A Counter-Example Guided Framework for Robust Synthesis of Switched Systems Using Control Certificates

Hadi Ravanbakhsh and Sriram Sankaranarayanan
University of Colorado, Boulder
firstname.lastname@colorado.edu

ABSTRACT

In this article, the problem of synthesizing switching controllers is considered through the synthesis of a "control certificate". Control certificates include control barrier and Lyapunov functions, which represent control strategies, and allow for automatic controller synthesis. Our approach encodes the controller synthesis problem as quantified nonlinear constraints. We extend an approach called Counterexample Guided Inductive Synthesis (CEGIS), originally proposed for program synthesis problems, to solve the resulting constraints. The CEGIS procedure involves the use of satisfiability-modulo theory (SMT) solvers to automate the problem of synthesizing control certificates. In this paper, we examine generalizations of CEGIS to attempt a richer class of specifications, including reach-while-stay with obstacles and control under disturbances. We demonstrate the ability of our approach to handle systems with non-polynomial dynamics as well. The abilities of our general framework are demonstrated through a set of interesting examples. Our evaluation suggests that our approach is computationally feasible, and adds to the growing body of formal approaches to controller synthesis.

1. INTRODUCTION

The problem of synthesizing switching controllers for important classes of specifications including safety, reach-while-stay with obstacles and stabilization under disturbances is examined in this article. The plant model is a switched system that consists of finitely many (controllable) modes, and the dynamics for each mode are specified using ODEs. The model also includes uncontrolled input disturbances. Furthermore, we consider nonlinear ODEs for each mode, including non-polynomial functions. The goal of the controller is to choose appropriate modes, so that all possible traces satisfy a resulting specification.

The controller synthesis is addressed in two phases: formulating control certificates and solving constraints. First, the control problem is reduced to finding a control certificate. The control certificate represents a strategy for the controller to satisfy the specifications. Additionally, this strategy can be effectively implemented as a feedback law. In the second phase, a counterexample guided inductive synthesis (CEGIS) framework is used to discover such control certificate [29]. This framework was originally proposed for program synthesis problems [29] and previously considered by the authors to solve nonlinear switched systems stabilization problems [26][25].

In this article, we adapt CEGIS for a larger class of properties starting from safety to reach-while-stay with obstacles. First, we show that safety properties can be addressed by finding a control invariant. Next, we encode the problem of finding a control invariant into a constraint solving problem, which can be solved by the CEGIS framework. Similarly, we address reach-while-stay properties in different settings by finding combinations of control invariants and control Lyapunov-like functions. This includes the general reach-while-stay with obstacles problem, and reach-while-stay with disturbances.

Once the control certificates are formulated, we obtain a system of quantified constraints that must be solved to find a suitable certificate. The CEGIS framework handles quantified formulas by alternating between a series of quantifier free formulas that are suitable for existing SMT solvers [7][10]. We also demonstrate a LMI relaxation that can be employed in place of expensive nonlinear solvers. This is shown to make the overall approach more scalable. However, the LMI relaxation is sometimes unable to find a control certificate even if one is known to exist due to the relaxation involved. Also, it does not extend as such to nonpolynomial systems.

We provide examples for each control problem and we demonstrate the proposed approach for finding control certificates is computationally feasible. The contributions of this article include: (a) We extend the CEGIS framework for finding robust control certificates and control certificates with general logical constraints. (b) In particular, we address how to use CEGIS framework for systems with non-polynomial dynamics, safety problems, reach-while-stay problems with obstacles and systems with disturbances.

1.1 Related Work

The goal of correct by construction switching systems is to design a switching logic, guaranteeing some given properties. One class of solution is based on iterative fixed-point computation. Many researches have investigated this approach and we point out some of them. For these methods, the system is usually approximated (abstracted) using a (bi)simulation relation. Once a solution is found for the approximated system (using iterative fixed-point computation), it is guaranteed the primal problem is also solved. The properties of interest in these systems can be as complicated as GR(1) (e.g. [34]) or even LTL formula. Some of these works discretize the time (e.g. [18][1]), while others consider continuous time [14][20][21]. As the procedure can get more complicated, most of these approaches consider linear dynamics or/and systems without any disturbances. To scale these techniques, different ap-
approaches have been proposed \[27, 17, 19, 24\], each of which is restricted to a certain class of systems. In this article, we consider continuous time systems with general dynamics. The dynamics are not even restricted to polynomials and our approach supports more complicated functions such as trigonometric and exponential ones. Also, systems with disturbances are considered. However, the specifications in this article are restricted to fundamental properties such as safety, and reach-while-stay. Also, our approach assumes that control certificates with a given form exist. As such, the existence of such certificates is not guaranteed and thus, our approach lacks the general applicability of a abstraction-based synthesis.

Another class of solutions is based on constraint solving. The goal in these approaches is to find a control certificate which yields a (control) strategy to guarantee the property. Most of these works have focused on stability and liveness properties. In these methods, a control Lyapunov function is discovered from which a control strategy for stabilizing the system is derived. The idea of control Lyapunov functions goes back to Artstein [3] and Sontag [30]. The problem of discovering a control Lyapunov function usually formulated as a bilinear matrix inequalities (BMI) [33]. Also, instead of solving such NP-hard problem, usually policy iteration is used [33] [11] to find a solution, conservatively. The control synthesis using control certificates is not restricted to stability and Dimitrova et. al. [8] have shown that control certificates can be extended to address more complicated specifications i.e. parity games.

Recently, Huang et. al. [12] used control certificates to solve the reach-while-avoid problem. The authors consider piecewise-linear systems with no disturbances and time is discretized. In contrast to other similar methods, piecewise constant functions are used for defining the certificate and state space is partitioned into cells to define such functions. Using this technique, any function can be approximated, which makes the method relatively complete.

Also, Taly et. al. [32, 31] used constraint solving approach to find control certificates for safety and reachability. The main differences between these works and our approach are as follows. First, our problem formulation is a little different and we guarantee the min-dwell time with much simpler constraints for the certificate. Second, authors use QEPcad SMT solver along with numerical simulation to solve the constraints, while similar to our previous works, we use counter-example guided inductive synthesis approach [26, 25]. Also, we can use LMI relaxation (as introduced in our previous work [25]) which makes our approach much more scalable. And finally, we consider systems with disturbances as well.

The CEGIS procedure has been primarily used for parameter synthesis in programming languages (e.g. [29, 2]) and hybrid systems [9, 35]. More recently, the CEGIS procedure was used for finding Lyapunov functions by Kapinski et. al. [13], and finally in our previous works it is used for finding control Lyapunov functions [26, 25]. In this work we extend our previous work in several directions: (i) finding robust control certificates for systems with disturbances, (ii) finding more complicated control certificates (e.g. control invariant), (iii) support of non-polynomial dynamics.

2. PRELIMINARIES

Let \( x \) represent a \( n \times 1 \) vector in \( \mathbb{R}^n \), \( x_i \) be the \( i \)th component of the vector, and \( |x| \) be its 2-norm. Given a function \( f(t) \), let \( f^+(t) := \lim_{s \to t^+} f(s) \) be the right limit of \( f \) at \( t \), and \( \dot{f}(t) \) represent the right derivative of \( f \) at time \( t \). \( B(\cdot, x) \) denotes a hyper-ball of radius \( r \) centered at \( x \). For a set \( S \subseteq \mathbb{R}^n \), \( \partial S \) and \( \text{int}(S) \) are its boundary and interior, respectively.

2.1 Switched Systems

We consider continuous-time switched system plants controlled by a controller that provides continuous-time switching feedback. The plant has a state defined by \( n \) continuous variables \( x \) in a state space \( X \subseteq \mathbb{R}^n \), along with a finite set of modes \( Q = \{q_1, \ldots, q_m\} \). The plant has uncontrollable inputs (disturbances) \( d \) belonging to a compact set \( D \) and a controllable input \( q \in Q \). The disturbance input \( d(t) \) can be any measurable function such that \( d(t) \in D \) for all \( t \geq 0 \). The state of the plant inside each mode evolves according to dynamics:

\[
\dot{x}(t) = f_q(t)(x(t), d(t)),
\]

wherein \( f_q : X \times D \to \mathbb{R}^n \) is a Lipschitz continuous function over \( X \) and continuous over \( d \), describing the vector field of the plant for mode \( q \). Given a disturbance input \( d(t) \), the trace of the system \( \sigma : (q(t), x(t))_{t \geq 0} \) maps time to mode \( q(.) : \mathbb{R}^+ \to Q \), and state \( x(.) : \mathbb{R}^+ \to X \).

The controller is defined as a function switch : \( Q \times X \to Q \) which given the current mode and state of the plant, decides the mode of the plant for the next time instance. Formally:

\[
q^+(t) = \text{switch}(q(t), x(t)).
\]

The goal in this article is to design a switch function, which makes the whole closed loop system satisfy an input specification. One key issue is that of zenoess: the switch function may switch infinitely often in a finite time interval. Therefore, in addition to the above requirements, we need to make sure zeno behaviors are avoided. In this article, we address this issue by guaranteeing a min-dwell time, so that once the control switches to a mode \( q \), it remains in \( q \) for a minimum time \( \delta > 0 \).

Once the function switch is defined, given a disturbance trace \( d \), initial mode \( (q(0)) \), and initial state \( (x(0)) \), a unique trace is defined for the system.

Specifications: The specifications we are interested include safety and reach-while-stay properties. Generally, we will consider specifications that describe possible sequences of plant states \( x(t) \) over time \( t \geq 0 \). In this article, we utilize temporal logic notation involving atomic propositions that are subsets of \( X \) and temporal properties \( \square, \Diamond, \text{ and } H \), including Boolean connectives \( \land, \lor, \text{ and } \neg \). For example, the specification \( R \Rightarrow H \) describes an invariant property, i.e. if \( x(0) \in R \), then \( \forall t \in \mathbb{R} \), \( x(t) \in R \).

2.2 Control Certificates

d Encoding verification and synthesis problems into constraints is a well-studied approach. We discuss control certificates and the generation of constraints from these certificates.

Considering switched systems, control certificates guarantee that the controller has a strategy to satisfy the specification and this strategy is effectively implementable for switched systems and respects the min-dwell time property.

In the first step, a suitable certificate is defined to enforce the property of interest. For example, to enforce stability, a control Lyapunov function \( V \) guarantees at each time instance, the controller can decrease its value. As an example, consider the problem of stabilizing a system \( \frac{dx}{dt} = f(x, u) \) for control inputs \( u \in U \). Let \( V(x) \) be a control Lyapunov function. The constraints translate to

\[
\begin{align*}
(\forall x) & \left\{ \begin{array}{l}
V(0) = 0 \\
V(x) \to \infty \text{ as } x \to \infty \\
x \neq 0 \implies V(x) > 0 \\
(\exists u \in U) (\forall V \cdot f(x, u) \leq 0)
\end{array} \right. 
\end{align*}
\]
Here the control Lyapunov function is a control certificate. Given a control Lyapunov function, one can design a controller which enforces stability.

However, in many cases, the control certificate is not known in advance. In such situations, we solve a parameterized version of Equation (1) for a parameterized (template) form $V(c, x)$ for unknown coefficients $c \in Y$. If $V$ is given as a parametric form $V(c, x)$, the problem becomes:

$$(\exists c \in Y) \ (\forall x) \left\{ \begin{array}{l}
V(c, 0) = 0 \\
V(c, x) \to \infty \text{ as } x \to \infty \\
x \neq 0 \implies V(c, x) > 0
\end{array} \right.$$  \hspace{1cm} (2)

In this article, for each problem we find suitable certificates to enforce the specification of interest. Next, we derive constraints from these certificates. The constraints will have a complex structure as in Equation (2). We modify an algorithm commonly used for program synthesis problems to the problem of synthesizing the coefficients $c \in Y$ [29].

**Assumption 1**. The problems we are interested in satisfy the following assumptions:

1. All the regions described by the atomic propositions are compact.
2. All certificates $V(c, x)$ sought for various properties are smooth functions, and thus, bounded in a compact region.
3. The vector field $f_q$ for each mode $q$ is continuously differentiable, and thus, bounded in a compact region.

### 3. CEGIS Procedure

The counterexample guided inductive synthesis (CEGIS) approach has its roots in program verification, wherein it was proposed as a general approach to solve $\exists \forall$ constraints that arise in such problems [29]. The key idea behind the CEGIS approach is to find solutions to such constraints while using a satisfiability solver for quantifier-free formulas. Numerous constraint solvers consider the problem of satisfiability or validity of quantifier-free constraint solvers. Solvers like Z3 allow us to solve many different classes of constraints with extensive support for linear arithmetic constraints [7]. On the other hand, general purpose nonlinear domain solvers like dReal, support the solving of quantifier free nonlinear constraints [10]. The presence of quantifiers drastically increases the complexity of solving these constraints. Here we briefly explain the idea of CEGIS procedure for $\exists \forall$ constraints of the form

$$(\exists c \in Y) \ (\forall x \in X) \ \exists \forall(c, x).$$

Here $c$ typically represents the unknown coefficients of a control certificate and $x$ represents the state variables of the system. Our goal is to find one witness for $c$ that makes the overall quantified formula true. The overall approach constructs, maintains, and updates two sets iteratively:

1. $X_i \subseteq X$ is a finite set of witnesses. This is explicitly represented as $X_i = \{x_0, \ldots, x_i\}$.
2. $Y_i \subseteq Y$ is a (possibly infinite) subset of available candidates. This is implicitly represented by a constraint $\psi_i(c)$ such that $Y_i : \{c \in Y \mid \psi_i(c)\}$.

To begin with, $X_0 = \{x_0\}$ for some initial point $x_0 \in X$ and $\psi_0 : \text{true}$ representing the set $Y_0 : Y$.

At each iteration, we perform the following steps:

(a) Choose a candidate solution $c_{i+1} \in Y_i$. This is achieved by solving the formula $\psi_i$ using a constraint solver. Throughout this paper, we will maintain $\psi_i$ as a linear arithmetic SMT formula and use the solver Z3 to tackle this step.

(b) Test the current candidate. This is achieved by testing the satisfiability of $\neg \psi(c_{i+1}, x)$.

If $\neg \psi(c_{i+1}, x)$ is unsatisfiable, then $\psi(c_{i+1}, x)$ is valid for all $x$. Therefore, we can stop with $c = c_{i+1}$ as the required solution.

Otherwise, if $\neg \psi$ is satisfiable for some $x = x_{i+1}$, we add it back as a witness: $X_{i+1} : X_i \cup \{x_{i+1}\}$. The formula $\psi_{i+1}$ is given by

$$\psi_{i+1} : \psi_i \land \psi(c, x_{i+1}).$$

Note that $\psi_{i+1} \models \psi_i$ and $c_{i+1} \not\models \psi_{i+1}$. The set $Y_{i+1}$ is described by $\psi_{i+1}$ is

$$Y_{i+1} : \{c \in Y \mid \psi(c, x_i) \text{ holds for each } x_i \in X_{i+1}\}.$$

The CEGIS procedure either runs forever or terminates with a witness $c : c_i$ whenever it terminates after $i$ iterations. In fact, we provide a modification of CEGIS for synthesizing control Lyapunov-like functions with termination guarantees in our previous work [26].

The CEGIS procedure involves two calls to solvers: (a) Testing satisfiability of $\psi_i(c)$. If the template for the control certificate is chosen as a linear combination of basis function, this is a linear arithmetic formula. (b) Testing the satisfiability of $\neg \psi(c_{i+1}, x)$.

Often for nonlinear switched systems, this is a nonlinear arithmetic satisfiability problem. We have explored two solutions to this problem: (a) use a delta-satisfiability solver such as dReal [10] and (b) if $\psi$ is semi-algebraic in $x$, we may use a LMI relaxation [25].

In this article, we use CEGIS framework for a richer set of specifications, not considered previously. For each different problem, we generalize CEGIS by considering a more general class of witnesses. In doing so, we will also strive to use efficient LMI relaxations to tackle these constraints and present numerical examples for each.

### 4. CEGIS for Safety

We recall control barrier functions for enforcing safety properties [22, 23]. Let $I$ be the initial region, and $S$ safe region s.t. $I \subseteq \text{int}(S)$. We are interested in finding a control invariant set $W$, i.e. $W \implies \Box W$. Suppose $W$ is defined as the sublevel set of a smooth function $C(x)$, i.e., $W = \{x \mid C(x) \leq 0\} \cap S$. First, we require that $I \subseteq \text{int}(W)$ and $W \subseteq \text{int}(S)$.

$$\begin{cases}
(\forall x) x \in I \implies C(x) < 0 \\
(\forall x) x \in \partial S \implies C(x) > 0.
\end{cases}$$

Next, we require that at the boundary of $W$, it is possible to find a control mode which can keep the state inside $W$. Let $\dot{C}_q(x)$ denote the Lie derivative of $C$ in the control mode $q \in Q$. Let $\epsilon > 0$ be a user-defined tolerance.

$$(\forall x \in S) C(x) = 0 \implies (\exists q \in Q) \dot{C}_q(x) < -\epsilon.$$  \hspace{1cm} (3)

The equation, combined with the smoothness of $C$ and $f_q$, ensure that as soon as the state is sufficiently “close” to the boundary of $W$, it is possible to choose a control mode that ensures the local decrease of the $C$. Note that since the number of control modes is finite, the existential quantifier $\exists q \in Q$, is equivalent to the disjunction $\lor q$. 

Remark 1. Equation \((5)\) appeals to Nagumo theorem for its justification, and requires extra constraint qualifications on \(C\) \([3]\).

To synthesize a barrier \(C\), we start with a template form \(C(e, x) : \sum_{i=1}^{N} e_i g_i(x)\) with some basis functions \(g_1(x), \ldots, g_N(x)\) chosen by the user and unknown coefficients \(e : (c_1, \ldots, c_N)\) such that \(c \in Y\). Note that \(\mathcal{C}_q(e, x) : \sum_{i=1}^{N} c_i \mathcal{C}_q(e, x)\), wherein \(\mathcal{C}_q\) is the Lie derivative of \(g_i\) in mode \(q\). This is a linear function over \(e\). Therefore, the constraints become

\[
\begin{align*}
\exists e \forall x \left\{ \begin{array}{l}
 x \in I \implies C(e, x) < 0 \\
 x \in \partial S \implies C(e, x) > 0 \\
 x \in S \implies \left( C(e, x) = 0 \implies \bigvee_{q \in Q} \mathcal{C}_q(e, x) < -\epsilon \right) .
\end{array} \right.
\end{align*}
\]

(4)

It is important to note the structure of these constraints. In the CEGIS procedure, the \(\Psi(e, x)\) will have the form below:

\[
\begin{align*}
 x \in R_1 \implies \varphi_1(e, x) \\
 x \in R_2 \implies \varphi_2(e, x) \\
 \ldots
 x \in R_{N_k} \implies \varphi_{N_k}(e, x) ,
\end{align*}
\]

(5)

and each \(\varphi_k\) for \(k = 1, \ldots, N_k\) has form \(\bigvee_i p_{k,i}(e, x) > 0\), where \(p_{k,i}(e, x)\) is a function linear in \(e\) and possibly nonlinear in \(x\), depending on the dynamics.

We now describe the CEGIS procedure for constraints represented in Equation \((5)\).

Witness Structure
For the constraints in Equation \((5)\) the witness is simply a state \(x \in X\) if a nonlinear SMT solver such as dReal is used.

Otherwise, if the LMI relaxation is to be used, the witness structure is more complex. The basic idea is introduced in our previous work \([25]\). This approach works only if in Equation \((5)\), each \(R_k\) is a conjunction of polynomial inequalities and each \(p_{k,i}\) is a polynomial. Briefly, the approach chooses a set of monomials \(x_i\) wherein \(x_i\) is a monomial over \(x\). The witnesses of the CEGIS procedure are defined to be \(Z = zz'\).

Finding Witnesses Finding a witness for a given candidate solution \(e_i\) involves checking the satisfiability of \(\neg \Psi\). Whereas \(\neg \Psi\) is a conjunction of \(N_k\) clauses, \(\neg \Psi\) is a disjunction of clauses. The \(k^{th}\) clause in \(\neg \Psi\) \((1 \leq k \leq N_k)\) has the form

\[
x \in R_k \land \bigwedge_i p_{k,i}(e_1, x) \leq 0 .
\]

(6)

We will test each clause separately for satisfiability. Assuming that \(p_{k,i}\) is a general nonlinear function over \(x\), SMT solvers like dReal \([10]\) can be used to solve this over a compact set \(R_k\). Numerical SMT solvers like dReal can either conclude that the given formula is unsatisfiable or provide a solution to a “nearby” formula that is \(\delta\) close. The parameter \(\delta\) is adjusted by the user of the procedure. As a result, dReal can correctly conclude that the current candidate yields a valid certificate. On the other hand, its witness may not be a witness for the original problem. In this case, using the spurious witness may cause the CEGIS procedure to potentially continue (needlessly) even when a solution \(e_i\) has been found. Nevertheless, the overall procedure produces a correct result whenever it terminates with an answer.

If LMI relaxations are used, we rewrite \((6)\) as

\[
\bigwedge_j (R_{k,j}, Z) \leq 0 \land \bigwedge_i (P_{k,i}, Z) \leq 0 \land Z \geq 0 .
\]

In particular, we drop the rank one constraint on \(Z\), since \(Z : zz'\). We write each polynomial \(p_{k,i}(e_1, x)\) as \((P_{k,i}, Z)\) wherein \((A, B) : tr(AB)\). The first set of conjunctions \(\bigwedge_j (R_{k,j}, Z) \leq 0\) represents \(x \in R_k\). The subsequent set represents \(\bigwedge_i p_{k,i}(e, x) \leq 0\). If this LMI is infeasible, then so is the original clause. Otherwise, the LMI is feasible and yields a solution \(Z\). This \(Z\) does not yield a witness \(x\) for the original clause. We simply extend CEGIS to incorporate \(Z\) as a witness.

Finding Candidate Solutions Given a finite set of witnesses \(X_i\), a solution exists for \(\psi_{i+1}\) iff there exists \(e \in C_0\) s.t. for all \(x \in X_i\) and \(1 \leq k \leq N_k\)

\[
\bigwedge_{i \in X_i} \bigwedge_{k=1}^{N_k} \left( x \in R_i \implies \bigvee_i p_{k,i}(e, x) > 0 \right) ,
\]

and since \(p_{k,i}\) is a linear function in \(e\), such \(e\) can be found by solving a formula in Linear Arithmetic Theory \((L\mathcal{A})\). If the witnesses are matrices of the form \(X_i : \{Z_0, \ldots, Z_N\}\), we rewrite the constraints \(x \in R_i\) and \(p_{k,i}(e, x)\) in terms of \(Z\). This will yield linear arithmetic constraints involving \(e\), as before.

4.1 Practical Issues The condition in Equation \((1)\) can be encoded into the CEGIS framework. However, the presence of the equality \(C(e, x) = 0\) poses practical problems. In particular, it requires for each candidate \(e_i\), to find a counterexample \(x\) such that \(C(e, x) \neq 0\). Unfortunately, such an assertion is easy to satisfy, resulting in the procedure always exceeding the maximum number of iterations permitted. One solution is to relax the third condition to the following condition:

\[
x \in S \setminus I \implies \bigvee_q \mathcal{C}_q(e, x) < -\epsilon .
\]

(7)

This expands the region for which \(C\) is to be decreased. Another idea involves exponential barrier certificates \([15]\):

\[
x \in S \setminus I \implies \bigvee_q \mathcal{C}_q(e, x) < \lambda C(e, x) - \epsilon .
\]

In fact, we find that the following generalization is particularly effective in our experiments

\[
x \in S \setminus I \implies \bigvee_q \left\{ \left( \mathcal{C}_q(e, x) < \lambda C(e, x) - \epsilon \right) \lor \left( \mathcal{C}_q(e, x) < -\lambda C(e, x) - \epsilon \right) \right\} ,
\]

(8)

for some constant \(\lambda\).

Intuitively, by choosing \(\lambda = 0\), the condition is identical to Equation \((7)\) (conservative), whereas as \(|\lambda| \to \infty\), the condition gets less conservative and in the limit, it is equivalent to \(C(e, x) < -\epsilon\) as \(C(e, x) = 0\). In fact, for smaller \(|\lambda|\) CEGIS terminates faster but at the cost of missing potential solutions. On the other hand, using larger \(|\lambda|\), is less conservative at the cost of CEGIS timing out.

Theorem 1. Given sets \(I\) and \(S(I \subseteq \text{int}(S))\), a certificate \(C\) satisfying Equation \((5)\), gives control strategy with min-dwell time property s.t. \(I \implies \square S\) under Assumption \([7]\).

The proof is provided in the appendix.
5. REACH-WHILE-STAY WITH OBSTACLES

Assume we are interested in $S \implies S \cup G$, where $S := \{x|p(x) \leq 0\}$ for some given smooth function $p$. In addition, $\partial S = \{x|p(x) = 0\}$ is empty as well as $\text{int}(S) = \{x|p(x) > 0\}$. We wish to ensure the system stays in $S$ until finally reaches $G$. The resulting certificate $C(e, x)$ guarantees that $C$ strictly decreases whenever $x \in S \setminus G$ and that $p$ decreases at the boundary of $S$. In particular, we use $p$ itself as a barrier to simplify the problem. Therefore, the constraints on the certificate will have the following form:

$$\forall x \in \text{int}(S) \setminus G \implies \bigvee_q \hat{C}_q(e, x) < -\epsilon$$

$$\forall x \in \partial S \setminus G \implies \bigvee_q \left( \hat{C}_q(e, x) < -\epsilon \land \hat{p}_q(x) < -\epsilon \right),$$

where $\hat{p}_q(x)$ is the derivative of $p(x)$ under dynamics of mode $q$.

Considering the CEGIS procedure, again the $\Psi(e, x)$ have the form of Equation (5). However, $\varphi_k$ has a slightly different form:

$$\bigvee_j p_{k,i,j}(e, x) > 0.$$  

Finding Witnesses For finding a counterexample $x$ (given a candidate $c_i$), we use a SMT solver to find a $x$ and a clause $1 \leq k \leq N_k$ s.t.

$$x \in R_k \land \bigvee_j p_{k,i,j}(c_i, x) \leq 0. \quad (10)$$

However, the LMI relaxation cannot be used directly, since there are disjunctions in Equation (10). We address this problem later in Section 3.

Finding Candidate Solutions In order to find a candidate $c_i$, one needs to check whether there exists a $c$ s.t.

$$\bigwedge_{x \in X_k} \bigwedge_{k=1}^{N_k} \left( x \in R_k \implies \bigvee_j p_{k,i,j}(c, x) > 0 \right).$$

Since each $p_{k,i,j}$ is linear in $c$, this problem also gives exactly a formula in $\mathcal{L}A$ and the conditions are similar to the problem in Section 3.

5.1 Solving Reach-While-Stay with Obstacles

Given a target region $G$ and a safe region $\hat{S} \subseteq \hat{S}$, we are interested in specication $\hat{S} \implies \hat{S} \cup G$. However, we define $\hat{S}$ as $\text{int}(\hat{S}) \setminus \{O_1 \cup \cdots \cup O_j\}$, wherein $\hat{S}$ is a compact outer region and $O_1, \ldots, O_j$ represent disjoint obstacles.

A nondegenerate basic semialgebraic set $K$ is defined as a conjunction of polynomials $K = \{x|p_{k,i}(x) \leq 0 \land \cdots \land p_{k,j}(x) \leq 0\}$. For each $i \in [1,j], h_i = \{x|x \in K \land p_{k,i}(x) = 0\}$. We require that (a) each $h_i$ is nonempty, (b) the boundary $\partial K$ is given by $\bigcup_{i=1}^j h_i$, and the interior by $\bigcap_{i=1}^j p_{k,i}(x) < 0$, and (c) the boundary is nonempty.

We will assume that sets $S, O_1, \ldots, O_k$ are nondegenerate semialgebraic sets. In these problems, the choice of mode $q$ must satisfy the liveness property $\hat{S} \setminus G$.

$$x \in (\hat{S} \setminus G) \implies \bigvee_q \hat{C}_q(e, x) < -\epsilon. \quad (11)$$

Next, we focus on the property of remaining in $\hat{S}$. In particular, we require a condition that ensures that the flow avoids crossing any point on the surface of $S$, $O_1, \ldots, O_j$. For simplicity, let $S : O_0$. Care should be taken to properly characterize the points at the surface of these sets.

Let each $O_i$ be represented as $\bigwedge_{j \neq o} p_{o,j}(x) \leq 0$, for $i = 0, \ldots, i$, and $H_{i,j} = \{x|x \in O_i \cap S \land p_{o,j}(x) = 0\}$ for each $O_i$ ($i > 0$). Also, we partition the boundary of $S$ into nonempty facets $F_1, \ldots, F_k$. Each facet $F_k$ is, in turn, defined by two sets of polynomials $F_k^c$ of inactive constraints and $F_k^e$ of active constraints.

$$F_k = \{x|\bigwedge_{p_{o,j}(x) < 0} \land \bigwedge_{p_{o,j}(x) = 0}\}.$$  

For each facet of $S$, we require the derivatives of the equalities of the facet to point inside $S$:

$$\begin{cases} x \in F_1 \implies \bigvee_q \left( \hat{C}_q(x) < -\epsilon \land \bigwedge_{p \in F_1^c} \hat{p}_q(x) < -\epsilon \right) \land \bigwedge_{p \in F_1^e} \hat{p}_q(x) < -\epsilon \right) \\

x \in F_i \implies \bigvee_q \left( \hat{C}_q(x) < -\epsilon \land \bigwedge_{p \in F_i^c} \hat{p}_q(x) < -\epsilon \right) \land \bigwedge_{p \in F_i^e} \hat{p}_q(x) < -\epsilon \right). \quad (12) \end{cases}$$

For each $H_{i,j}$ of each $O_i$, the flow must point outwards from the
obstacle $O_i$.

\[
\begin{aligned}
\forall x \in H_{i,1} & \implies \forall q\left( \hat{C}_q(x) < -\epsilon \land \hat{p}_{i,j q}(x) > \epsilon \right) \\
\forall x \in H_{i,2} & \implies \forall q\left( \hat{C}_q(x) < -\epsilon \land \hat{p}_{i,j q}(x) > \epsilon \right).
\end{aligned}
\]  
(13)

And finally, if $H_{i,j}$ has intersection with $F_{i'}$, then the flow must respect both constraints:

\[
\forall x \in H_{i,j} \cap F_{i'} \implies \forall q\left( \hat{C}_q(x) < -\epsilon \land \hat{p}_{i,j q}(x) > \epsilon \right).
\]  
(14)

The overall condition is a conjunction of equations (11), (12), (13), (14):

\[
(\exists \epsilon) \forall x \left( \text{(11)} \land \text{(12)} \land \text{(13)} \land \text{(14)} \right).
\]  
(15)

**Theorem 2.** Given regions $\hat{S}$ and $G (G \subseteq \hat{S})$, and a certificate $C$ satisfying Equation (15), there exists a control strategy respecting min-dwell time property which guarantees $\hat{S} \implies \tilde{S} \cup G$ under Assumption 7.

The proof can be found in the appendix.

The condition above is in the form of constraints explained in this section for the CEGIS framework. Now, consider two such problem instances.

**Example 2.** This example is adopted from [20]. There are two variables and three control modes. The reader can refer to [20] for dynamics of each mode. The goal is to reach the target set $G$ as shown in Figure 2, while staying in the safe region $S$. The authors in [20] used an abstraction-based method using CEGAR procedure to solve such problem. Alternatively, we are using a constraint-based method using CEGIS procedure.

First, we change the bases and set $(-0.75, 1.75)$ as the new origin. Then, we use a quadratic template for the CLF $(c_1 x_1^2 + c_2 x_2^2 + c_3 x_1 x_2)$, $\epsilon = 0.1$ and we are able to find a certificate $C$ in 4 iterations. After we find a certificate, we translate the function back to the original system (before changing the origin):

\[
C(x, y) = 100x_1^2 + 30.375x_1x_2 + 96.84375x_1 + 42.938x_2^2 - 127.50175x_2 + 147.8804375.
\]

The following example is a more complicated one where obstacles are completely inside the safety region.

**Example 3.** The goal is to reach $G$ as shown in Figure 2. There are two variables and three different modes with the following dynamics.

\[
\begin{aligned}
q_1 \left\{ \begin{array}{l}
x = -x - 2x^2 + 2.5y \\
y = -3.3x
\end{array} \right., \\
q_2 \left\{ \begin{array}{l}
x = x \\
y = 2x - 2y
\end{array} \right., \\
q_3 \left\{ \begin{array}{l}
x = 1 \\
y = 0.2y
\end{array} \right.
\end{aligned}
\]

However, there is no strategy to guarantee $\hat{S} \implies \tilde{S} \cup G$, because there are states on the boundary of $S$, from which the safety is violated for each mode. Therefore, we are interested in ensuring $I \implies \tilde{S} \cup G \subseteq \text{int}(S)$, where $I : \{(x, y) | x^2 + y^2 \leq 0.8\}$. Adding the following conditions will ensures there is an invariant inside $S$, which contains $I$.

\[
\begin{aligned}
\forall x \in I & \implies C(c, x) < 0 \\
\forall x \in \partial S & \implies C(c, x) > 0.
\end{aligned}
\]

See Section 6.2 for more details. We used template of the form $c_1 x_1^2 + c_2 x_2^2 + c_3 x_1 x_2 - 1$. The CEGIS procedure using dReal could find a CLF with parameters $\epsilon = 0.001$ within 3 iterations:

\[
C(x, y) = 1.1914y^2 + 0.67188xy + 1.1016x^2 - 1.
\]

**6. SYSTEMS WITH DISTURBANCES**

Let us suppose a control Lyapunov-like function $C(c, x)$ that guarantees an eventuality property. We guarantee that for each state $x$, there exists a switching mode $q$ so that $\hat{C}_q$ is negative:

\[
(\exists \epsilon) \forall x \in R \implies \forall q \hat{C}_q(c, x) < -\epsilon.
\]  
(16)

Let us now consider disturbances to this formulation:

\[
(\exists \epsilon) \forall x \in R \implies \forall \forall d \in D \hat{C}_q(c, x, d) < -\epsilon.
\]
where \( \dot{C}_{\gamma}(c, x, d) \) is the Lie derivative of \( C(c, x) \) under dynamics of mode \( q \) and disturbance \( d \). Using CEGIS procedure, again the \( \Psi(c, x) \) have the form of Equation [5]. However, unlike previous problems, \( \varphi_k \) has form below:
\[
\bigvee_i (\forall d \in D) \; p_{k,i}(c, x, d) > 0.
\]  

(17)

6.1 Extension to \( \forall \exists \forall \) Constraints

We will now extend the original CEGIS framework to handle further quantifier alternations that arise in synthesis problems involving disturbances. Considering general structure for problems with disturbances, \( \Psi \) has the form
\[
\bigwedge_{k=1}^{N_k} \left( x \in R_k \Rightarrow \bigvee_{i=1}^{N_i} (\forall d) \; p_{k,i}(c, x, d) > 0 \right).
\]

(18)

A simple solution consists of applying CEGIS for \( \forall \) described previously. However, doing so yields quantified constraints for the problem step of generating a new candidate and for the step where these candidates are tested. To avoid quantified constraints, we modify the structure of our witnesses.

Witness Structure: Originally, our witnesses included a set of states \( X_i = \{x_0, \ldots, x_i\} \). With disturbances, each witness has the following structure:
\[
\gamma : (x, (1, d_1), \ldots, (N, d_{N_i}))
\]

In other words, the witness consists of a state of the plant and a disturbance input for each possible disjunctive clause in Equation (18) of the plant. Its purpose is to describe a possible violation of the formula \( \Psi \) in Equation (18). Note from the structure of Equation (18), that such a violation provides a value for \( x \) and a map from each \( i \) to a disturbance.

In the \( I^{th} \) iteration, the set \( X_i \) becomes a set of witnesses of the form \( \left\{ \gamma_0, \ldots, \gamma_i \right\} \). For each witness \( \gamma \), we define an instantiation \( \Psi[\gamma] \) of Equation (18):
\[
\Psi[\gamma] : \bigwedge_{k=1}^{N_k} \left( x \in R_k \Rightarrow \bigvee_{i=1}^{N_i} \psi_i(c, x, d_1) \vee \cdots \vee \psi_{N_i}(c, x, d_{N_i}) \right).
\]

Note that \( \Psi[\gamma] \) is a formula that only involves \( c \).

Given a set of witnesses \( X_i \), the new candidate \( c_{i+1} \) is generated by solving:
\[
\bigwedge_{j=0}^{i} \Psi[\gamma_j].
\]

A satisfiable solution \( c = c_{i+1} \) forms the next candidate. Given a candidate \( c = c_{i+1} \), we check \( \neg \Psi \) that has the following form:
\[
\bigwedge_{k=1}^{N_k} \left( x \in R_k \land \bigwedge_{i} (\exists d) \psi_i(c, x, d) \right).
\]

To check whether \( \neg \Psi \) is satisfiable, we query each disjunct of this formula in order, separately. Normally, the inner existential quantifier for \( d \) will pose an issue. However, we remove it by introducing fresh variables \( d_i \) corresponding to \( i \). As a result, we obtain
\[
x \in R_k \land \bigwedge_i \psi_i(c, x, d_i).
\]

A satisfiable solution to this problem of the form \( (x, d_1, \ldots, d_{N_i}) \) yields a witness. Otherwise, if all disjuncts are unsatisfiable, we conclude that the current certificate is valid.

Table 3: Result of CEGIS Framework for Example

| \( t_D \) | Itr | Time |
|--------|-----|------|
| 0.0001 | 2   | 1.3  |
| 0.04   | 2   | 2.0  |
| 0.05   | 3   | 22.7 |
| 0.06   | 3   | 19.4 |
| 0.07   | 5   | 15.9 |
| 0.08   | 17  | 63.7 |

Legend: Itr : # iterations, Time : total computation time (seconds)

6.2 Reach-While-Stay with Disturbances

In our previous work, we have shown that a reach-while-stay property can be addressed by finding a control Lyapunov function and also by making sure a level-set of the CLF is a control barrier certificate. More precisely, given a target region \( G \), an initial region \( I \) and a safe region \( S \) s.t. \( G \subseteq I \subseteq \text{int}(S) \), we are interested in specification \( I \Rightarrow SU(G) \). A set of condition on certificate \( C \) which guarantees the reach-while-stay property is as follows:
\[
\begin{align*}
\{ x \in I \Rightarrow C(c, x) < 0 \\
x \in \partial S \Rightarrow C(c, x) > 0 \\
x \in S \setminus G \Rightarrow \bigvee_q \dot{C}_q(c, x) < -\epsilon.
\end{align*}
\]

(19)

For a CLF \( C \) in simple words, we need at each point, the existence of a mode \( q \) which can decrease the value of CLF \( \dot{C}_q(c, x) < 0 \). To guarantee the min-dwell time property, we use a more restricted condition \( \dot{C}_q(c, x) < -\epsilon \).

The disturbances for this problem can be handled in two ways. The simplest solution is to make the controller robust by increasing the size of \( \epsilon \) in Equation (19). However, the more precise solution can be obtained by solving the following problem encoding
\[
\begin{align*}
\{ x \in I \Rightarrow C(c, x) < 0 \\
x \in \partial S \Rightarrow C(c, x) > 0 \\
x \in S \setminus G \Rightarrow \bigvee_q (\forall d \in D) \dot{C}_q(c, x, d) < -\epsilon.
\end{align*}
\]

(20)

Theorem 3. Under Assumption [7] given compact regions \( G \), \( I \), and \( S \) \( (G \subseteq I \subseteq \text{int}(S)) \), and a certificate \( C \) satisfying Equation (20), there exists a control strategy respecting min-dwell time property which guarantees \( I \Rightarrow SU(G) \) in the presence of disturbances.

The proof is provided in the appendix.

To evaluate the CEGIS framework, we consider several problem instances and we compare it with cases where there is no disturbances. These examples are carefully chosen s.t. the abilities and weaknesses of these methods are demonstrated.

In the following examples, we assume \( D \) is a hyper-box in the form \([-t_D, t_D]^n\) and similarly, \( S \) is \([-t_S, t_S]^n\). Also, \( G \) and \( I \) are hyper-ball with radius \( r_G \) and \( r_I \). Also, for all examples, we use template \( (\sum_{i,j} c_{i,j} x_{i,j}) - 1 \).

Example 4. We consider Example without obstacles and with disturbances. We use \( \epsilon = 0.0001, r_G = 0.3 \) and \( t_D = 1.0 \).

To evaluate the effect of disturbances on the CEGIS procedure, we use different disturbance sizes. The results are shown in Table [3]

As results suggests, bigger disturbances impose harder restrictions on the CLF and more search of candidate space may be needed to find a CLF, as the size of disturbance gets bigger.
Example 5. This problem instance is taken from [22] with two variables and a control input $u \in [-4, 4]$.

\[
\begin{align*}
\dot{x} &= u + d_x \\
\dot{y} &= y^3 x + d_y.
\end{align*}
\]

Considering discrete version of the control input, there are two modes ($u \in \{-4, 4\}$). The specification is $I \implies$ SLG, with $r_I = 0.5$, $r_S = 0.2$, and $r_D = 0.0002$. To find a CLF for switched systems, we use $\epsilon = 0.0001$.

The CEGIS procedure terminates within 13 iterations (30 seconds). The LMI relaxation can also be used. However, using the LMI relaxation, one can only find a weak control Lyapunov function (i.e., $\epsilon = 0$ and $r_D = 0$). This example demonstrates that the LMI relaxation can be conservative.

Example 6. The following example is taken from [6]. The system has 3 continuous variables with 4 different modes as follows:

\[
\begin{align*}
q_1: \quad & \dot{x} = 4.15x - 1.06y - 6.7z + 1 + d_x \\
& \dot{y} = 5.74x + 4.78y - 4.68z - 4 + d_y \\
& \dot{z} = 26.38x - 6.38y - 8.29z + 1 + d_z \\
q_2: \quad & \dot{x} = -3.2x - 7.6y - 2z + 4 + d_x \\
& \dot{y} = 0.9x + 1.2y - z - 2 + d_y \\
& \dot{z} = x + 6y + 5z - 1 + d_z \\
q_3: \quad & \dot{x} = 5.75x - 16.48y - 2.41z - 2 + d_x \\
& \dot{y} = 9.51x - 9.49y + 19.55z + 1 + d_y \\
& \dot{z} = 16.19x + 4.64y + 14.05z - 1 + d_z \\
q_4: \quad & \dot{x} = -12.38x + 18.42y + 0.54z - 1 + d_x \\
& \dot{y} = -11.9x + 3.24y - 16.32z + 2 + d_y \\
& \dot{z} = -26.5x - 8.64y - 16.6z + 1 + d_z.
\end{align*}
\]

The specification is again $I \implies$ SLG where $r_G = 0.1$, $r_I = 0.5$, $r_D = 1.0$ and $r_D = 0.1$. We consider $\epsilon = 0.001\|x\|^2$.

While the CEGIS framework finds a solution in absence of disturbances in 77 seconds (12 iterations), the CEGIS framework fails (timed out) when disturbances are considered as the number of variables in witness space grows to 15. However, using the LMI relaxation, the procedure can successfully find a CLF in 7 seconds even when the disturbance is allowed.

Example 7. This example is adopted from [19, 23]. The goal is to keep different rooms of an apartment warm, using few number of active heaters. The reader can refer to the mentioned articles for details description of these systems. While, the problems are similar, the number of variables are different and we use these problem instances to demonstrate the scalability of the CEGIS procedure for $\epsilon = 0.001$. The results are shown in Table 2.

The results suggest that the CEGIS framework can get scaled to bigger problems using LMI relaxation. It is worth mentioning that the last problem instance with disturbances (9 state variables and witness space with 45 variables) failed using LMI relaxation because of numerical issues in the SDP solver. Nevertheless, it was solved in less than 6 hours when $r_D = 0.0002$.

7. CEGIS WITH LMI RELAXATION

Recall that in Section 5 LMI relaxation could not be used for solving the problem of interest as Equation (10) contained disjunctions. In this section, we discuss solving such problem using the LMI relaxation.

We say vector $\lambda$ is in set $\Lambda (\lambda \in \Lambda)$ iff

\[\bigwedge_j \lambda_j \geq 0 \land \sum_j \lambda_j = 1.\]

It is easy to verify that

\[\bigwedge_j p_j(x) > 0 \iff \forall (\lambda \in \Lambda) \sum_j \lambda_j p_j(x) > 0.\]

Therefore, Equation (9) can be replaced by

\[\bigwedge_i \left(\forall (\lambda \in \Lambda) \left(\sum_j \lambda_j y^{i,j}(c, x) > 0\right)\right),\]

which is equivalent to Equation (17). In other words, the problem in Section 5 can be reduced to the problem in Section 6.

One can apply the CEGIS framework to solve such problem using LMI relaxation. However, this reduction comes at the cost of bigger witness space. On the other hand, LMI relaxation is much more scalable and this increase in the witness space will not pose a big challenge. In conclusion, if LMI relaxation is the method of choice for finding witnesses, the reduction explained above solves the problem. Otherwise, (if SMT solvers are used for finding witnesses), the solution explained in Section 5 practically works better as the size of witness space is much smaller.

Example 8. The unicycle (adapted from [16]) has three variables $x$, $y$, and $\theta$. The velocity and angular velocity are control inputs.

\[
\begin{align*}
\dot{x} &= u_1 \cos(\theta) \\
\dot{y} &= u_1 \sin(\theta) \\
\dot{\theta} &= u_2,
\end{align*}
\]

and once treated as a switched system, the input is $(u_1, u_2) \in \{(-0.1, 0.1), (-5, 5)\}$. The goal is again $I \implies$ SLG with $r_G = 0.1$ and $r_I = 0.4$ and $r_S = -1$. 

| Problem | dReal | LMI |
|---------|-------|-----|
| No Dist | Dist  | No Dist | Dist |
| $n$ | $m$ | $r_D$ | Time | Status | Time | Status | Time | Status | Time | Status |
| 3 | 4 | 0.02 | 2.2 | ✓ | 14.5 | ✓ | 0.5 | ✓ | 7.7 | ✓ |
| 4 | 5 | 0.01 | 14.9 | ✓ | - | ✓ | 1.5 | ✓ | 64.6 | ✓ |
| 5 | 6 | 0.0015 | 596.5 | ✓ | - | ✓ | 3.7 | ✓ | 484.8 | ✓ |
| 6 | 4 | 0.01 | 2995.6 | ✓ | - | ✓ | 9.2 | ✓ | 679.0 | ✓ |
| 9 | 4 | 0.01 | - | ✓ | - | ✓ | 202.3 | ✓ | - | Failed |

Legend: $n$ : # state variables, $m$ : # modes, Time : total computation time (seconds), ✓ : Success, × : Timed Out (> 1 hour)
Notice that there are trigonometrical terms in the dynamics. While some SMT solvers cannot be used for the CEGIS framework, it is possible to use the ones which can handle trigonometrical terms (e.g., dReal).

We choose to use template of form $c_1 x^2 + c_2 xy + c_3 y^2 - 1$ and $c = 0.001$.

The traditional condition on CLF (condition on first order derivative) fails to find a solution. This issue comes from the fact that by choosing a CLF which is independent of $\theta$, there is no benefit coming from input $u_2$ ($\dot{C}_q$ is independent of $u_2$). And obviously, if we do not take $u_2$ into account, we cannot satisfy the property.

Here, we consider a more flexible condition on the certificate.

$$
\begin{align*}
\{ & x \in I \implies C(c, x) < 0 \\
& x \notin \partial S \implies C(c, x) > 0 \\
& x \in S \setminus G \implies \bigvee_q \left( \dot{C}_q(c, x) < -\epsilon \lor \dot{C}_q(c, x) \leq 0 \land \dot{C}_q(c, x) < -\epsilon \right) \}.
\end{align*}
$$

Theorem 4. Given sets $G, I, S (G \subseteq I \subseteq \text{int}(S))$, and a certificate $C$ satisfying Equation (21), there is a control strategy guaranteeing min-dwell time property s.t. $I \implies \text{SUG under Assumption}^7$.

The proof is provided in the appendix.

This condition seems more complicated. However, the second derivative helps to take the advantage of $u_2$. The conditions in Equation (21) can be encoded into CEGIS framework as it has form of the problem discussed in Section 5. The method explained in Section 5 can find a CLF using dReal as witness finder.

Also, if one prefers to use LMI relaxation, a possible solution is to change the bases of the state space s.t. the dynamics for each mode can be described using polynomial functions. For example, here we chose to use independent variables $s$ (for $\sin(\theta)$) and $c$ (for $\cos(\theta)$) instead of $\theta$ with the following dynamics

$$
\begin{align*}
\dot{x} &= u_1 c \\
y &= u_1 s \\
\dot{s} &= u_2 c \\
\dot{c} &= -s u_2.
\end{align*}
$$

And also we consider just region $s^2 + c^2 = 1$. Now, using the reduction discussed above, the CEGIS framework with LMI relaxation finds a CLF.

8. CONCLUSIONS

In this paper, given a switched system, we addressed some controller synthesis problems for safety and reach-while-stay properties, namely, (i) safety, (ii) reach-while-stay with obstacles (iii) reach-while-stay for systems with disturbances. For each problem, we provided a sufficient conditions in terms of “existence of a control certificate”. Also, we provided a general CEGIS framework which is an extension of our previously established framework to find such certificates. In the future, we wish to investigate how this approach can be extended for more general properties such as LTL. One other possible direction for future work is to investigate using linear relaxations [1][28], instead of LMI relaxation, to make the approach even more scalable.

9. ACKNOWLEDGMENTS

This work was supported by the US National Science Foundation (NSF) under CAREER award # 0953941 and CCF-1527075. All opinions and conclusions are those of the authors and not necessarily of the NSF.

10. REFERENCES

[1] A. A. Ahmadi and A. Majumdar. Dsos and dsos optimization: Lp and socp-based alternatives to sum of squares optimization. In Information Sciences and Systems (CISS), 2014 48th Annual Conference on, pages 1–5. IEEE, 2014.

[2] R. Alur, R. Bodik, G. Juniwal, M. M. Martin, M. Raghothaman, S. Seshia, R. Singh, A. Solar-Lezama, E. Torlak, A. Udupa, et al. Syntax-guided synthesis. In Formal Methods in Computer-Aided Design (FMCAD), 2013, pages 1–8. IEEE, 2013.

[3] Z. Artstein. Stabilization with relaxed controls. Nonlinear Analysis: Theory, Methods & Applications, 7(11):1163–1173, 1983.

[4] E. Aydin Gol, M. Lazar, and C. Belta. Language-guided controller synthesis for discrete-time linear systems. In Proceedings of the 15th ACM international conference on Hybrid Systems: Computation and Control, pages 95–104. ACM, 2012.

[5] F. Blanchini and S. Miani. Set-theoretic methods in control. Birkhauser, 2008.

[6] P. Bolzern and W. Spinelli. Quadratic stabilization of a switched affine system about a nonequilibrium point. In American Control Conference, 2004. Proceedings of the 2004, volume 5, pages 3890–3895. IEEE, 2004.

[7] L. de Moura and N. Bjørner. Z3: An efficient SMT solver. In TACAS, volume 4963 of LNCS, pages 337–340. Springer, 2008.

[8] R. Dimitrova and R. Majumdar. Deductive control synthesis for alternating-time logics. In Embedded Software (EMSOFT), 2014 International Conference on, pages 1–10. IEEE, 2014.

[9] G. Frehse, S. K. Jha, and B. H. Krogh. A counterexample-guided approach to parameter synthesis for linear hybrid automata. In Hybrid Systems: Computation and Control, pages 187–200. Springer, 2008.

[10] S. Gao, S. Kong, and E. M. Clarke. dreal: An SMT solver for nonlinear theories over the reals. In Intl. Conference on Automated Deduction (CADE), pages 208–214, 2013.

[11] L. E. Ghaoui and V. Balakrishnan. Synthesis of fixed-structure controllers via numerical optimization. In Decision and Control, 1994., Proceedings of the 33rd IEEE Conference on, volume 3, pages 2678–2683. IEEE, 1994.

[12] Z. Huang, Y. Wang, S. Mitra, G. E. Dullerud, and S. Chaudhuri. Controller synthesis with inductive proofs for piecewise linear systems: an smt-based algorithm. arXiv preprint arXiv:1509.04623, 2015.

[13] J. Kapinski, J. V. Deshmukh, S. Sankaranarayanan, and N. Aréchiga. Simulation-guided lyapunov analysis for hybrid dynamical systems. In Proceedings of the 17th international conference on Hybrid systems: computation and control, pages 133–142. ACM, 2014.

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

A. CONTROLLER DESIGN

For all the proofs which guarantee that there exists a switching strategy respecting min-dwell time property, common approach is used. Given a certificate, the goal is to guarantee some function $g_q(x, d)$ is negative for some time if the mode $q$ is fixed, where $g_q(x) = \max_i g_{i,j,q}(x, d)$. Let $g^{0}_{i,j,q}(x, d) = g_{i,j,q}(x, d)$ and $g^{k}_{i,j,q}$ be the $k$th derivative of $g_{i,j,q}$ w.r.t. $x$ for dynamics of mode $q$. That is

$$g^{k}_{i,j,q}(x, d) = \left( \frac{dg^{k-1}_{i,j,q}}{dx} \right)^t f_q(x).$$

One of the conditions for the certificate has the form

$$\bigvee_q (\bigvee_i \psi_{q,i}(x, \epsilon)),$$

where $\psi_{q,i}(x, \epsilon)$ holds, one can guarantee that $\psi_{q,i}(x, \epsilon^*)$ holds, one can guarantee that $\psi_{q,i}(x, 0)$ holds for some minimum time $\delta$. Therefore, the function switch for a region of interest $R$ is defined as below

$$\text{switch}(q, x) := \begin{cases} q' & \text{if } \left( \bigwedge_i \neg\psi_{q,i}(x, \gamma) \right) \\
q & \text{otherwise} \end{cases}$$

for some fixed $\gamma > 1$.

**Lemma 1.** Given region $S$ is bounded, all functions are differentiable (and thus bounded in $S$) and $\Box S$, if $\psi_{q,i}(x(T), \epsilon)$, there is a time $\delta$ s.t.

$$(\forall t \in [T, T + \delta]) \psi_{q,i}(x(t), \epsilon),$$

Proof. Let $T + \delta$ be the minimum time where $\psi_{q,i}(x(T), \gamma)$ does not hold if

$$(\forall t \in [T, T + \delta]) q(t) = q$$
At time $T$,
$$(\forall j)(\forall d) \left( \sum_{k=1}^{K-1} g_{i,j_k}(x(T),d) \leq 0 \lor g_{i,j_k}^K(x(T),d) < -\varepsilon \right)$$

And as $g_{i,j_q}$ cannot increase, unless $g_{i,j_q}^{k+1}$ becomes positive, at time $T + \delta$, $(\forall j, d)$
$$(\sum_{k=1}^{K-1} g_{i,j_k}(x(T + \delta), d) \leq 0 \lor g_{i,j_k}^K(x(T + \delta), d) = -\varepsilon \gamma \right)$$

Since $S$ is a bounded set, and $f_q(x)$ is bounded over $S$, as well as each $g_{i,j}$, there exists $\Lambda > 0$ s.t.
$$(\forall x \in S, d \in D, j) g_{i,j_q}^{K+1}(x, d) \leq \Lambda.$$ (23)

Therefore,
$$g_{i,j_q}^{K}(x(T + \delta),d(T + \delta)) = g_{i,j_q}^{K}(x(T),d(T)) + \int_T^{T + \delta} g_{i,j_q}^{K+1}(x(t),d(t))dt$$

$$\tag{Equation 22} = -\frac{\varepsilon}{\gamma} \leq -\varepsilon + \Lambda \delta .$$

Then, we can conclude
$$-\frac{\varepsilon}{\gamma} \leq -\varepsilon + \Lambda \delta \implies \frac{(\gamma - 1)\varepsilon}{\Lambda \gamma} \leq \delta .$$

The above arguments suggest that there exists a fixed $\delta > 0$ s.t.
$$(\forall t \in [T, T + \delta]) \psi_{q,i}(x(t), \frac{\varepsilon}{\gamma}) .$$

Now, we can prove that the controller gives a switching strategy.

**Lemma 2.** Given a region of interest $R$ and conditions
$$\psi_q(x, \varepsilon) = \bigvee_q \psi_{q,i}(x, \varepsilon), \text{ s.t.}$$
$$(\forall x \in R) (3q \in Q) \psi_q(x, \varepsilon) .$$

If $(\forall t \in [t_1, t_2]) x(t) \in R$, the controller defined in Equation 22 guarantees for any $\gamma > \gamma$
1. $(\forall t \in [t_1, t_2]) \psi_{q,i}(x(t), \frac{\varepsilon}{\gamma}) .$
2. The controller respects min-dwell time property.

**Proof.** By the definition of the controller, if $\psi_{q,i}(x(t), \frac{\varepsilon}{\gamma})$ does not hold, the controller switches to another mode $q^+(t)$ s.t.
$\psi_{q^+(t)}(x(t), \varepsilon)$ and therefore, $\psi_{q^+(t)}(x(t), \frac{\varepsilon}{\gamma})$ (for any $\gamma > \gamma$) as long as $x(t) \in R$. Also, by Lemma 1, the controller is guaranteed to respect min-dwell time.

**B. PROOFS**

In the following proofs, $C(x) = C(e, x)$ for some fixed $e$. Also, $C(t) = C(x(t))$ and $p(t) = p(x(t))$.

**Proof of Theorem 1.** Given sets $I$ and $S (I \subseteq int(S))$, a certificate $C$ satisfying Equation 8, gives control strategy with min-dwell time property s.t. $I \implies \square S$ under Assumption 1.

**Proof.** We show that there exists a set $W$ s.t.
1. $I \implies \square W$.
2. $I \subseteq int(W)$.
3. $W \subseteq int(S)$.

and as a result, $W \implies \square(S)$. $W$ is defined as $W : \{x|C(x) \leq 0\} \cap S$. By Equation 3, $W \subseteq int(S)$ and $I \subseteq int(W)$.

Having Equation 5 and setting region of interest $R \subseteq S \cap I$ and $\psi_q(x, \varepsilon) \to C_q(x) + \lambda C(x) \leq -\varepsilon \implies C_q(x) + \lambda C(x) \leq -\varepsilon$, according to Lemma 2, there exists a controller with min-dwell time that can guarantee $C(t) < \lambda C(t) - \frac{\varepsilon}{\gamma}$, as long as $x(t) \in S \cap I$. Now we show that $\square(W)$.

In the beginning, $x \in I \implies x \in int(W)$. Trace cannot leave $W$ before reaching $\partial W$. Let $t_3$ be the time at which the trace reaches $\partial W$. Let $t_4$ be the last time $x \in I$, $C(t_4) < 0$ by definition and for all times $t \in (t_3, t_2], x(t) \in S \setminus I$. As mentioned above $\hat{C}(t) < -\lambda C(t) - \frac{\varepsilon}{\gamma}$ for some $\lambda \geq 0$. As a result
$$C(t_2) = C(t_4) + \int_{t_4}^{t_2} \hat{C}(t)dt$$
$$< C(t_4) + \int_{t_4}^{t_2} -\lambda C(t) - \frac{\varepsilon}{\gamma}dt$$
$$< e^{-\lambda(t_2 - t_4)}C(t_4) < 0 .$$

However, $C(t_2) = 0$, which is a contradiction. Therefore, $\square(W)$ holds.

**Proof of Theorem 2.** Given sets $G, I$ and $S (G \subseteq I \subseteq int(S))$ and a certificate $C$ satisfying Equation 21, there is a control strategy guaranteeing min-dwell time property s.t. $I \implies SUg$ under Assumption 1.

**Proof.** We show that there exists a set $W$ s.t.
1. $I \implies WUG$.
2. $I \subseteq int(W)$.
3. $W \subseteq int(S)$.

$W$ is defined as $W : \{x|C(x) \leq 0\} \cap S$. By Equation 21, $W \subseteq int(S)$ and $I \subseteq int(W)$. Having Equation 21, and setting region of interest $S \setminus G$ and $\psi_q(x, \varepsilon) \to \hat{C}_q(x) \leq -\varepsilon \vee (\hat{C}_q(x) \leq 0 \land \hat{C}_q(x) \leq -\varepsilon)$, according to Lemma 2, there exists a controller which respects the min-dwell time property. Also, the controller guarantees $\hat{C}(t) < \frac{\varepsilon}{\gamma} \vee (\hat{C}(t) \leq 0 \land \hat{C}(t) < \frac{\varepsilon}{\gamma})$ as long as $x(t) \in S \setminus G$. This, ensures $C(t)$ does not increase $\hat{C}(t) \leq 0$ and eventually decreases i.e. $(\forall t) C(t + \delta) < C(t) - \Delta C$ (for some $\Delta C > 0$) which means $C(t)$ decreases at minimum average rate $\frac{\Delta C}{\delta}$. Now we show that $I \implies WUG$. Let $T \geq 0$ be the first time instance s.t. $x(T) \in \partial W$ reaches $\partial W (C(T) = 0)$ before reaching $G$. Since $C(0) < 0 (x(0) \in I)$ and $(\forall t \in [0, T]) \hat{C}(t) \leq 0$, the following contradiction is obtained
$$C(T) = C(0) + \int_0^T \hat{C}(t)dt \leq C(0) < 0.$$ Therefore, state trace never leaves $W$ before entering $G$. If $\square(W \setminus G)$, by the construction of the controller, we can conclude time diverges (because the controller respects the min-dwell time property). Also since $C(t)$ decreases at minimum average rate of $\frac{\Delta C}{\delta}$, $C(t)$ decreases to infinity. However, the value of $C$ is bounded on bounded set $W \setminus G$. Therefore, $x$ cannot remain in $W \setminus G$ and the only possible outcome for the trace is to reach $G$.

**Lemma 3.** If for a compact set $R$,
$$(\forall x \in R) \ p(x) < 0 \vee (p(x) = 0 \land \hat{p}(x) < -\varepsilon)$$
holds, then
$$(\forall x \in R) \ p(x) < -\varepsilon \vee (p(x) \leq 0 \land \hat{p}(x) < -\varepsilon),$$ (24)
for small enough $\varepsilon$. 
Proof. First, by Assumption \(A1\) one can show that if \(\hat{p}_q(x^*) < -\epsilon\), then there is a \(\sigma^* > 0\) s.t. for all \(x \in B_{\sigma^*}\), \(\hat{p}_q(x) < -\frac{\epsilon}{2}\). Again by Assumption \(A1\) there is a \(\sigma\) s.t.

\[
(\forall x \in R) \quad p(x) < -\sigma \vee (p(x) \leq 0 \wedge \hat{p}_q(x) < -\frac{\epsilon}{2}).
\]

\(\epsilon' = \min(\sigma, \frac{\epsilon}{2})\) gives Equation (23).

**Proof of Theorem 2**

Given regions \(\hat{S}\) and \(G (G \subseteq \hat{S})\), and a certificate \(C\) satisfying Equation (15), there exists a control strategy respecting min-dwell time property which guarantees \(\hat{S} \implies \hat{S} \cap G\) under Assumption \(A1\).

Proof: In the first step of the proof, we drive another alternative form of Equation (15) which will be used by the controller. There are four cases: (i) If \(x \in \hat{S} \setminus G\), then for all \(i\), \(p_{0,i}(x) < 0\) and also for each obstacle \(O_i\), there is at least one \(j\) s.t. \(p_{i,j}(x) > 0\).

In summary for all \(x \in \hat{S}\) by Equation (11)

\[
(\exists q)
\begin{cases}
\dot{C}_q(x) < -\epsilon \\
\forall j \exists p_{0,j}(x) < 0 \\
\forall j \exists p_{i,j}(x) > 0.
\end{cases}
\]

(ii) If \(x\) is on boundary of \(S\) and not on boundary of any obstacle, there is exactly one \(F_i\) s.t. \(x \in F_i\) and by Equation (12)

\[
(\exists q)
\begin{cases}
\dot{C}_q(x) < -\epsilon \\
\forall p_{0,i}(x) < 0 \\
\forall p_{i,1} < \hat{p}_q(x) < -\epsilon \\
\forall \exists p_{i,2} \exists p_{i,j}(x) > 0.
\end{cases}
\]

(iii) If \(x\) is on boundary of obstacles and not in \(\partial S\), since obstacles are disjoint, there is exactly one \(i'\) s.t. \(x \in \partial O_{i'}\). If \(x \in \text{int}(S)\), then by Equation (13)

\[
(\exists q)
\begin{cases}
\dot{C}_q(x) < -\epsilon \\
\forall p_{0,i}(x) < 0 \\
\exists p_{i',j}(x) > \epsilon \\
\forall p_{i',1} \exists p_{i,j}(x) > 0.
\end{cases}
\]

(iv) If \(x\) is on boundary of obstacles and boundary of \(S\), then there is exactly one \(i'\) s.t. \(x \in \partial O_{i'}\) and exactly one \(1\) s.t. \(x \in F_i\) and by Equation (14)

\[
(\exists q)
\begin{cases}
\dot{C}_q(x) < -\epsilon \\
\forall p_{0,i}(x) < 0 \\
\exists p_{i',j}(x) > \epsilon \\
\forall p_{i',1} \exists p_{i,j}(x) > 0.
\end{cases}
\]

By the conditions above, it is concluded that

\[
(\forall x \in (\hat{S} \cup \partial \hat{S}) \setminus G) \quad (\exists q)
\begin{cases}
\dot{C}_q(x) < -\epsilon \\
\forall j \exists p_{0,j}(x) < 0 \vee \left( p_{0,j}(x) = 0 \wedge \hat{p}_{i,j}(x) < -\epsilon \right) \\
\forall j \exists p_{i,j}(x) > 0 \vee \left( p_{i,j}(x) = 0 \wedge \hat{p}_{i,j}(x) > \epsilon \right)
\end{cases}
\]

Using Lemma \(A3\) it is possible to show that there exists a \(\epsilon'\) s.t.

\[
(\forall x \in (\hat{S} \cup \partial \hat{S}) \setminus G) \quad (\exists q)
\begin{cases}
\dot{C}_q(x) < -\epsilon' \\
\forall j \exists p_{0,j}(x) < -\epsilon' \vee \left( p_{0,j}(x) = 0 \wedge \hat{p}_{i,j}(x) < -\epsilon' \right) \\
\forall j \exists p_{i,j}(x) > \epsilon' \vee \left( p_{i,j}(x) = 0 \wedge \hat{p}_{i,j}(x) > \epsilon' \right)
\end{cases}
\]

Given \(\psi_q(x, \epsilon^*)\) as

\[
\begin{cases}
\dot{C}_q(x) < -\epsilon \\
\forall j \exists p_{0,j}(x) < -\epsilon' \vee \left( p_{0,j}(x) - \epsilon' < -\epsilon' \wedge \hat{p}_{i,j}(x) < -\epsilon' \right) \\
\forall j \exists p_{i,j}(x) > \epsilon' \vee \left( p_{i,j}(x) + \epsilon' \geq \epsilon' \wedge \hat{p}_{i,j}(x) > \epsilon' \right)
\end{cases}
\]

by Lemma \(A2\) there is a controller with min-dwell time property which guarantees \(\psi_q(x(t), \frac{\epsilon'}{\gamma'})\) as long as the trace is in \(\hat{S}\).

Now, assume at time \(T\) for the first time, \(x(T) \in \partial \hat{S}\). If \(x \in \partial S\), then there is a \(j\) s.t. \(p_{0,j}(x(T)) = 0\). Let \(t_1\) be the last time before \(T\) that the controller switches to a mode \(q\) (\(\psi_q(x(t_1), \epsilon')\)). If \(a_1 p_{0,j}(x(t_1)) < -\epsilon'\), by (Lemma \(A1\)), \(p_{0,j}(x(T)) = -\epsilon'\) (contradiction). Otherwise, \(b_1 \hat{p}_{i,j}(x(t_1)) < -\epsilon'\) and again by (Lemma \(A1\))

\[
(\forall t \in [t_1, T]) \quad \hat{p}_{i,j}(x(t)) < -\frac{\epsilon'}{\gamma'},
\]

and consequently,

\[
p_{i,j}(x(T)) = p_{i,j}(x(t_1)) + \int_{t_1}^{T} \hat{p}_{i,j}(x(t)) dt
\]

\[
< p_{i,j}(x(t_1)) + \int_{t_1}^{T} \frac{-\epsilon'}{\gamma'} dt
\]

\[
< p_{i,j}(x(t_1)) < 0,
\]

which is a contradiction. Therefore, \(x(T) \in \partial O_i\) for some \(i\). Let \(t_2\) be the last time before \(T\) the controller switches to a mode \(q\). By the design of the controller, there is a \(j\) s.t.

\[
p_{i,j}(x(t_1)) = \epsilon' \vee (p_{i,j}(x(t_1)) \geq 0 \wedge \hat{p}_{i,j}(x(t_1)) > \epsilon').
\]

If \((a) p_{i,j}(x(t_1)) \geq \epsilon'\) then it is guaranteed \(p_{i,j}(x(T)) > \frac{\epsilon'}{\gamma'}\), which means \(x(T)\) is not on the boundary of \(O_i\). Otherwise, \(\epsilon' < \hat{p}_{i,j}(x(t_1))\). Let \(t_2\) be the first time that \(p_{i,j}(x(t_2)) = 0\). If no such time exists then \(\partial O_i\) will never reach in \([t_1, T]\). Assume \(t_2\) exists. Considering the fact below (obtained by (Lemma \(A1\))

\[
(\forall t \in [t_1, t_2]) \hat{p}_{i,j}(x(t)) > \frac{\epsilon'}{\gamma'},
\]

the contradiction below can be obtained

\[
p_{i,j}(x(t_2)) = p_{i,j}(x(t_1)) + \int_{t_1}^{t_2} \hat{p}_{i,j}(x(t)) dt
\]

\[
> p_{i,j}(x(t_1)) + \int_{t_1}^{t_2} \frac{\epsilon'}{\gamma'} dt
\]

\[
> p_{i,j}(x(t_1)) \geq 0.
\]

Therefore \(\square(\hat{S})\). If \(\square(\hat{S} \setminus G)\), by the construction of the controller, we can conclude time diverges and for all times \(\hat{C}(t)\) is less
than \( -\frac{\epsilon'}{\gamma'} \). With similar reasoning used in Theorem 4, it is guaranteed \( \odot G \) and therefore \( \hat{S}UG \).

\[ \square \]

**Proof of Theorem 3** Under Assumption 1, given compact regions \( G, I \) and \( S \) (\( G \subseteq I \subseteq \text{int}(S) \)), and a certificate \( C \) satisfying Equation (20), there exists a control strategy respecting min-dwell time property which guarantees \( I \implies \hat{S}UG \) in the presence of disturbances.

**Proof.** Using Lemma 2, the proof is similar to the proof of Theorem 4. \( \square \)