An interval analysis approach to invariance control synthesis for discrete-time switched systems

Yinan Li and Jun Liu

Abstract— **Safety control constitutes an important aspect of hybrid systems and control. Invariance controllers guarantee that a system can stay within a given safe set for all future time. While abstraction-based approach to control synthesis takes the advantages of formal methods in automatic synthesis, abstractions often introduce spurious transitions that can lead to failure of controller synthesis for a given specification, even though the original system can be controlled to satisfy this specification. For discrete-time switched systems, this paper presents an interval arithmetic-based approach for invariance control synthesis. The main synthesis algorithms rely on partition refinement techniques and backward reachable set computation using interval analysis. The use of rigorous numerics allow us to prove formal guarantees of finding an invariance controller via abstraction refinement, provided that a robustly invariant condition is satisfied for the original switched system. The results are illustrated with polynomial dynamics.**

I. INTRODUCTION

The switched systems considered in this paper are the hybrid systems whose control variables are restricted to the discrete modes only. This restriction often makes conventional control methods difficult to apply [1]. Control of switched systems arises in a variety of applications, e.g., switching control of converters [2], multi-mode engines [3], robotics [4], etc.

Abstraction-based approaches gained popularity in recent years for solving control problems for hybrid systems from high-level specifications. The underlying principle is to search for discrete controllers in finite abstractions of the original systems with continuous or hybrid dynamics, avoiding handling highly nontrivial dynamics and rich specifications at the same time. Leveraging the advantages of formal methods for automatic searching and verification, such approaches are successfully applied to synthesize controllers for dynamical systems from relatively complex specifications, e.g., control of linear systems [5], piecewise affine systems [6], and nonlinear systems [7], [8] from temporal logic specifications, with applications in robotics [9], electric power systems [10], automotive adaptive cruise control [11].

Most abstractions considered in the literature are conservative approximations of the original system models, with the exception of bisimilar symbolic models that can be constructed for incrementally stable systems [12], [13]. Without such stability assumptions, over-approximations [7], [8], [14] and alternatingly similar models [15] can be computed for nonlinear systems. These conservative abstractions are sound in the sense that, if a discrete controller can be found, it is guaranteed to work for the original system. However, they may contain spurious transitions that can lead to infeasibility of the discrete synthesis problem, despite that there may exist a controller for the original system. To mitigate the conservativeness of abstractions, abstraction refinement techniques are introduced [16] and better approximations via local reachable set computation are considered [17]. Despite such efforts, it remains an issue to identify conditions for the existence of conservative abstractions of possibly unstable nonlinear systems, which are guaranteed to yield a controller, if one exists for the original system. This motivates the current paper.

In this paper, we focus on the invariance control problem of discrete-time switched nonlinear systems. Our approach does not assume that the subsystems are asymptotically stable or have common equilibrium points. To be specific, our contribution lies in two aspects: (1) to automatically construct the finite abstractions of discrete-time switched systems, yielding invariant controllers with respect to the specifications. Interval analysis [18] is used for computing backward reachable sets, and partition refinement techniques for automatic partitioning [19]. Compared with abstraction-based methods, our approach generates non-uniform grids according to both dynamics and specifications, resulting in a lower computational complexity. (2) to address the invariance control guarantee, despite the use of conservative abstractions for possibly unstable nonlinear systems. To counter the problem in abstraction-based methods that the over-approximations are incomplete for control synthesis, we introduce a robust invariance property that has to be imposed on the original systems to counter the unavoidable approximation errors. A rule for choosing the precision parameter is also derived as a guarantee for successful invariance control synthesis.

The organization of this paper is as follows. In section II, we define the robustly controlled invariance condition for discrete-time switched systems, and formulate the continuous invariance synthesis problem. In section III, the discrete invariance synthesis problem is given based on an abstraction of the original swiched systems. Section IV presents our main result, which is the partitioning algorithm that constructs an abstraction automatically while generating an invariance controller. A condition for the completeness of this method is also provided in this section. In section V, we illustrate our approach by an example of polynomial dynamical system.

Notation: $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{R}^n$ denote the set of all integral numbers,

Yinan Li and Jun Liu are with Department of Applied Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada `yinan.li@uwaterloo.ca, j.liu@uwaterloo.ca`

real numbers, and n-dimensional vectors, respectively; $\mathbb{Z}_{\geq 0}$, $\mathbb{R}_{\geq 0}$, and $\mathbb{R}^n_{\geq 0}$ are the corresponding sets that only have the non-negative members (component-wise non-negative for n-dimensional vectors); a compact set is called *full* if it is equal to the closure of its interior; $\|\cdot\|$ denotes infinity norm in $\mathbb{R}^n$; given $\varepsilon \in \mathbb{R}_{\geq 0}$ and $x \in \mathbb{R}^n$, define $\mathcal{B}_\varepsilon(x) := \{y \in \mathbb{R}^n \mid \|y - x\| \leq \varepsilon\}$, and $\mathcal{B}_\varepsilon := \mathcal{B}_\varepsilon(0)$; given $y \in \mathbb{R}^n$ and $A \subset \mathbb{R}^n$, the distance from y to A is defined by $\|x\|_A := \inf_{x' \in A} \|y - x\|$; given two sets $A_1, A_2 \subset \mathbb{R}^n$, the Pontryagin difference is defined as $A_1 \ominus A_2 := \{x_1 \in \mathbb{R}^n \mid x_1 + x_2 \in A_1, \forall x_2 \in A_2\}$; the boundary of A is denoted by ∂A, the interior of A is denoted by $\mathrm{int}(A)$, and $\mathrm{cl}(A)$ is the closure of A; given two sets $A, B \subset \mathbb{R}^n$, $B \setminus A := \{x \in B \mid x \notin A\}$; an interval vector (or box) in $\mathbb{R}^n$ is denoted by $[x]$, where $[x] := [x_1] \times \cdots \times [x_n] \subset \mathbb{R}^n$ and $[x_i] = [\underline{x}_i, \overline{x}_i] \subset \mathbb{R}$ for $i = 1, \cdots, n$; the width of the interval $[x]$ is defined as $w([x]) := \max_{1 \leq i \leq n}\{\overline{x_i} - \underline{x_i}\}$.

II. Invariance Control Synthesis Problem

A. Discrete-time switched systems

We consider discrete-time switched systems described by:

$$x_{k+1} = \Phi_{l_k}(x_k), \quad k \in \mathbb{Z}_{\geq 0}, \tag{1}$$

where x_k, $x_{k+1} \in \mathbb{R}^n$ denote the continuous system states at time k and $k+1$, respectively. The set $\mathcal{M} := \{1, \ldots, m\}$, where $m \in \mathbb{Z}_{\geq 0}$, defines the finite set of modes. The switching mode is the only control variable and is denoted by $l_k \in \mathcal{M}$, the mode chosen at time k. The family of continuously differentiable functions $\{\Phi_l : \mathbb{R}^n \to \mathbb{R}^n \mid l \in \mathcal{M}\}$ determine the nonlinear dynamics for all subsystems.

Any infinite sequence in $\mathcal{M}$ defines a *switching signal* for system (1). We denote a particular switching signal by $\sigma := \{l_k\}_{k=0}^{\infty}$, where $l_k \in \mathcal{M}$ for all $k \geq 0$. Given a switching signal $\sigma := \{l_k\}_{k=0}^{\infty}$ and an initial state $x_0 \in \mathbb{R}^n$, the solution of system (1) is the unique sequence $\{x_k\}_{k=0}^{\infty}$ in $\mathbb{R}^n$ such that (1) is satisfied.

B. Controlled invariance

In this paper, we focus on the invariance control problem for system (1), which aims to prevent the solutions of (1) from leaving a predefined set of states by applying proper controllers. The definition given below is central to this problem.

Definition 1: A compact set $\Omega \in \mathbb{R}^n$ is said to be *controlled invariant* for system (1) if, for any initial state in Ω, there exists a switching signal σ such that the resulting solution of (1) remains in Ω.

To characterize controlled invariant sets, we rely on the following definition of reachable sets.

Definition 2: Given a set of initial states X_0, the *one-step forward reachable set* for system (1) from X_0 is defined by

$$\mathcal{R}(X_0) := \{x \in \mathbb{R}^n \mid x = \Phi_l(x_0), \text{for all}\, x_0 \in X_0, l \in \mathcal{M}\},$$

and

$$\mathcal{R}_l(X_0) := \{x \in \mathbb{R}^n \mid x = \Phi_l(x_0), \text{for all}\, x_0 \in X_0\}$$

denotes the corresponding reachable set under mode $l \in \mathcal{M}$.

Definition 3: Given a set of states X_0, the *one-step backward reachable set* for system (1) from X_0 is defined by

$$Pre(X_0) := \{x \in \mathbb{R}^n \mid \exists l \in \mathcal{M}, \text{ s.t. } \Phi_l(x) \in X_0\}.$$

Similarly, we denote by

$$Pre_l(X_0) := \{x \in \mathbb{R}^n \mid \Phi_l(x) \in X_0\}.$$

the one-step backward reachable set of X_0 under mode l.

Obviously,

$$\mathcal{R}(X_0) = \bigcup_{l \in \mathcal{M}} \mathcal{R}_l(X_0),$$
$$Pre(X_0) = \bigcup_{l \in \mathcal{M}} Pre_l(X_0).$$

For system (1), we provide this condition in the following proposition, which is a straightforward result from [20], [21].

Proposition 1: Consider the discrete-time switched system (1). A set Ω is controlled invariant for system (1) if and only if

$$\Omega \subseteq Pre(\Omega), \tag{2}$$

or equivalently

$$\Omega \subseteq \bigcup_{l \in \mathcal{M}} Pre_l(\Omega). \tag{3}$$

C. Robustly controlled invariance

Abstraction-based control relies on finite approximations of the original system models. Due to the mismatches between system models and their finite abstractions, one may not be able to find a controller using abstraction-based methods, even if there exists a controller for the original system. To preserve the feasibility of invariance control despite the mismatches, we introduce the following robustness definition.

Definition 4: A compact set Ω is said to be a *r-robustly controlled invariant set* for system (1) if and only if

$$\Omega \subseteq \bigcup_{l \in \mathcal{M}} (Pre_l(\Omega) \ominus \mathcal{B}_r), \tag{4}$$

where $\ominus$ denotes the Pontryagin difference between two sets. Denote by r^* the supremum of r such that (4) is satisfied, which is called the *robust invariance margin*.

The above definition essentially says that, for each point $x \in \Omega$, there exists at least one mode $l \in \mathcal{M}$ such that under this mode the next-step states of system (1) starting from the set $\mathcal{B}_r(x)$ is guaranteed to be inside Ω if $r \leq r^*$.

D. Problem statement

To formulate the invariance control problem, we define switching invariance controllers as follows.

Definition 5: A *(memoryless) switching controller* of system (1) is a function

$$c : \mathbb{R}^n \to 2^{\mathcal{M}}. \tag{5}$$

A (state-dependent) switching signal $\sigma = \{l_k\}_{k=0}^{\infty}$ is said to conform to a switching controller c, if

$$l_k \in c(x_k), \quad \forall k \geq 0, \tag{6}$$

where $\{x_k\}_{k=0}^{\infty}$ is the resulting solution of (1).

In other words, a switching controller maps a current state into a set of modes that are allowed to apply. A switching signal chooses at each time a specific mode that is allowed by the switching controller.

Definition 6: A switching controller c is said to be an *invariance controller* for system (1) with respect to a given compact set $\Omega \in \mathbb{R}^n$ if, for any initial state $x_0 \in \Omega$ and any switching signal $\sigma = \{l_k\}_{k=0}^{\infty}$ that conforms to c, the resulting solution $\{x_k\}_{k=0}^{\infty}$ of (1) stays inside Ω for all future time, i.e., $x_k \in \Omega$ for all $k \geq 0$.

Based on the above definitions, the main problem is stated as follows.

*Problem 1 (**Continuous Invariance Synthesis**):* Suppose that $\Omega \subset \mathbb{R}^n$ is a compact r-robustly controlled invariant set for system (1). Synthesize an invariance controller c with respect to Ω, and find the condition under which the synthesis approach is guaranteed to succeed.

The completeness of the existing abstraction-based control synthesis methods is guaranteed by (approximate) bisimulation relation in constructing abstractions, which is developed for controllable discrete-time linear systems [22] or systems satisfying incremental stability [23], [24]. For the systems that do not satisfy the incremental stability requirement, non-deterministic over-approximations can be used but are only guaranteed to be sound. In Problem 1, we aim to identify the condition under which the synthesis algorithm to be proposed in this paper can be complete.

III. Discrete Representation of The Synthesis Problem

In this section, we define finite abstractions of system (1), which are formulated as transition systems, for solving the invariance control synthesis problem.

A. Transition systems

Definition 7: A *transition system* is a tuple

$$\mathcal{T} = (\mathcal{Q}, \mathcal{Q}_0, \mathcal{A}, \to_{\mathcal{T}}),$$

where

- $\mathcal{Q}$ is a set of states;
- $\mathcal{Q}_0 \subset \mathcal{Q}$ is the set of initial states;
- $\mathcal{A}$ is a set of actions;
- $\to_{\mathcal{T}} \subset \mathcal{Q} \times \mathcal{A} \times \mathcal{Q}$ is a transition relation.

It is *finite* if $\mathcal{Q}$ and $\mathcal{A}$ both contain finite number of elements. A transition $(q, a, q') \in \to_{\mathcal{T}}$ means that the system state will go from q to q' under the action a, where q is called the *predecessor* and q' is the *successor*, relative to each other. The transition system $\mathcal{T}$ is *deterministic* if there is only one successor from a certain state under a given action, and *non-deterministic* if there are multiple such successors.

A (memoryless) *control strategy* for $\mathcal{T}$ is a function $\mu : Q \to 2^{\mathcal{A}}$. An *execution* of a transition system is an alternating sequence of states and actions. It is finite if there are finite number of states and actions, and it ends with a state; it is infinite otherwise. An infinite execution of a transition system $\mathcal{T}$ is denoted by $\varrho = q_0 a_0 q_1 a_1 \cdots q_n a_n \cdots$, where $(q_i, a_i, q_{i+1}) \in \to_{\mathcal{T}}$ for all $i \geq 0$. An execution of $\mathcal{T}$ following a control strategy μ satisfies $a_i \in \mu(q_i)$ for all $i \geq 0$. A *path* is obtained from an execution by omitting all the actions, e.g., $\rho = q_0 q_1 \cdots q_n \cdots$ is the path resulted from the execution ϱ above.

B. Abstraction by over-approximation

In the following, we use the concept of forward reachable set to define finite abstractions of system (1).

Definition 8: An *abstraction map* α is a function $\alpha : \mathbb{R}^n \to 2^{\mathcal{Q}}$ that maps $\mathbb{R}^n$ into a subset of a finite set $\mathcal{Q}$, and each member of Q is called a *cell*.

Let $\alpha^{-1}(q) := \{x \in \mathbb{R}^n \,|\, \alpha(x) = q\}$ denote the set of states in $\mathbb{R}^n$ that are mapped into $q \in \mathcal{Q}$ under α.

Definition 9: Given an abstraction map $\alpha : \mathbb{R}^n \to 2^{\mathcal{Q}}$, a finite transition system

$$\mathcal{T} = (\mathcal{Q}, \mathcal{Q}_0, \mathcal{A}, \to_{\mathcal{T}})$$

is said to be an *α-induced over-approximation* of system (1), if

- $\mathcal{Q}_0 = \bigcup_{x \in X_0} \{\alpha(x)\}$;
- $\mathcal{A} = \mathcal{M}$;
- $(q,\, l,\, q') \in \to_{\mathcal{T}}$ if the following condition is satisfied

$$\alpha^{-1}(q') \cap \mathcal{R}_l(\alpha^{-1}(q)) \neq \varnothing. \tag{7}$$

It is called an over-approximation because condition (7) indicates that a discrete state transition from q to q' will be included into the abstraction, as long as the region $\alpha^{-1}(q')$ intersects with the one-step forward reachable set of $\alpha^{-1}(q)$, i.e., the transitions in $\mathcal{T}$ covers all the possible state transitions from $\alpha^{-1}(q)$ to $\alpha^{-1}(q')$ under the dynamics of (1).

As a result of using over-approximation, $\mathcal{T}$ is often a non-deterministic transition system. To see this, note that the one-step reachable set of $\mathcal{R}^l_{\alpha^{-1}(q)}$, for some $q \in Q$ and some action $l \in \mathcal{M}$, may intersect with multiple regions of the form $\alpha^{-1}(q')$, where $q' \in Q$. In other words, there can be several successors of a single predecessor under the same action. Furthermore, in many cases, the forward reachable set cannot be computed exactly. Its outer approximations will be used instead, which can further introduce spurious transitions and consequently increase the non-determinism of the abstraction.

C. Discrete invariance control

Based on the finite abstraction defined above, we can formulate the following discrete synthesis problem.

*Problem 2 (**Discrete Invariance Synthesis**):* Given an α-induced over-approximation $\mathcal{T}$ of system (1) and the set

$$\alpha(\Omega) := \bigcup_{x \in \Omega} \alpha(x),$$

design a control strategy μ for $\mathcal{T}$ such that all resulting paths of $\mathcal{T}$ stay fully inside $\alpha(\Omega)$.

If the abstraction map α is preserving the target invariance set Ω in the sense that $\alpha^{-1} \circ \alpha(\Omega) = \Omega$, then, by the definition of an over-approximation, it is not difficult to show that the controller μ can be implemented on the original system (1) as an invariance controller. This is guaranteed by the soundness of over-approximation [17]. Here we focus on completeness of the approach. In other words, we aim to find an α-induced over-approximation based on which an invariance controller can be synthesized if there exists one for the original system.

As a result of non-determinism, an invariance controller cannot be guaranteed to exist for the abstraction, although the original system is proved to be controlled invariant with respect to a full and compact set of states Ω. This is because, affected by spurious transitions in the abstraction, the permissible control actions in the original system may not be allowed to use.

Therefore, the key problem lies in finding a proper abstraction map α such that the α-induced over-approximation does not lose the controlled invariant property with respect to a given set. We formalize the problem as follows.

*Problem 3 (**Construction of Abstraction**):* Suppose that $\Omega \subset \mathbb{R}^n$ is a compact r-robustly controlled invariant set for system (1). Find an abstraction map α such that one can solve the discrete invariance synthesis problem for the α-induced over-approximation of system (1).

IV. Invariance control via abstraction refinement based on interval analysis

This section is devoted to the main result of this paper, which presents a partition refinement algorithm based on interval analysis. The refinement procedure yields an abstraction map such that the induced finite abstraction of the original system is guaranteed to have an invariance controller.

A. Partition refinment

Definition 10: Given a set $\Omega \in \mathcal{C}(\mathbb{R}^n)$, a finite collection of sets

$$\mathcal{P} = \{P_1, P_2, \cdots, P_N\},$$

is said to be a *partition* of Ω, if the following conditions are satisfied:

1) $P_i \subset \Omega$, for all $i \in \{1, \cdots, N\}$;
2) $\operatorname{int}(P_i) \cap \operatorname{int}(P_j) = \varnothing$, for all $i, j \in \{1, \cdots, N\}$;
3) $\Omega \subset \bigcup_{i=1}^{N} P_i$.

Moreover, each element P_i of the partition $\mathcal{P}$ is called a *cell.*

If we consider each cell P_i of a partition $\mathcal{P}$ as a discrete state q_i and the complement of the set Ω in $\mathbb{R}^n$ by a single state q_o, an abstraction map $\alpha : \mathbb{R}^n \to 2^{\mathcal{Q}}$ such that for all $x \notin \Omega$, $\alpha(x) = q_o$; for all $x \in \Omega$ and all $i \in \{1, \cdots, N\}$, $q_i \in \alpha(x)$, if and only if $x \in P_i$. Clearly, $Q = \{q_o, q_1, \cdots, q_N\}$. Hence, the problem of finding an abstraction map for the state space is equivalent to designing a partition.

To guarantee that the invariance control problem is feasible for an α-induced over-approximation, we have to find a partition $\mathcal{P}$ of Ω such that, for any cell in $\mathcal{P}$, there exists a switching mode such that the one-step forward reachable set is fully covered by Ω.

The proposed partitioning method consists of four steps.

Step 1. Let
$$S_l := Pre_l(\Omega). \tag{8}$$

Step 2. Split Ω into two parts: $\Omega_a^l := S_l \cap \Omega$ and $\Omega_b^l = \Omega \setminus \Omega_a^l$.

Step 3. Repeat Steps 1 and 2 to compute $\left\{\Omega_a^l,\, \Omega_b^l\right\}$ for each mode $l \in \mathcal{M}$.

Step 4. Return a partition $\mathcal{P}$ by intersecting all the parts for all modes:
$$\left\{\Omega_a^l,\, \Omega_b^l : \, l \in \mathcal{M}\right\}.$$

Algorithm 1 is an implementation of the above partitioning method using the *partition refinement* technique, which incrementally splits a finite set according to a series of *pivot* subsets S [19]. The process of refining a partition $\mathcal{P} = \{P_1, \cdots, P_N\}$ with respect to a single pivot set S is the process of replacing each cell P_i by two cells $P_i^a = P_i \cap S$ and $P_i^b = P_i \setminus S$. In this paper, the pivot sets are chosen to be $\{S_l : \, l \in \mathcal{M}\}$ as defined in (8).

Algorithm 1 examines every switching mode by looping over the set $\mathcal{M}$. Line 4 produces a pivot set S_l for mode l. The current partition $\mathcal{P}$ as well as the associated action set Act is refined with respect to S_l by calling a refine procedure in line 8, which is outlined in Algorithm 2. The refined partition and the set of permissible actions together will naturally define an invariance controller for the original system. In Algorithm 2, the set of permissible actions for cell P is denoted by $A_P \in Act$.

Algorithm 1 Partition Algorithm

```
Require: $\Omega, \mathcal{M}, \tau_s, \varepsilon$
1: $\mathcal{P} = \{\Omega\}$
2: $Act = \varnothing$
3: for all $l \in \mathcal{M}$ do
4:     $S_l = Pre_l(\Omega)$
5:     if $S_l \neq \varnothing$ then
6:         $refine(\mathcal{P}, Act, S_l, l)$
7:     end if
8: end for
       return $\mathcal{P}$
```

B. Reachable set approximation via interval arithmetic

The remaining question of implementing Algorithm 1 is how to compute the pivot set S_l for each mode $l \in \mathcal{M}$, which, by definition, involves the computation of backward reachable sets. Since it is difficult to obtain the exact forward and backward reachable sets for nonlinear systems, their approximations are considered instead.

In this paper, we apply interval analysis. More specifically, to approximate the set S_l, we apply *Set Inversion Via Interval Analysis* (SIVIA) algorithm (see [18] for details and pseudo code). SIVIA is designed to approximate the reverse image X of a set Y under a function f, i.e., $X = f^{-1}(Y)$. The inputs are Y, f, a prior box $[x_0]$ to which X is confined, and an approximation accuracy parameter ε. It returns two sets $\underline{X}, \overline{X}$ satisfying $\underline{X} \subset X \subset \overline{X}$. The advantage of this algorithm is that the image approximation is controlled by the given accuracy parameter ε, and is guaranteed to converge as ε decreases to zero, provided that the function f^{-1} is a

Algorithm 2 Partition Refinement

```
procedure REFINE($\mathcal{P}, Act, S, l$)
    if $S = \varnothing$ then
        return
    end if
    for all $P \in \mathcal{P}$ do
        if $P \neq \varnothing$ then
            remove $P$ from $\mathcal{P}$
            $P_a = P \cap S$, $P_b = P \setminus S$
            if $P_a \neq \varnothing$ then
                insert $P_a$ as a new partition to $\mathcal{P}$
                $A_a = A_P \cup l$, add $A_a$ to $Act$ for $P_a$
            end if
            if $P_b \neq \varnothing$ then
                insert $P_b$ to replace $P$
                keep $A_P$ for $P_b$
            end if
        end if
    end for
end procedure
```

continuous in the sense of a certain set distance for some compact and full set X [18].

In our implementation of SIVIA, for system (1) under a given mode $l \in \mathcal{M}$, the function f is taken to be a state transition function Φ_l, the set Y is the given controlled invariant set Ω, and the prior box $[x_0]$ is a set that contains S_l. As such, the output $\underline{S_l}, \overline{S_l}$ under- and over- approximate the precise one-step backward reachable set S_l separately. In the following, we denote our application of SIVIA by $(\underline{S_l}, \overline{S_l}) = \text{SIVIA}(\Phi_l, \Omega, [x_0], \varepsilon_r)$, where ε_r is the algorithm accuracy parameter.

C. Invariance control guarantees

The completeness guarantee of the control synthesis on the resulting partition relies on the following assumption.

Assumption 1: Let Φ_l is invertible for all $l \in \mathcal{M}$. There exist $\rho_1, \rho_2 > 0$ such that system (1) satisfies the following condition for some compact set $\Omega \subset \mathbb{R}^n$ for all $l \in \mathcal{M}$:

$$\|\Phi_l(x) - \Phi_l(y)\| \leq \rho_1 \|x - y\|, \quad \forall x, y \in \Omega,$$
$$\|\Phi_l^{-1}(x) - \Phi_l^{-1}(y)\| \leq \rho_2 \|x - y\|, \quad \forall x, y \in Pre_l(\Omega),$$

where Φ_l^{-1} is the inverse function of Φ_l.

If Φ_l is continuously differentiable on Ω for all $l \in \mathcal{M}$, then $\rho_1 = \max_{x \in \Omega, l \in \mathcal{M}} \|J_x \Phi_l\|$, where J_x is the Jacobian matrix at x. Likewise, if Φ_l^{-1} is Lipschitz continuous on Ω for all $l \in \mathcal{M}$, then $\rho_2 = \max_{x \in \Omega, l \in \mathcal{M}} \|J_x \Phi_l^{-1}\|$.

Now we are ready to present the condition such that an invariance controller is guaranteed for the discrete synthesis problem.

Theorem 1: Let $\Omega \subset \mathbb{R}^n$ be compact. Suppose that Assumption 1 holds on Ω, and system (1) is r-robustly controlled invariant with respect to Ω. The partition generated by Algorithm 1, with the pivot sets computed by SIVIA$(\Phi_l, \Omega, [x_0], \varepsilon_r)$, can solve Problem 3, if the precision parameter ε_r is chosen such that

$$\rho_2 \rho_1 \varepsilon_r \leq r, \quad \forall l \in \mathcal{M}. \tag{9}$$

Proof: Denote by ΔS_l the set of intervals that are included in $\overline{S_l}$ but not in $\underline{S_l}$, where $\underline{S_l}$ is the under-approximation of S_l returned by SIVIA$(\Phi_l, \Omega, [x_0], \varepsilon_r)$ and S_l is defined in (8).

Given that system (1) is r-robustly controlled invariant with respect to Ω, then for any $x \in \Omega$, there always exists a switching mode $l \in \mathcal{M}$ such that $x \in S_l \ominus \mathcal{B}_r$. We aim to show that $x \in \underline{S_l}$.

Suppose this is not the case. Then $x \in [x] \in \Delta S_l$, since $\Phi_l(x) \in \Omega$. There exists a point $x' \in \partial S_l$ such that $\|x' - x\| < \rho_2 \rho_1 \varepsilon_r \leq r$. Let $\|x' - x\| = \gamma < \rho_1 \varepsilon_r$. Then for any given $\delta > 0$ satisfying $\delta + \gamma < r$, there exists a point $x'' \in \mathbb{R}^n \setminus S_l$ such that $\|x'' - x'\| \leq \delta$. Thus, $\|x'' - x\| \leq \|x'' - x'\| + \|x' - x\| \leq \delta + \gamma < r$. This implies there exists a point $z \in \mathcal{B}_r$ such that $z + x = x'' \notin S_l$, which means $x \notin \Omega \ominus \mathcal{B}_r$. This is a contradiction.

Therefore, for any $x \in \Omega$, there exists at least one mode $l \in \mathcal{M}$ such that $x \in \underline{S_l}$. This implies

$$\Omega \subset \cup_{l \in \mathcal{M}} \underline{S_l} \subset \cup_{l \in \mathcal{M}} S_l.$$

Define a set of discrete states $\mathcal{Q} = \{q_o, q_1, \cdots, q_N\}$. Construct the abstraction map $\alpha : \mathbb{R}^n \to 2^{\mathcal{Q}}$ such that for all $x \notin \Omega$, $\alpha(x) = q_o$; for all $x \in \Omega$ and all $i \in \{1, \cdots, N\}$, $q_i \in \alpha(x)$, if and only if $x \in P_i$.

We then construct the α-induced over-approximation according to Definition 9. Denote by $\{q_i'\}$ the set of successors of q_i satisfying (7), for all $i \in \{1, \cdots, N\}$ and mode $l \in \mathcal{M}$. According to property A, we have $\mathcal{R}_{P_i}^l \subset \Omega$. Then we can conclude that, if l belongs to the set of permissible actions for P_i, $\{q_i'\} \subset \mathcal{Q} \setminus q_o$, and otherwise $\{q_i'\} = q_o$.

Given the condition that $\Omega \subset \cup_{l \in \mathcal{M}} S_l$, for any $x \in \Omega$, it should be covered by at least one set S_l. Suppose P_i is the cell that contains x. Thus, refined by Algorithm 2, the associate set of permissible actions for P_i contains l, and the permissible action set for each cell should be non-empty. This defines a control strategy such that all the resulting paths are inside Ω, which means that the discrete invariance synthesis problem can be solved. ■

According to Algorithm 1, any states that can stay inside Ω in one step time under the same set of switching modes belong to the same cell. The number of pivot sets is the number of switching modes, which is finite. This implies that Algorithm 1 will terminate after a finite number of iterations. Therefore, it is complete.

D. Computational complexity

The time complexity of the proposed partition refinement algorithm, which directly yields an invariant controller, is a combined complexity of the partition algorithm and SIVIA.

Our partition algorithm has fixed number of iterations, which equals to the number of modes, and there is no order for the intervals that belong to the same cell. Then the complexity relies on the number intervals in each pivot set.

Denote the size of each pivot set by $\mathcal{O}(m)$, and the total number of intervals is N, then he time complexity of the overall procedure is $\mathcal{O}(m \log n)$. To lower it, the intervals returned by SIVIA should be kept as fewer as possible. This can be achieved by using a greater ε_r while still satisfying (9), and merging intervals based on proper data structures, if the overall number of the intervals is huge.

For SIVIA, the iterations performed before termination would be $(w([x_0])/\varepsilon_r + 1)^n$ in the worst case [18], which is equivalent to the abstraction-based methods based on uniform grids. Under most of system dynamics, the number of subdivisions is lower than the worst case. Hence our method gains lower computational complexity than the abstraction-based methods with the same precision parameter.

V. Example of Polynomial Dynamics

We consider a discrete-time nonlinear switched system with polynomial dynamics:

$$x_{k+1} = f_l(x_k), l \in \{1, 2, 3, 4\}, \tag{10}$$

where $x = [x_1, x_2]^T$ and

$$f_1(x) = \begin{bmatrix} 0.85x_1 - 0.1x_2 - 0.05x_1^3 \\ x_2 - 0.1x_2^2 + 0.1x_1 + 0.2 \end{bmatrix},$$

$$f_2(x) = \begin{bmatrix} 0.85x_1 - 0.1x_2 - 0.05x_1^3 \\ 0.9x_2 + 0.1x_1 \end{bmatrix},$$

$$f_3(x) = \begin{bmatrix} 0.99x_1 - 0.02x_2 - 0.01x_1^3 + 0.04 \\ x_2 + 0.02x_1 + 0.2 \end{bmatrix},$$

$$f_4(x) = \begin{bmatrix} 0.99x_1 - 0.02x_2 - 0.01x_1^3 - 0.03 \\ x_2 + 0.02x_1 - 0.2 \end{bmatrix}.$$

This is a 2-dimensional, 4-mode discrete-time nonlinear switched system. It is adapted from the polynomial system example in [7], [8]. Compared with modes 1 and 2, modes 3 and 4 provide faster dynamics. Given the target invariant set $\Omega = [-0.7, 0] \times [0.2, 0.8]$, which is is a 0.3-robustly controlled invariant set for system (10), we aim to design an invariance controller to keep the state trajectory inside Ω for all future time. Evaluation of the Jacobian matrix around Ω for each mode gives $\rho_{21} = 1.06$, $\rho_{12} = 1$, $\rho_{13} = 1.02$, $\rho_{14} = 1.02$, and $\rho_{21} = 1.60$, $\rho_{22} = 1.43$, $\rho_{23} = 1.05$, $\rho_{24} = 1.06$, where the second number in the subscript denotes modes. Since Ω is an interval, by Theorem 1, we set the accuracy parameter $\varepsilon_r = 0.03$ for all four modes.

The target invariance set Ω is divided into 8 cells after performing Algorithm 1. The partition is shown in Figure 1, where each cell shown in different gray scales and marked by red numbers. The whole partition algorithm takes around 9 seconds to complete, which is implemented using Matlab and runs on a 2.4 GHz Intel Core i5 processor.

The set of permissible modes for each cell are {1,2,3,4}, {1,2,3}, {1,2,4}, {1,2}, {1,3}, {1}, {2,4}, and {2}, respectively. Applying a time minimal control strategy based on the partition and its resulting finite abstraction (shown in Figure 2), we simulate the closed-loop control system with an initial condition $x_0 = [-0.67, 0.77]^T \in \Omega$. The simulation results are shown in Figures 3 and 4. As a result of time optimal control strategy, after a period of time, the system is switching between mode 3 and 4, both of which are fast dynamics.

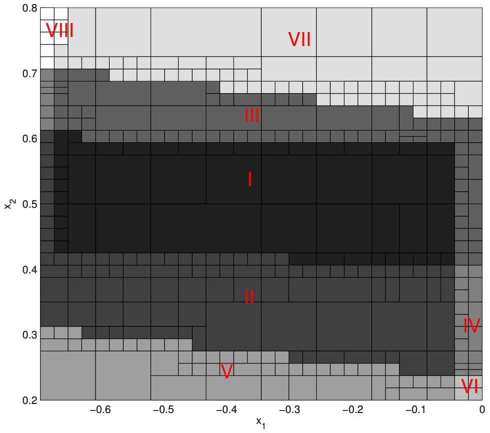

Fig. 1. The partition result of the polynomial dynamics.

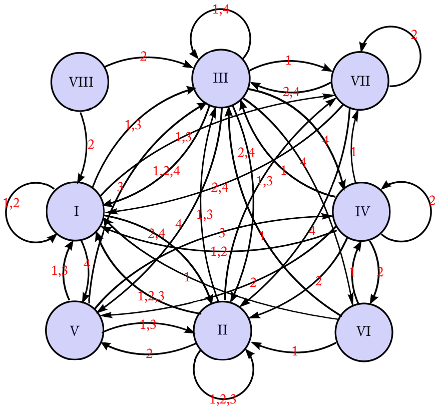

Fig. 2. The resulting finite abstraction.

VI. CONCLUSIONS AND FUTURE WORKS

In this paper, we presented an interval arithmetic based method to solve an invariance control synthesis problem for discrete-time switched nonlinear systems. The invariance controller was designed by finite abstraction, which is an over-approximation of the original system induced by an abstraction map. Usually as a result of spurious transitions introduced by over-approximation, the invariance control synthesis problem for the discrete abstraction is not guaranteed to be feasible, even if the original system can be proved to be controlled invariant. We have addressed this issue by introducing a robust invariance condition for the original system. With such a condition, and enabled by the guaranteed convergence of interval computation (under mild assumptions), we have been able to prove guarantees for the feasibility of discrete invariance control problem resulting from conservative abstractions.

The given set is controlled invariant for discrete-time

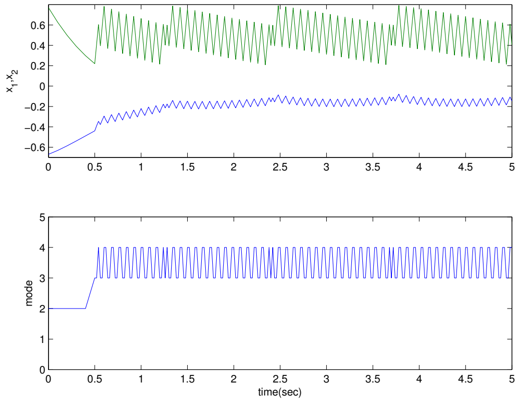

Fig. 3. The simulation results showing the system state time history.

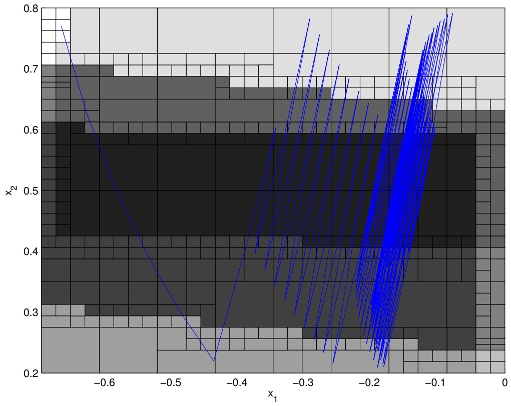

Fig. 4. The simulation results showing the state evolution on 2-dimensional phase plane.

switched system (1) is a special case in invariance control. Generally, there might be a maximal controlled invariant set inside a given specification. Future work will focus on computing the maximal controlled invariant set and the robust invariance margin. Extending the interval analysis methods to provide guarantees for abstraction-based control synthesis for more general specifications than invariance and analysis of robustness of the controllers synthesized using such methods will also be investigated, especially since one would expect a robust controller has to somehow exist for the original system to render the discrete synthesis feasible.

VII. ACKNOWLEDGMENTS

This work was supported in part by a Marie Curie Career Integration Grant PCIG13-GA-2013-617377 and a University of Waterloo startup grant.

REFERENCES

[1] D. Liberzon, *Switching in systems and control*. Springer Science & Business Media, 2003.

[2] J. Buisson, P.-Y. Richard, and H. Cormerais, "On the stabilisation of switching electrical power converters," in *Proc. of Hybrid Systems: Computation and Control (HSCC)*. Springer, 2005, pp. 184–197.

[3] M. Rinehart, M. A. Dahleh, D. Reed, and I. Kolmanovsky, "Suboptimal control of switched systems with an application to the disc engine," *IEEE Trans. Control Syst. Technol.*, vol. 16, no. 2, pp. 189–201, 2008.

[4] H. Kress-Gazit, G. E. Fainekos, and G. J. Pappas, "Temporal-logic-based reactive mission and motion planning," *IEEE Trans. Robot.*, vol. 25, no. 6, pp. 1370–1381, 2009.

[5] M. Kloetzer and C. Belta, "A fully automated framework for control of linear systems from temporal logic specifications," *IEEE Trans. Autom. Control*, vol. 53, no. 1, pp. 287–297, 2008.

[6] B. Yordanov, J. Tůmová, I. Černá, J. Barnat, and C. Belta, "Temporal logic control of discrete-time piecewise affine systems," *IEEE Trans. Autom. Control*, vol. 57, no. 6, pp. 1491–1504, 2012.

[7] N. Ozay, J. Liu, P. Prabhakar, and R. M. Murray, "Computing augmented finite transition systems to synthesize switching protocols for polynomial switched systems," in *Proc. of American Control Conf. (ACC)*, 2013, pp. 6237–6244.

[8] J. Liu, N. Ozay, U. Topcu, and R. M. Murray, "Synthesis of reactive switching protocols from temporal logic specifications," *IEEE Trans. Autom. Control*, vol. 58, no. 7, pp. 1771–1785, 2013.

[9] M. Kloetzer and C. Belta, "Automatic deployment of distributed teams of robots from temporal logic motion specifications," *IEEE Trans. Robot.*, vol. 26, no. 1, pp. 48–61, 2010.

[10] R. Rogersten, H. Xu, N. Ozay, U. Topcu, and R. M. Murray, "Control software synthesis and validation for a vehicular electric power distribution testbed," *Journal of Aerospace Information Systems*, vol. 11, no. 10, pp. 665–678, 2014.

[11] P. Nilsson, O. Hussien, Y. Chen, and et al., "Preliminary results on correct-by-construction control software synthesis for adaptive cruise control," in *Proc. of Conf. Decision and Control (CDC)*, 2014.

[12] G. Pola, A. Girard, and P. Tabuada, "Approximately bisimilar symbolic models for nonlinear control systems," *Automatica*, vol. 44, no. 10, pp. 2508–2516, 2008.

[13] A. Girard, G. Pola, and P. Tabuada, "Approximately bisimilar symbolic models for incrementally stable switched systems," *IEEE Trans. Autom. Control*, vol. 55, no. 1, pp. 116–126, 2010.

[14] J. Liu and N. Ozay, "Abstraction, discretization, and robustness in temporal logic control of dynamical systems," in *Proc. of Hybrid Systems: Computation and Control (HSCC)*, 2014, pp. 293–302.

[15] M. Zamani, G. Pola, M. M. Jr., and P. Tabuada, "Symbolic models for nonlinear control systems without stability assumptions," *IEEE Trans. Autom. Control*, vol. 57, no. 7, pp. 1804–1809, 2012.

[16] P. Nilsson and N. Ozay, "Incremental synthesis of switching protocal via abstraction refinement," in *Proc. of Conf. Decision and Control (CDC)*, 2014.

[17] Y. Li, J. Liu, and N. Ozay, "Computing finite abstractions with robustness margin via local reachable set over-approximation," in *Proc. of IFAC Conf. Analysis and Design of Hybrid Systems (ADHS)*, 2015.

[18] L. Jaulin and E. Walter, "Set inversion via interval analysis for nonlinear bounded-error estimation," *Automatica*, vol. 29, no. 4, pp. 1053 – 1064, 1993.

[19] M. Habib, C. Paul, and L. Viennot, "Partition refinement techniques: An interesting algorithmic tool kit," *International Journal of Foundations of Computer Science*, vol. 10, no. 02, pp. 147–170, 1999.

[20] E. C. Kerrigan, "Robust constraint satisfaction: invariant sets and predictive control," Ph.D. dissertation, Department of Engineering, University of Cambridge, 2000.

[21] C. E. T. Dórea and J. C. Hennet, "(a, b)-invariant polyhedral sets of linear discrete-time systems," *J. Optimiz. Theory App.*, vol. 103, no. 3, pp. 521–542, 1999.

[22] P. Tabuada and G. J. Pappas, "Model checking ltl over controllable linear systems is decidable," in *Proc. of Hybrid Systems: Computation and Control (HSCC)*. Springer, 2003, pp. 498–513.

[23] M. Rungger, M. Mazo, Jr., and P. Tabuada, "Specification-guided controller synthesis for linear systems and safe linear-time temporal logic," in *Proc. of Hybrid Systems: Computation and Control (HSCC)*, 2013, pp. 333–342.

[24] E. Aydin Gol, M. Lazar, and C. Belta, "Language-guided controller synthesis for discrete-time linear systems," in *Proc. of Hybrid Systems:*