next theorem essentially states that if two systems are related by a uniformly continuous alternating simulation relation, then it preserves robust controllers with respect to uncertain dynamics.

Theorem. Let $\mathcal{T}_1 = (\mathcal{Q}_1, d_1^{\mathcal{Q}}, \mathcal{A}_1, d_1^{\mathcal{A}}, \longrightarrow_1, \Pi_1^{\mathcal{Q}}, \Pi_1^{\mathcal{A}}, \mathcal{L}_1^{\mathcal{Q}}, \mathcal{L}_1^{\mathcal{A}})$ and $\mathcal{T}_2 = (\mathcal{Q}_2, d_2^{\mathcal{Q}}, \mathcal{A}_2, d_2^{\mathcal{A}}, \longrightarrow_2, \Pi_2^{\mathcal{Q}}, \Pi_2^{\mathcal{A}}, \mathcal{L}_2^{\mathcal{Q}}, \mathcal{L}_2^{\mathcal{A}})$ be metric transition systems and $\mathcal{P}$ be a property. Let $\mathcal{R} = (\mathcal{R}_{\mathcal{Q}}, \mathcal{R}_{\mathcal{A}})$ be a uniformly continuous alternating simula-

tion relation from $\mathcal{T}_1$ to $\mathcal{T}_2$. Let $q_1 \in \mathcal{Q}_1$ and $q_2 \in \mathcal{Q}_2$ be two states such that $(q_1, q_2) \in \mathcal{R}_{\mathcal{Q}}$. If there is a $3, \delta_2$-robust winning strategy for $\mathcal{T}_2$ with respect to $\mathcal{P}$ from q_2 for some $\delta_2 > 0$, then there is a $3, \delta_1$-robust winning strategy for $\mathcal{T}_1$ with respect to $\mathcal{P}$ from q_1 for some $\delta_1 > 0$.

6. CONCLUSION

In this paper, we formalized the robust controller synthesis problems with respect to sensor measurement errors, actuation errors and processing delays using a generalized framework of metric timed transition systems. We showed that a robust controller with respect to the above perturbations can be computed by synthesizing a controller that is robust to perturbations in the transitions of the system. Next, we investigated preorders on systems that preserve robust controllers, and proposed the notion of uniformly continuous alternating simulation relations. This will serve as the foundation for abstraction-based synthesis of robust controllers. In the future, we intend to investigate abstraction techniques, including finite-state abstractions, for the purpose of robust controller synthesis based on these foundations.

REFERENCES

Alur, R., Henzinger, T., Kupferman, O., and Vardi, M. (1998). Alternating refinement relations. In *Proc. 9th Conferance on Concurrency Theory*, Lecture Notes in Computer Science. Springer-Verlag, Nice.

Baier, C. and Katoen, J.P. (2008). *Principles of Model Checking (Representation and Mind Series)*. The MIT Press.

Belta, C., Yordanov, B., and Gol, E.A. (2017). *Formal Methods for Discrete-Time Dynamical Systems*, volume 89. Springer.

Bloem, R., Chatterjee, K., Greimel, K., Henzinger, T.A., Hofferek, G., Jobstmann, B., Könighofer, B., and Könighofer, R. (2014). Synthesizing robust systems. *Acta Inf.*, 51(3-4), 193–220.

DeCastro, J.A. and Kress-Gazit, H. (2013). Guaranteeing reactive high-level behaviors for robots with complex dynamics. In *IEEE/RSJ International Conference on Intelligent Robots and Systems*, 749–756.

Dullerud, G.E. and Paganini, F. (2013). *A Course in Robust Control Theory: A Convex Approach*, volume 36. Springer Science & Business Media.

Grädel, E., Thomas, W., and Wilke, T. (eds.) (2002). *Automata, Logics, and Infinite Games: A Guide to Current Research*, volume 2500 of *Lecture Notes in Computer Science*. Springer.

Henzinger, T., Kopke, P., Puri, A., and Varaiya, P. (1995). What's decidable about hybrid automata? In *Proceedings of the ACM Symposium on Theory of Computation*, 373–382.

Henzinger, T.A. (2008). Two challenges in embedded systems design: predictability and robustness. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 366(1881), 3727–3736.

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

Liu, J. and Ozay, N. (2014). Abstraction, discretization, and robustness in temporal logic control of dynamical systems. In *Proceedings of the 17th international conference on Hybrid systems: computation and control*, 293–302. ACM.

Majumdar, R., Render, E., and Tabuada, P. (2011). Robust discrete synthesis against unspecified disturbances. In *Proc. of HSCC*, 211–220.

Nilsson, P., Ozay, N., and Liu, J. (2017). Augmented finite transition systems as abstractions for control synthesis. *Discrete Event Dynamic Systems*, 27(2), 301–340.

Pola, G. and Tabuada, P. (2009). Symbolic models for nonlinear control systems: Alternating approximate bisimulations. *SIAM Journal on Control and Optimization*, 48(2), 719–733.

Prabhakar, P., Liu, J., and Murray, R.M. (2017). Simulations and bisimulations for analysis of stability with respect to inputs of hybrid systems. *Discrete Event Dynamic Systems*, 1–26.

Reissig, G., Weber, A., and Rungger, M. (2017). Feedback refinement relations for the synthesis of symbolic controllers. *IEEE Transactions on Automatic Control*, 62(4), 1781–1796.

Rungger, M. and Tabuada, P. (2014). Abstracting and refining robustness for cyber-physical systems. In *Proc. of HSCC*, 223–232.

Rungger, M. and Zamani, M. (2016). Scots: A tool for the synthesis of symbolic controllers. In *Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control*, 99–104. ACM.

Sankur, O., Bouyer, P., Markey, N., and Reynier, P. (2013). Robust controller synthesis in timed automata. In *CONCUR 2013 - Concurrency Theory - 24th International Conference, CONCUR 2013, Buenos Aires, Argentina, August 27-30, 2013. Proceedings*, 546–560.

Tabuada, P. (2009). *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media.

Tabuada, P., Pappas, G.J., and Lima, P.U. (2002). Composing abstractions of hybrid systems. In *Proceedings of the International Conference on Hybrid Systems: Computation and Control*, 436–450.

Tarraf, D., Megretski, A., and Dahleh, M.A. (2008). A framework for robust stability of systems over finite alphabets. *IEEE Transactions on Automatic Control*, 53(5), 1133–1146.

Tarraf, D.C. (2012). A control-oriented notion of finite state approximation. *IEEE transactions on automatic control*, 57(12), 3197–3202.

Topcu, U., Ozay, N., Liu, J., and Murray, R.M. (2012). On synthesizing robust discrete controllers under modeling uncertainty. In *Proc. of HSCC*, 85–94.

Wongpiromsarn, T., Topcu, U., Ozay, N., Xu, H., and Murray, R. (2011). TuLiP: a software toolbox for receding horizon temporal logic planning. In *Hybrid Systems: Computation and Control*, 313–314.

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

Zhou, K. and Doyle, J.C. (1998). *Essentials of Robust Control*, volume 104. Prentice hall Upper Saddle River, NJ.