Title

Sufficient conditions for satisfaction of formulas with until operators in hybrid systems

ISBN

9781450370189

Authors

Han, Hyejin
Maghenem, Mohamed
Sanfelice, Ricardo G

Publication Date

2020-04-22

DOI

10.1145/3365365.3382223

Peer reviewed

Sufficient Conditions for Satisfaction of Formulas with Until Operators in Hybrid Systems

Hyejin Han
University of California, Santa Cruz,
CA 95064, USA
hhan7@ucsc.edu

Mohamed Maghenem
University of California, Santa Cruz,
CA 95064, USA
mmaghene@ucsc.edu

Ricardo G. Sanfelice
University of California, Santa Cruz,
CA 95064, USA
ricardo@ucsc.edu

ABSTRACT

In this paper, we introduce tools to verify the satisfaction of temporal logic specifications using the until operator for hybrid dynamical systems. Hybrid dynamical systems are given in terms of differential and difference inclusions, which capture the continuous and discrete dynamics (or events), respectively. For such systems, conditional invariance and eventual conditional invariance are employed to characterize dynamical properties associated with the until operators. Sufficient conditions for the satisfaction of temporal logic specifications involving the until operator are provided by guaranteeing properties of the data defining the systems and the existence of barrier functions or Lyapunov-like functions. Examples illustrate the results throughout the paper.

CCS CONCEPTS

• **Theory of computation → Logic and verification**; **Modal and temporal logics**; *Linear logic*; • **Computer systems organization →** Embedded and cyber-physical systems.

KEYWORDS

Linear temporal logic, until operator, forward invariance, conditional invariance, hybrid systems.

ACM Reference Format:
Hyejin Han, Mohamed Maghenem, and Ricardo G. Sanfelice. 2020. Sufficient Conditions for Satisfaction of Formulas with Until Operators in Hybrid Systems. In *23rd ACM International Conference on Hybrid Systems: Computation and Control (HSCC '20), April 22–24, 2020, Sydney, NSW, Australia.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3365365.3382223

1 INTRODUCTION

Linear Temporal logic (LTL) is a useful language to express complex temporal properties of dynamical systems. By combining a set of propositions and a set of temporal and logical operators, the required task that the system needs to achieve is formulated as a single (temporal logic) formula. LTL provides a general framework to analyze complex tasks in dynamical systems that go beyond the classical control tasks such as convergence, stability, safety, etc; see, e.g., [7, 15, 28, 31].

HSCC '20, April 22–24, 2020, Sydney, NSW, Australia

ACM ISBN 978-1-4503-7018-9/20/04…$15.00
https://doi.org/10.1145/3365365.3382223

LTL was introduced for the verification of computer programs [23]. LTL provides a unified approach to specify and certify behaviors of programs, in particular, invariance and eventuality. In recent years, LTL has been introduced for dynamical systems with various applications in modeling, analysis, design, and control of systems. In [29], the proposed approach employs LTL for motion and task planning of multi-agent systems. Assigned tasks including safety constraints are formulated as LTL formulas and, in their setting, such formulas are verified in real-time so that each agent avoids all obstacles while performing their tasks. In [3], the authors formulate a desired property of a physical plant by using co-safe LTL (sc-LTL), which is a fragment of LTL, and propose a hybrid barrier certificate to verify the satisfaction of sc-LTL specifications. Furthermore, extensions based on LTL have appeared in the literature, such as metric temporal logic (MTL) [14, 26], signal temporal logic (STL) [25], and alternating-time temporal logic (ATL*) [1].

A widely used approach to ensure specifications for dynamical systems consists in constructing a transition system that terminates only when the solution (or trajectory) of the dynamical system satisfies the required specification; see, e.g., [11, 13, 20]. This approach is typical in model checking and software verification methods [4, 10]. It is to be noted that such an approach works well on finite horizon specifications; namely, when the formula needs to be verified within a bounded amount of time. However, this approach does not provide any guarantees when the formula is satisfied at unknown large times. As an example, we can consider temporal logic specifications (formulas) involving the until operator. Such formulas may require arbitrarily long time to be certified. In fact, as pointed out in [22], model-checking-based approaches for certifying formulas using the until operator may require exponential time.

The until operator is one of the basic (yet very powerful) operators in LTL language. In particular, the until operator has *strong* and *weak* versions, named as strong until ($\mathcal{U}_s$) and weak until ($\mathcal{U}_w$); see, e.g., [5]. For example, given two propositions p and q, the satisfaction of the formula $p\,\mathcal{U}_s q$ implies that p is true until q happens to be true, and q must become true eventually. For the weak version, the satisfaction of the formula $p\,\mathcal{U}_w q$ implies that p is true until q happens to be true; however, q is not required to become true if p is true forever. Verifying formulas involving (strong) until operators suggests that one has to show that a given proposition needs to remain satisfied until another proposition becomes satisfied. A simple but concrete application where the until operator is useful concerns autonomous navigation problems in constrained environments [6, 30]. In such applications, mobile vehicles typically need to navigate their environment without colliding with obstacles and following a particular sequence of tasks. For instance, consider the

situation where the vehicle needs to exit a room only via its exit door while avoiding an obstacle in the center of the room. In such setting, the vehicle needs to remain in the room without touching the obstacle until reaching the exit door. Such a temporal behavior can be expressed in terms of an LTL formula involving the until operator.

In this paper, the required dynamical behavior for the solutions to a hybrid system to satisfy temporal logic formulas involving the until operator are presented. For this purpose, we employ two properties: 1) conditional invariance, namely, the property that the solutions to the system remain in a set if they start from a (likely different) set; and 2) eventual conditional invariance, which consists of the solutions reaching a set in finite time when they start from a (likely different) set. These properties are used to formulate sufficient conditions that use minimal information about solutions, yet guarantee the satisfaction of temporal logic formulas involving until operators. For the weak until operator, we present sufficient conditions using barrier functions tailored to conditional invariance for hybrid systems. These conditions use those in [19]. Furthermore, we propose original sufficient conditions to certify eventual conditional invariance for hybrid systems. Those conditions extend the ones proposed in [16] for continuous-time systems. Moreover, they are shown to be useful to formulate sufficient conditions that verify formulas involving the strong until operator.

The remainder of this paper is organized as follows. Hybrid systems, LTL for hybrid systems, and invariance notions are introduced in Section 2. The characterizations of until operators using invariance properties are presented in Section 3.1. The sufficient conditions to guarantee invariance notions for hybrid systems and the satisfaction of LTL formulas involving until operators for hybrid systems are presented in Section 3.2 and Section 3.3, respectively. Academic examples are provided to illustrate the results.

Notation. Let $\mathbb{R}_{\geq 0} := [0, \infty)$ and $\mathbb{N} := \{0, 1, \ldots, \infty\}$. For x, $y \in \mathbb{R}^n$, $x^\top$ denotes the transpose of x, $|x|$ the Euclidean norm of x, $|x|_K := \inf_{y \in K} |x - y|$ defines the distance between x and the nonempty set K, and $\langle x, y \rangle = x^\top y$ denotes the inner product between x and y. For a set $K \subset \mathbb{R}^n$, we use $\text{int}(K)$ to denote its interior, ∂K to denote its boundary, $\overline{K}$ to denote its closure, and $U(K)$ to denote any open neighborhood of K. For a set $O \subset \mathbb{R}^n$, $K \setminus O$ denotes the subset of elements of K that are not in O. By C^1, we denote the set of continuously differentiable functions. Finally, $F : \mathbb{R}^m \rightrightarrows \mathbb{R}^n$ denotes a set-valued map associating each element $x \in \mathbb{R}^m$ to a subset $F(x) \subset \mathbb{R}^n$.

2 PRELIMINARIES

2.1 Hybrid Systems

Following the modeling framework proposed in [8], we consider hybrid systems modeled by general hybrid inclusions of the form

$$\mathcal{H} : \begin{cases} x \in C & \dot{x} \in F(x) \\ x \in D & x^+ \in G(x), \end{cases} \tag{1}$$

with the state variable $x \in \mathbb{R}^n$, the flow set $C \subset \mathbb{R}^n$, the jump set $D \subset \mathbb{R}^n$, and the flow and jump maps, respectively, $F : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$ and $G : \mathbb{R}^n \rightrightarrows \mathbb{R}^n$.

A hybrid arc ϕ is defined on a hybrid time domain denoted $\text{dom}\, \phi \subset \mathbb{R}_{\geq 0} \times \mathbb{N}$. The hybrid arc ϕ is parameterized by an ordinary time variable $t \in \mathbb{R}_{\geq 0}$ and a discrete jump variable $j \in \mathbb{N}$. A hybrid time domain $\text{dom}\, \phi$ is such that for each $(T, J) \in \text{dom}\, \phi$, $\text{dom}\, \phi \cap ([0, T] \times \{0, 1, \ldots, J\}) = \cup_{j=0}^{J-1} \left([t_j, t_{j+1}] \times \{j\}\right)$ for a sequence $\{t_j\}_{j=0}^{J+1}$, such that $t_{j+1} \geq t_j$ and $t_0 = 0$. Note that the structure of a hybrid time domain $\text{dom}\, \phi$ is such that, given $(t, j), (t', j') \in \text{dom}\, \phi$, $t + j \leq t' + j'$ if $t \leq t'$ and $j \leq j'$.

Definition 2.1 (Concept of solutions to $\mathcal{H}$). *A hybrid arc $\phi : \text{dom}\, \phi \to \mathbb{R}^n$ is a* solution *to $\mathcal{H}$ if*

(S0) $\phi(0, 0) \in \overline{C} \cup D$;

(S1) for all $j \in \mathbb{N}$ such that $I^j := \{t : (t, j) \in \text{dom}\, \phi\}$ has nonempty interior, $t \mapsto \phi(t, j)$ is absolutely continuous and

$$\begin{aligned} &\phi(t, j) \in C && \text{for all } t \in \text{int}\,(I^j), \\ &\dot{\phi}(t, j) \in F(\phi(t, j)) && \text{for almost all } t \in I^j; \end{aligned}$$

(S2) for all $(t, j) \in \text{dom}\, \phi$ such that $(t, j + 1) \in \text{dom}\, \phi$,

$$\phi(t, j) \in D, \qquad \phi(t, j + 1) \in G(\phi(t, j)).$$

A solution ϕ to $\mathcal{H}$ is said to be maximal if there is no solution ϕ' to $\mathcal{H}$ such that $\phi(t, j) = \phi'(t, j)$ for all $(t, j) \in \text{dom}\, \phi$ with $\text{dom}\, \phi$ a proper subset of $\text{dom}\, \phi'$. It is said to be trivial if $\text{dom}\, \phi$ contains only one element. Finally, it is said to be complete if its domain is unbounded. The system $\mathcal{H}$ is said to be complete if the domain of each maximal solution is unbounded.

For convenience, we define the range of a solution ϕ to $\mathcal{H}$ as $\text{rge}\, \phi = \{x \in \mathbb{R}^n : x = \phi(t, j),\ (t, j) \in \text{dom}\, \phi\}$. We use $\mathcal{S}_\mathcal{H}(x)$ to denote the set of maximal solutions to $\mathcal{H}$ starting from $x \in \overline{C} \cup D$.

Given a set $K \subset \mathbb{R}^n$, $\mathcal{R}(K)$ denotes the reachable set from K for all hybrid time. Furthermore, for a given closed set $Q \subset \mathbb{R}^n$, the function $\mathcal{T}_Q : \mathcal{S}_\mathcal{H}(\mathbb{R}^n \setminus Q) \mapsto \mathbb{R}_{\geq 0}$ is given by, for each solution ϕ to $\mathcal{H}$ from $\mathbb{R}^n \setminus Q$

$$\mathcal{T}_Q(\phi) := \begin{cases} \infty & \text{if } \mathcal{R}(\phi(0, 0)) \cap Q = \emptyset \\ \min\limits_{\substack{\phi(t,j) \in Q \\ (t,j) \in \text{dom}\, \phi}} t + j & \text{otherwise.} \end{cases} \tag{2}$$

Given a solution ϕ to $\mathcal{H}$ starting from $\mathbb{R}^n \setminus Q$, the function $\mathcal{T}_Q$ provides (when finite) the first hybrid time at which the solution ϕ reaches the set Q. If the solution never reaches Q, the function $\mathcal{T}_Q$ is set to infinity. See [8] for more details about hybrid dynamical systems.

2.2 Linear Temporal Logic and Until Operators

Linear Temporal Logic (LTL) provides a framework to specify and to formulate desired properties for dynamical systems [27]. In this section, we introduce syntax and semantics of LTL.

Definition 2.2 (Atomic Proposition). *An atomic proposition p is a statement on the system state x that, for each x, $p(x)$ is either* `True` *(1 or $\top$) or* `False` *(0 or $\bot$).*

Definition 2.3 (Logical Operators).

- $\neg$ *is the* negation *operator*
- $\vee$ *is the* disjuction *operator*
- $\wedge$ *is the* conjunction *operator*
- $\Rightarrow$ *is the* implication *operator*
- $\Leftrightarrow$ *is the* equivalence *operator*

Definition 2.4 (Temporal Operators).

- $\bigcirc$ *is the* next *operator*
- $\Diamond$ *is the* eventually *operator*
- $\Box$ *is the* always *operator*
- $\mathcal{U}_s$ *is the* strong until *operator*
- $\mathcal{U}_w$ *is the* weak until *operator*

A proposition p is treated as a (single-valued) function of x, that is, as the function $x \mapsto p(x)$. The set of all possible atomic propositions is denoted by $\mathcal{P}$. For simplicity, we consider the case of state-dependent atomic propositions with no inputs. That is, for a given hybrid system $\mathcal{H}$, consider a solution ϕ to $\mathcal{H}$ and $(t,j) \in \operatorname{dom}\phi$. When a proposition p is `True` at (t,j), i.e., $p(\phi(t,j)) = 1$, it is denoted by $(\phi,(t,j)) \vDash p$; whereas if p is `False` at (t,j), it is written as $(\phi,(t,j)) \nvDash p$.

Moreover, an LTL formula is a sentence consisting of atomic propositions and operators of LTL. When an LTL formula f is satisfied by a solution ϕ to a hybrid system $\mathcal{H}$ at $(t,j) \in \operatorname{dom}\phi$, it is denoted by $(\phi,(t,j)) \vDash f$; however, when f is not satisfied by a solution ϕ at (t,j), it is denoted by $(\phi,(t,j)) \nvDash f$.

Let $p, q \in \mathcal{P}$ be two atomic propositions. Given a solution ϕ to $\mathcal{H}$ and $(t,j) \in \operatorname{dom}\phi$, the semantics of LTL is based on a set of basic operators yielding to the following basic formulas:

$$(\phi,(t,j)) \vDash \neg p \;\Leftrightarrow\; (\phi,(t,j)) \nvDash p \tag{3a}$$

$$(\phi,(t,j)) \vDash p \vee q \;\Leftrightarrow\; (\phi,(t,j)) \vDash p \text{ or } (\phi,(t,j)) \vDash q \tag{3b}$$

$$(\phi,(t,j)) \vDash \bigcirc p \;\Leftrightarrow\; (\phi,(t,j+1)) \vDash p \text{ and } (t,j+1) \in \operatorname{dom}\phi \tag{3c}$$

$$(\phi,(t,j)) \vDash p \wedge q \;\Leftrightarrow\; (\phi,(t,j)) \vDash p \text{ and } (\phi,(t,j)) \vDash q \tag{3d}$$

$$(\phi,(t,j)) \vDash \Box p \;\Leftrightarrow\; (\phi,(t',j')) \vDash p \quad \forall\,(t',j') \in \operatorname{dom}\phi,\ t'+j' \geq t+j \tag{3e}$$

$$(\phi,(t,j)) \vDash \Diamond p \;\Leftrightarrow\; \exists (t',j') \in \operatorname{dom}\phi,\ t'+j' \geq t+j \text{ s.t. } (\phi,(t',j')) \vDash p. \tag{3f}$$

In the following, we introduce strong and weak versions of the until operator studied in this paper.

Definition 2.5 (Strong until operator). *Given two atomic propositions $p, q \in \mathcal{P}$, a solution $(t,j) \mapsto \phi(t,j)$ to a hybrid system $\mathcal{H}$ satisfies the formula*

$$f := p\,\mathcal{U}_s\,q \tag{4}$$

at $(t,j) \in \operatorname{dom}\phi$ if there exists $(t',j') \in \operatorname{dom}\phi$ such that $t'+j' \geq t+j$ and $\phi(t',j')$ satisfies q; and $\phi(t'',j'')$ satisfies p for all $t+j \leq (t'',j'') < t'+j'$. In other words,

$$\begin{aligned}(\phi,(t,j)) \vDash p\,\mathcal{U}_s q \;\Leftrightarrow\; &\exists\,(t',j') \in \operatorname{dom}\phi,\ t'+j' \geq t+j \ \text{ s.t.}\\ &(\phi,(t',j')) \vDash q; \text{ and}\\ &\forall\,(t'',j'') \in \operatorname{dom}\phi \ \text{ s.t.}\\ &t+j \leq t''+j'' < t'+j', (\phi,(t'',j'')) \vDash p.\end{aligned}$$

Definition 2.6 (Weak until operator). *Given two atomic propositions $p, q \in \mathcal{P}$, a solution $(t,j) \mapsto \phi(t,j)$ to $\mathcal{H}$ satisfies the formula*

$$f := p\,\mathcal{U}_w\,q \tag{5}$$

at $(t,j) \in \operatorname{dom}\phi$ if

1) *$\phi(t',j')$ satisfies p for all $(t',j') \in \operatorname{dom}\phi$ such that $t'+j' \geq t+j$; or*
2) *there exists $(t',j') \in \operatorname{dom}\phi$ such that $t'+j' \geq t+j$ and $\phi(t',j')$ satisfies q; and $\phi(t'',j'')$ satisfies p for all (t'',j'') such that $t+j \leq t''+j'' < t'+j'$.*

In other words,

$$\begin{aligned}(\phi,(t,j)) \vDash p\,\mathcal{U}_w q \;\Leftrightarrow\; &(\phi,(t',j')) \vDash p\\ &\forall\,(t',j') \in \operatorname{dom}\phi \ \text{ s.t. } t'+j' \geq t+j, \text{ or}\\ &(\phi,(t,j)) \vDash p\,\mathcal{U}_s q.\end{aligned}$$

2.3 Invariance Notions

In this section, we introduce the invariance notions that will play a key role in the proposed sufficient infinitesimal conditions to verify LTL formulas using until operators for hybrid systems.

Definition 2.7 (Forward (pre-)Invariance). *A set K is said to be forward pre-invariant for $\mathcal{H}$ if, for each solution $\phi \in \mathcal{S}_{\mathcal{H}}(K)$, rge $\phi \subset K$. A set K is said to be forward invariant for $\mathcal{H}$ if it is forward pre-invariant for $\mathcal{H}$ and, for every $x \in K$, every solution $\phi \in \mathcal{S}_{\mathcal{H}}(K)$ is complete.*

Definition 2.8 (Conditional Invariance). *A set $K \subset \mathbb{R}^n$ is said to be conditionally invariant with respect to a set $K_o \subset K$ for $\mathcal{H}$ if, for each solution $\phi \in \mathcal{S}_{\mathcal{H}}(K_o)$, $\phi(t,j) \in K$ for all $(t,j) \in \operatorname{dom}\phi$.*

Remark 2.9. *Note that when $K_o = K$, conditional invariance of K with respect to K_o is equivalent to forward pre-invariance of K_o.*

Next, we introduce the definition of safety.

Definition 2.10 (Safety). *A hybrid system $\mathcal{H}$ is said to be safe with respect to $(\mathcal{X}_o, \mathcal{X}_u)$, where $\mathcal{X}_u \subset \mathbb{R}^n$ denotes the unsafe set and $\mathcal{X}_o \subset \mathbb{R}^n \setminus \mathcal{X}_u$ denotes the initial set, if each solution ϕ to $\mathcal{H}$ from $\mathcal{X}_o$ satisfies rge $\phi \subset \mathbb{R}^n \setminus \mathcal{X}_u$.*

Remark 2.11. *Conditional invariance of K with respect to K_o is equivalent to safety with respect to $(K_o, \mathcal{X}_u)$, where $\mathcal{X}_u := \mathbb{R}^n \setminus K$ defines the region of the state space that the solutions to $\mathcal{H}$ must avoid when starting from the set of initial conditions K_o [17].*

Next, inspired by the ideas in [16] for continuous-time systems with maximal solutions that are complete, we introduce the following eventual conditional invariance notion. This notion plays an important role when formulating a characterization of the strong until operator via conditional invariance.

Definition 2.12 (Eventual Conditional Invariance). *Given two sets $K_o, K \subset \mathbb{R}^n$, the set K is said to be* eventually conditionally invariant *with respect to K_o for $\mathcal{H}$ if every maximal solution $\phi \in \mathcal{S}_{\mathcal{H}}(K_o)$ is such that $\mathcal{T}_K(\phi) < \infty$ and*

- *$\phi(t,j) \in K$ for every $(t,j) \in \operatorname{dom}\phi$ such that $t+j \geq \mathcal{T}_K(\phi)$.*

Since $\mathcal{H}$ can have maximal solutions that are not complete, we introduce the following pre-eventual conditional invariance notion which, compared to Definition 2.12, requires that only the complete solutions to $\mathcal{H}$ must reach the set K.

Definition 2.13 (pre-Eventual Conditional Invariance). *Given two sets $K_o, K \subset \mathbb{R}^n$, K is said to be* pre-eventually conditionally invariant *with respect to K_o for $\mathcal{H}$ if every complete solution $\phi \in \mathcal{S}_{\mathcal{H}}(K_o)$ is such that $\mathcal{T}_K(\phi) < \infty$ and*

- *$\phi(t,j) \in K$ for every $(t,j) \in \operatorname{dom}\phi$ such that $t+j \geq \mathcal{T}_K(\phi)$.*

3 MAIN RESULTS

In this section, as a first step, we characterize the until operators using the previously mentioned invariance notions. Then, we propose infinitesimal characterizations of the considered invariance notions. The latter will allow us to provide sufficient infinitesimal conditions to verify LTL formulas with until operators for hybrid systems.

Our results are valid for the general class of hybrid systems $\mathcal{H}$ satisfying the following mild assumption:

(SA) The system $\mathcal{H}$ is such that F is outer semicontinuous, nonempty, and locally bounded with convex images on C. Furthermore, the jump map G is nonempty on D.

We notice that the hybrid basic conditions in [8, Chapter 6] further require the sets C and D to be closed and the jump map G to be locally bounded. Our conditions in (SA) are less restrictive than the hybrid basic conditions.

3.1 Characterization of Until Operators Using Invariance Notions

To propose necessary and sufficient conditions for the satisfaction of the LTL formulas in (4) and (5) using set-invariance notions, we introduce the following sets where the atomic propositions p and q are satisfied, respectively:

$$P := \{x \in \mathbb{R}^n : p(x) = 1\} \text{ and } Q := \{x \in \mathbb{R}^n : q(x) = 1\}. \quad (6)$$

With the sets P and Q as in (6), when a solution ϕ to $\mathcal{H}$ satisfies $p\,\mathcal{U}_w q$ at $(t, j) = (0, 0)$ with $(\phi, (0, 0)) \models p \vee q$, we have the following cases:

1) ϕ starts and remains in the set P for all hybrid time; or
2) ϕ starts and remains in the set P up to when ϕ reaches Q. After ϕ reaches Q, ϕ may leave $P \cup Q$ or stay in $P \cup Q$; or
3) ϕ starts from the set Q.

Remarkably, these properties can be assured using the conditional invariance notion in Definition 2.8. In fact, notice that based on items 1) - 3), the solution needs to either remain in P or remain in $P \cup Q$ for some time. Such a property coincides with conditional invariance of $P \cup Q$ with respect to $P \setminus Q$ for the following auxiliary system $\mathcal{H}_m$: given a closed set Q and a hybrid system $\mathcal{H} = (C, F, D, G)$, we consider the system $\mathcal{H}_m = (C_m, F_m, D_m, G_m)$ given by

$$\begin{aligned} &F_m(x) := F(x) && \forall x \in C_m := C \setminus Q \\ &G_m(x) := \begin{cases} x & \text{if } x \in Q \\ G(x) & \text{otherwise} \end{cases} && \forall x \in D_m := D \cup Q. \end{aligned} \quad (7)$$

The intuition behind the construction of the system $\mathcal{H}_m$ is as follows. The system $\mathcal{H}_m$ is used to characterize the behavior of the system $\mathcal{H}$ outside the set Q. Indeed, the solutions to $\mathcal{H}$ are the solutions to $\mathcal{H}_m$ (and vice versa) up to when they reach (if they do) the set Q. Furthermore, the solutions to $\mathcal{H}_m$ starting from an initial condition in Q are purely discrete solutions that remain at the initial condition.

Example 3.1 (Timer). *Consider a hybrid system $\mathcal{H} = (C, F, D, G)$ modeling a constantly evolving timer with the state $x \in \mathbb{R}$ and*

$$\begin{aligned} &F(x) := 1 && \forall x \in C := [0, 1], \\ &G(x) := 0 && \forall x \in D := \{x \in \mathbb{R} : x = 1\}. \end{aligned}$$

Define two atomic propositions p and q such that

$$p(x) := \begin{cases} 1 & \text{if } x \in [1/2, 1) \\ 0 & \text{otherwise} \end{cases}$$

and

$$q(x) := \begin{cases} 1 & \text{if } x = 1 \\ 0 & \text{otherwise.} \end{cases}$$

The sets P and Q in (6) and the system $\mathcal{H}_m$ in (7) are given by $Q = D$, $P = [1/2, 1)$, and

$$\begin{aligned} &F_m(x) := 1 && \forall x \in C_m := [0, 1), \\ &G_m(x) := x && \forall x \in D_m := D = Q. \end{aligned}$$

We notice that each solution to $\mathcal{H}_m$ from P flows in P and reaches the set Q. Once this solution reaches Q, it jumps according to the jump map $G_m(x) = x$ for all $x \in Q = D$ and cannot flow. Hence, the solutions to $\mathcal{H}_m$ starting from $P \setminus Q$ never leave the set $P \cup Q$, which concludes that the set $Q \cup P$ is conditionally invariant with respect to $P \setminus Q$ for $\mathcal{H}_m$. However, conditional invariance of $Q \cup P$ with respect to $P \setminus Q$ does not hold for system $\mathcal{H}$ since once a solution to $\mathcal{H}$ reaches Q, it jumps outside $P \cup Q$. Furthermore, we also notice that the formula $f = p\,\mathcal{U}_w q$ is satisfied for every maximal solution ϕ to $\mathcal{H}$ at $(t, j) = (0, 0)$ with $(\phi, (0, 0)) \models p \vee q$ since the solutions to $\mathcal{H}$ starting from $P \setminus Q$ remain in P until reaching the jump set $D = Q$.

Theorem 3.2 (Weak Until vs Conditional Invariance). *Consider a hybrid system $\mathcal{H} = (C, F, D, G)$. Given two atomic propositions p and q, let the sets P and Q be given as in (6) and let the system $\mathcal{H}_m$ be as in (7). The formula $f = p\,\mathcal{U}_w q$ is satisfied for every maximal solution ϕ to $\mathcal{H}$ at $(t, j) = (0, 0)$ with $(\phi, (0, 0)) \models p \vee q$ if and only if $P \cup Q$ is conditionally invariant with respect to $P \setminus Q$ for $\mathcal{H}_m$.*

Sketch of Proof. ($\Rightarrow$) Suppose that $f = p\,\mathcal{U}_w q$ is satisfied at $(t, j) = (0, 0)$ for every maximal solution ϕ to $\mathcal{H}$ such that $(\phi, (0, 0)) \models p \vee q$. Then, we need to show that each solution ψ to $\mathcal{H}_m$ starting from $P \setminus Q$ stays in $P \cup Q$ for all $(t, j) \in \operatorname{dom} \psi$. Recall that $\mathcal{T}_Q(\cdot)$ is introduced in (2). For every maximal solution ψ to $\mathcal{H}_m$ with $\psi(0, 0) \in P \setminus Q$, we consider a solution ϕ to $\mathcal{H}$ such that $\phi(0, 0) = \psi(0, 0)$ and

$$\psi(t, j) = \phi(t, j) \quad \forall (t, j) \in \operatorname{dom} \psi \text{ s.t. } t + j \leq \mathcal{T}_Q(\psi) = \mathcal{T}_Q(\phi). \quad (8)$$

- By construction of $\mathcal{H}_m$, both systems $\mathcal{H}$ and $\mathcal{H}_m$ have the same data in $(C \cup D) \setminus Q$. Hence, a solution ϕ satisfying (8) with respect to ψ always exists.
- By definition of the $\mathcal{U}_w$ operator, we conclude that $\phi(t, j)$ satisfies p or q for all $(t, j) \in \operatorname{dom} \phi$ such that $t + j = \mathcal{T}_Q(\phi)$, which implies that $\phi(t, j) \in P \cup Q$ for all $(t, j) \in \operatorname{dom} \phi$ such that $t + j \leq \mathcal{T}_Q(\phi)$.

Furthermore, one of the following must hold:

- When $\mathcal{T}_Q(\phi) < \infty$, the solution ψ to $\mathcal{H}_m$ remains equal to its value when it reaches the set Q for the first time; and thus, we conclude that $\psi(t, j) \in P \cup Q$ for all $(t, j) \in \operatorname{dom} \psi$.
- When $\mathcal{T}_Q(\phi) = \infty$, the solution ϕ satisfies $\phi(t, j) \in P \setminus Q$ for all $(t, j) \in \operatorname{dom} \phi$ by definition of the $\mathcal{U}_w$ operator. Furthermore, since both systems $\mathcal{H}$ and $\mathcal{H}_m$ have the same data in $(C \cup D) \setminus Q$, it follows that $\phi(t, j) = \psi(t, j) \in P \setminus Q$ for all $(t, j) \in \operatorname{dom} \phi = \operatorname{dom} \psi$.

In either case, each solution ψ to $\mathcal{H}_m$ starting from $P \setminus Q$ stays in $P \cup Q$ for all $(t, j) \in \operatorname{dom} \psi$. Hence, $P \cup Q$ is conditionally invariant with respect to $P \setminus Q$ for $\mathcal{H}_m$.

($\Leftarrow$) Now, suppose that $P \cup Q$ is conditionally invariant with respect to $P \setminus Q$ for $\mathcal{H}_m$. We show that, for each solution ϕ to $\mathcal{H}$ such that $\phi(0,0) \in P \setminus Q$, ϕ stays in $P \cup Q$ for all $(t, j) \in \operatorname{dom} \phi$ such that $t + j \leq \mathcal{T}_Q(\phi)$.

- Let ψ be a maximal solution to $\mathcal{H}_m$ such that $\psi(t, j) = \phi(t, j)$ for all $(t, j) \in \operatorname{dom} \phi$ such that $t + j \leq \mathcal{T}_Q(\phi)$; the solution ψ to $\mathcal{H}_m$ always exists since the systems $\mathcal{H}$ and $\mathcal{H}_m$ share the same data outside the set Q.
- Since $P \cup Q$ is conditionally invariant with respect to $P \setminus Q$ for $\mathcal{H}_m$, we conclude that $\psi(t, j) \in P \cup Q$ for all $(t, j) \in \operatorname{dom} \psi$. Therefore, $\phi(t, j) \in P \cup Q$ for all $(t, j) \in \operatorname{dom} \phi$ such that $t + j \leq \mathcal{T}_Q(\phi)$. □

The bouncing ball example in [8, Example 1.1] illustrates Theorem 3.2.

Example 3.3 (Bouncing Ball). *Consider a hybrid system $\mathcal{H} = (C, F, D, G)$ modeling a ball bouncing vertically on the ground, with the state $x = (x_1, x_2) \in \mathbb{R}^2$ and the data*

$$F(x) := \begin{bmatrix} x_2 \\ -\gamma \end{bmatrix} \qquad \forall x \in C := \{x \in \mathbb{R}^2 : x_1 \geq 0\}$$

$$G(x) := \begin{bmatrix} 0 \\ -\lambda x_2 \end{bmatrix} \qquad \forall x \in D := \{x \in \mathbb{R}^2 : x_1 = 0, x_2 \leq 0\},$$

where x_1 denotes the height above the surface and x_2 is the vertical velocity. The parameter $\gamma > 0$ is the gravity coefficient and $\lambda \in (0, 1)$ is the restitution coefficient. Let $\varepsilon > 0$ and define atomic propositions p and q such that

$$p(x) := \begin{cases} 1 & \text{if } x_1 \in [0, \varepsilon] \text{ and } x_2 \leq 0 \\ 0 & \text{otherwise,} \end{cases}$$

and

$$q(x) := \begin{cases} 1 & \text{if } x_1 \geq 0 \text{ and } x_2 > 0 \\ 0 & \text{otherwise.} \end{cases}$$

The sets P and Q in (6) and the system $\mathcal{H}_m$ in (7) are given by $P = [0, \varepsilon] \times \mathbb{R}_{\geq 0}$, $Q = \mathbb{R}_{\geq 0} \times \mathbb{R}_{>0}$, and

$$F_m(x) = F(x) \qquad \forall x \in C_m = \mathbb{R}_{\geq 0} \times \mathbb{R}_{\leq 0}$$

$$G_m(x) = \begin{cases} x & \text{if } x \in \mathbb{R}_{\geq 0} \times \mathbb{R}_{>0} \\ G(x) & \text{if } x \in \{0\} \times \mathbb{R}_{\leq 0} \end{cases} \qquad \forall x \in D_m,$$

where $D_m = (\{0\} \times \mathbb{R}_{\leq 0}) \cup (\mathbb{R}_{\geq 0} \times \mathbb{R}_{>0})$.

We notice that each solution to $\mathcal{H}_m$ from $P \setminus \{0\}$ flows in P and reaches the set Q after jumping from the set $\{0\} \times \mathbb{R}_{\leq 0} \subset D_m$. However, the solution starting from the origin is a constant discrete solution that remains in the set P and never reaches Q. Once the solutions reach Q, they jump according to the jump map $G_m(x) = x$ for all $x \in Q$. Hence, the solutions to $\mathcal{H}_m$ starting from $P \setminus Q = P$ never leave the set $P \cup Q$, which concludes that the set $Q \cup P$ is conditionally invariant with respect to $P \setminus Q$ for $\mathcal{H}_m$. Hence, using Proposition 3.8, we conclude that the formula $f = p\,\mathcal{U}_w q$ is satisfied for every maximal solution ϕ to $\mathcal{H}$ at $(t, j) = (0, 0)$ with $(\phi, (0, 0)) \vDash p \vee q$.

Next, we consider the definition of the $\mathcal{U}_s$ operator. With the same sets P and Q in (6), to assure that a solution ϕ to $\mathcal{H}$ satisfies $p\,\mathcal{U}_s q$ at $(t, j) = (0, 0)$ with $(\phi, (0, 0)) \vDash p \vee q$,

1) ϕ starts and remains in the set P until reaching the set Q at $\mathcal{T}_Q(\phi) < \infty$; or
2) ϕ starts from the set Q.

Note that $p\,\mathcal{U}_w q$ is less restrictive than $p\,\mathcal{U}_s q$. When $p\,\mathcal{U}_w q$ is satisfied for all solutions ϕ to $\mathcal{H}$ with $(\phi, (0, 0)) \vDash p \vee q$, solutions with $(\phi, (0, 0)) \vDash p$ may satisfy p for all future hybrid time. Due to this, compared to Theorem 3.2, the following result for the satisfaction of $p\,\mathcal{U}_s q$ requires additional conditions to guarantee that there exists $(t, j) \in \operatorname{dom} \phi$ such that $\phi(t, j)$ satisfies q. Such a property consists of Q being eventually conditionally invariant with respect to the set $P \setminus Q$ for $\mathcal{H}_m$ in (7).

Theorem 3.4 (Strong Until vs Weak Until + Eventual Conditional Invariance). *Consider a hybrid system $\mathcal{H} = (C, F, D, G)$. Given two atomic propositions p and q, let the sets P and Q be given in (6) and let the system $\mathcal{H}_m$ be as in (7). The formula $f = p\,\mathcal{U}_s q$ is satisfied for every solution ϕ to $\mathcal{H}$ at $(t, j) = (0, 0)$ with $(\phi, (0, 0)) \vDash p \vee q$ if and only if*

1) *the formula $p\,\mathcal{U}_w q$ is satisfied for every solution ϕ to $\mathcal{H}$ at $(t, j) = (0, 0)$ with $(\phi, (0, 0)) \vDash p \vee q$ (see Theorem 3.2); and*
2) *The set Q is eventually conditionally invariant with respect to $P \setminus Q$ for $\mathcal{H}_m$.*

Sketch of Proof. ($\Rightarrow$) Suppose that $f = p\,\mathcal{U}_s q$ is satisfied at $(t, j) = (0, 0)$ for every solution to $\mathcal{H}$ such that $(\phi, (0, 0)) \vDash p \vee q$.

- By definition, the aforementioned fact implies that $f = p\,\mathcal{U}_w q$ is satisfied at $(t, j) = (0, 0)$ for every solution to $\mathcal{H}$ such that $(\phi, (0, 0)) \vDash p \vee q$.
- We show that the set Q is eventually conditionally invariant with respect to $P \setminus Q$ for $\mathcal{H}_m$. Indeed, for every solution ψ to $\mathcal{H}_m$ with $\psi(0, 0) \in P \setminus Q$, we consider a solution ϕ to $\mathcal{H}$ such that $\phi(0, 0) = \psi(0, 0)$ and $\psi(t, j) = \phi(t, j)$ for all $(t, j) \in \operatorname{dom} \psi$ such that $t + j \leq \mathcal{T}_Q(\psi) = \mathcal{T}_Q(\phi)$. In fact, such a solution ϕ always exists since both $\mathcal{H}$ and $\mathcal{H}_m$ have the same data outside the set Q. By definition of the $\mathcal{U}_s$ operator, we conclude that $\phi(t, j) \in P \cup Q$ for all $(t, j) \in \operatorname{dom} \phi$ such that $t + j \leq \mathcal{T}_Q(\phi)$ and that $\mathcal{T}_Q(\phi) < \infty$. Hence, $\psi(t, j) \in P \cup Q$ for all $(t, j) \in \operatorname{dom} \psi$ such that $t + j \leq \mathcal{T}_Q(\psi)$ and $\mathcal{T}_Q(\psi) < \infty$.

($\Leftarrow$) Suppose that the formula $p\,\mathcal{U}_w q$ is satisfied for every solution ϕ to $\mathcal{H}$ at $(t, j) = (0, 0)$ with $(\phi, (0, 0)) \vDash p \vee q$. This fact implies that, using Theorem 3.2, the solutions to $\mathcal{H}_m$ starting from $P \setminus Q$ remain in the set $P \cup Q$.

- When additionally Q is eventually conditionally invariant with respect to $P \setminus Q$ for $\mathcal{H}_m$, we conclude that the solutions to $\mathcal{H}_m$ starting from $P \setminus Q$ remain in the set $P \cup Q$ and reach the set Q.
- We show that, for each solution ϕ to $\mathcal{H}$ such that $\phi(0, 0) \in P \setminus Q$, ϕ stays in $P \cup Q$ for all $(t, j) \in \operatorname{dom} \phi$ such that $t + j \leq \mathcal{T}_Q(\phi)$, and $\mathcal{T}_Q(\phi) < \infty$. Let ϕ be a solution to $\mathcal{H}$. Since both $\mathcal{H}$ and $\mathcal{H}_m$ share the same data outside the set Q, there always exists a solution ψ to $\mathcal{H}_m$ such that $\psi(t, j) = \phi(t, j)$ for all $(t, j) \in \operatorname{dom} \phi$ provided that $t + j \leq \mathcal{T}_Q(\phi) = \mathcal{T}_Q(\psi)$. Since we already know that $\psi(t, j) \in P \cup Q$ for all $(t, j) \in \operatorname{dom} \psi$, we conclude that $\phi(t, j) \in P \cup Q$ for all $(t, j) \in \operatorname{dom} \phi$ provided that $t + j \leq \mathcal{T}_Q(\phi)$. □

The bouncing ball example in Example 3.3 is used to illustrate Theorem 3.4.

Example 3.5 (Bouncing ball). *Consider the system $\mathcal{H} = (C, F, D, G)$ in Example 3.3 while replacing the atomic proposition p therein by $\tilde{p}$ such that*

$$\tilde{p}(x) := \begin{cases} p(x) & \text{if } x \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

Hence, the set $\widetilde{P}$, according to (6), is given by $\widetilde{P} = P \setminus \{0\}$. We already showed, in Example 3.3, that the formula $f = p\,\mathcal{U}_w q$ is satisfied for every maximal solution ϕ to $\mathcal{H}$ at $(t, j) = (0, 0)$ with $(\phi, (0, 0)) \models p \vee q$. Furthermore, since the solutions not starting from the origin will never reach the origin, we conclude that $f = \tilde{p}\,\mathcal{U}_w q$ is also satisfied for every maximal solution ϕ to $\mathcal{H}$ at $(t, j) = (0, 0)$ with $(\phi, (0, 0)) \models \tilde{p} \vee q$. Furthermore, we also showed that all the solutions to $\mathcal{H}_m$ starting from $\widetilde{P} \setminus Q = \widetilde{P}$ reach Q, which concludes that the set Q is eventually conditionally invariant with respect to $\widetilde{P} \setminus Q$ for $\mathcal{H}_m$. Hence, using Theorem 3.4, we conclude that $f = \tilde{p}\,\mathcal{U}_s q$ is satisfied for every maximal solution ϕ to $\mathcal{H}$ at $(t, j) = (0, 0)$ with $(\phi, (0, 0)) \models \tilde{p} \vee q$.

Example 3.6 (Thermostat). *Consider a hybrid system $\mathcal{H} = (C, F, D, G)$ modeling a thermostat system, with the state $x := (h, z) \in \mathbb{R}^2$ and*

$$\begin{aligned} F(x) &:= \begin{bmatrix} 0 & -z + z_0 + z_\triangle h \end{bmatrix}^\top && \forall x \in C := C_0 \cup C_1 \\ G(x) &:= \begin{bmatrix} 1 - h & z \end{bmatrix}^\top && \forall x \in D := D_0 \cup D_1, \end{aligned}$$

where

$$C_0 := \{x \in \mathcal{X} : h = 0, z \geq z_{\min}\},\ C_1 := \{x \in \mathcal{X} : h = 1, z \leq z_{\max}\},$$
$$D_0 := \{x \in \mathcal{X} : h = 0, z \leq z_{\min}\},\ D_1 := \{x \in \mathcal{X} : h = 1, z \geq z_{\max}\}.$$

The variable h denotes the state of the heater, i.e., $h = 1$ implies the heater is on and $h = 0$ implies the heater is off. the variable z is the room temperature, z_0 denotes the room temperature when the heater is off, and $z_\triangle$ denotes the capacity of the heater to raise the temperature such that

$$z_0 < z_{\min} < z_{\max} < z_0 + z_\triangle. \tag{9}$$

Define two atomic propositions p and q such that

$$p(x) := \begin{cases} 1 & \text{if } x \in \{1\} \times (-\infty, z_{\max}] \\ 0 & \text{otherwise} \end{cases} \tag{10}$$

and

$$q(x) := \begin{cases} 1 & \text{if } x = \{0\} \times [z_{\max}, +\infty) \\ 0 & \text{otherwise.} \end{cases} \tag{11}$$

The sets P and Q in (6) and the system $\mathcal{H}_m$ in (7) are given by $P = \{1\} \times (-\infty, z_{\max}]$, $Q = \{0\} \times [z_{\max}, +\infty)$, and

$$\begin{aligned} F_m(x) &= F(x) && \forall x \in C_m = C \setminus Q \\ G_m(x) &= \begin{cases} x & \text{if } x = \begin{bmatrix} 0 & [z_{\max}, +\infty) \end{bmatrix}^\top \\ G(x) & \text{if } x \in D \end{cases} && \forall x \in D_m. \end{aligned}$$

We notice that each solution to $\mathcal{H}_m$ from $P \setminus Q$ flows in P and reaches the set Q after jumping from $\{\begin{bmatrix} 0 & z_{\max} \end{bmatrix}^\top\} \subset D_m$. Once the solutions reach Q, they jump according to the jump map $G_m(x) = x$ for all $x \in Q$ and they cannot flow. Hence, the solutions to $\mathcal{H}_m$ starting from $P \setminus Q = P$ never leave the set $P \cup Q$, which concludes that the set $Q \cup P$ is conditionally invariant with respect to $P \setminus Q$ and Q is eventually conditionally invariant with respect to $P \setminus Q$ for $\mathcal{H}_m$. Hence, using Theorems 3.2 and 3.4, we conclude that the formula $f = p\,\mathcal{U}_s q$ is satisfied for every maximal solution ϕ to $\mathcal{H}$ at $(t, j) = (0, 0)$ with $(\phi, (0, 0)) \models p \vee q$.

3.2 Sufficient Conditions for Forward Invariance Notions

In this section, we present sufficient conditions to guarantee the different invariance notions in Section 2.3. First, we recall the sufficient conditions for invariance notions using a barrier function in [18, 19] for hybrid systems. Then, we propose new sufficient conditions for eventual conditional invariance for hybrid systems inspired from [16] in the setting of continuous-time systems. Below, the concept of the tangent cone[1] to a set is used; see [8, Definition 5.12]. The tangent cone at a point $x \in \mathbb{R}^n$ of a set $C \subset \mathbb{R}^n$ given by

$$T_C(x) := \left\{ v \in \mathbb{R}^n : \liminf_{h \to 0^+} \frac{|x + hv|_C}{h} = 0 \right\}. \tag{12}$$

We also recall the equivalence [2, Page 122]

$$\begin{aligned} &v \in T_C(x) \Leftrightarrow \\ &\quad \exists \{h_i\}_{i \in \mathbb{N}} \to 0^+ \text{ and } \{v_i\}_{i \in \mathbb{N}} \to v : x + h_i v_i \in C\ \forall i \in \mathbb{N}. \end{aligned} \tag{13}$$

Furthermore, for the given sets $\mathcal{X}_o, \mathcal{X}_u \subset \mathbb{R}^n$ with $\mathcal{X}_o \cap \mathcal{X}_u = \emptyset$, we recall from [18] the notion of a barrier function candidate with respect to $(\mathcal{X}_o, \mathcal{X}_u)$ for $\mathcal{H}$.

Definition 3.7 (Barrier Function Candidate). *Consider $\mathcal{H} = (C, F, D, G)$. Given sets $\mathcal{X}_o$ and $\mathcal{X}_u \subset \mathbb{R}^n$ with $\mathcal{X}_o \cap \mathcal{X}_u = \emptyset$, a function $B : \mathbb{R}^n \to \mathbb{R}$ is said to be a barrier function candidate with respect to $(\mathcal{X}_o, \mathcal{X}_u)$ for $\mathcal{H}$ if*

$$\begin{cases} B(x) \leq 0 & \forall x \in \mathcal{X}_o \\ B(x) > 0 & \forall x \in (C \cup D) \cap \mathcal{X}_u. \end{cases} \tag{14}$$

In the following, we recall a result on safety for hybrid systems [18, Theorem 3.2] to derive sufficient conditions for conditional invariance for hybrid systems. Given two sets $\mathcal{X}_o, \mathcal{X}_u$, the conditions given below provide sufficient conditions to verify that $\mathbb{R}^n \setminus \mathcal{X}_u$ is conditionally invariant with respect to $\mathcal{X}_o$ for $\mathcal{H}$.

Proposition 3.8 (Conditional Invariance). *Consider a hybrid system $\mathcal{H} = (C, F, D, G)$ satisfying (SA). Let two sets $\mathcal{X}_o$ and $\mathcal{X}_u$ such that $\mathcal{X}_o$, $\mathbb{R}^n \setminus \mathcal{X}_u \subset C \cup D$. The set $\mathbb{R}^n \setminus \mathcal{X}_u$ is conditionally invariant with respect to $\mathcal{X}_o$ for $\mathcal{H}$ if there exists a $\mathcal{C}^1$ barrier function candidate B with respect to $(\mathcal{X}_o, \mathcal{X}_u)$ for $\mathcal{H}$ as in (14) such that $K := \{x \in C \cup D : B(x) \leq 0\}$ is closed and the following hold:*

1) *$\langle \nabla B(x), \eta \rangle \leq 0$ for all $x \in (U(\partial K) \setminus K) \cap C$ and all $\eta \in F(x) \cap T_C(x)$; and*
2) *$B(\eta) \leq 0$ for all $x \in D \cap K$ and all $\eta \in G(x)$; and*
3) *$G(D \cap K) \subset C \cup D$.*

According to Remark 2.9, when $\mathcal{X}_o = \mathbb{R}^n \setminus \mathcal{X}_u$, conditional invariance of $\mathbb{R}^n \setminus \mathcal{X}_u$ with respect to $\mathcal{X}_o$ reduces to forward pre-invariance of the set $K := \mathcal{X}_o$. In the next statement, we recall from [19, Theorem 1 and Proposition 2] sufficient conditions for forward invariance using barrier functions.

Proposition 3.9 (Forward Invariance). *Consider a hybrid system $\mathcal{H} = (C, F, D, G)$ satisfying (SA). Let K be a closed set such that $K \subset C \cup D$. The set K is forward pre-invariant for $\mathcal{H}$ if there exists a $\mathcal{C}^1$ barrier function candidate B with respect to $(K, \mathbb{R}^n \setminus K)$ for $\mathcal{H}$ as in (14) such that the following hold:*

[1] This tangent cone is also known as the contingent cone, or the Bouligand tangent cone.

1) $\langle \nabla B(x), \eta \rangle \leq 0$ *for all* $x \in C \cap (U(\partial K) \setminus K)$ *and all* $\eta \in F(x) \cap T_C(x)$.
2) $B(\eta) \leq 0$ *for all* $x \in D \cap K$ *and all* $\eta \in G(x)$.
3) $G(D \cap K) \subset (C \cup D)$.

Furthermore, the set K *is forward invariant for* $\mathcal{H}$ *if the following additional conditions hold:*

4) No maximal solution to $\mathcal{H}$ *starting from* K *has a finite time escape within* $C \cap K$.
5) Every maximal solution from $(\partial C \cap K) \setminus D$ *is nontrivial.*

Remark 3.10. *One can guarantee that the solutions to* $\mathcal{H}$ *do not have a finite escape time*[2] *inside the set* $K \cap C$ *when, for example, the set* $K \cap C$ *is compact or when the flow map* F *has a global linear growth on* $K \cap C$. *Furthermore, according to [19, Proposition 3], the existence of a nontrivial solution starting from each point in* $(K \cap \partial C) \setminus D$ *can be proved by verifying the following infinitesimal condition.*

$$F(x) \cap T_{K \cap C}(x) \neq \emptyset \quad \forall x \in U(x_o) \cap (K \cap \partial C) \text{ and } \forall x_o \in (K \cap \partial C) \setminus D. \tag{15}$$

In the following, inspired by [16, Theorem 3.4], we propose sufficient conditions for pre-eventual conditional invariance for hybrid systems.

Theorem 3.11 (pre-Eventual Conditional Invariance). *Consider a hybrid system* $\mathcal{H} = (C, F, D, G)$ *and two sets* $K_o, K \subset \mathbb{R}^n$. *Then, the set* K *is pre-eventually conditionally invariant with respect to the set* K_o *for* $\mathcal{H}$ *if the following properties hold:*

1a) There exist a C^1 *function* $v : \mathbb{R}^n \to \mathbb{R}$ *and a locally Lipschitz function* $f_c : \mathbb{R} \to \mathbb{R}$ *such that*

$$\begin{aligned} &\langle \nabla v(x), \eta \rangle \leq f_c(v(x)) && \forall \eta \in F(x) \cap T_C(x),\ \forall x \in C, \\ &v(\eta) \leq v(x) && \forall \eta \in G(x),\ \forall x \in D. \end{aligned} \tag{16}$$

1b) There exists $r_1 > 0$ *such that*

$$S_1 := \{x \in C : v(x) < r_1\} \subset K, \tag{17}$$

and the solutions to $\dot{y} = f_c(y)$ *starting from* $v(K_o)$ *converge to* $(-\infty, r_1]$ *in finite time.*[3]

2a) There exist a C^1 *function* $w : \mathbb{R}^n \to \mathbb{R}$ *and a function* $f_d : \mathbb{R} \to \mathbb{R}$ *such that*

$$\begin{aligned} &\langle \nabla w(x), \eta \rangle \leq 0 && \forall \eta \in F(x) \cap T_C(x),\ \forall x \in C, \\ &w(\eta) \leq f_d(w(x)) && \forall \eta \in G(x),\ \forall x \in D. \end{aligned} \tag{18}$$

2b) There exists $r_2 > 0$ *such that*

$$S_2 := \{x \in D : w(x) < r_2\} \subset K \tag{19}$$

and the solutions to $z^+ = f_d(z)$ *starting from* $w(K_o)$ *converge to* $(-\infty, r_2]$ *in finite time.*

Sketch of Proof. According to the definition of pre-eventual conditional invariance, we need to show that for each complete solution ϕ to $\mathcal{H}$ starting from K_o, $\mathcal{T}_K(\phi) < \infty$ and $\phi(t, j) \in K$ for all $(t, j) \in \operatorname{dom} \phi$ such that $t + j \geq \mathcal{T}_K(\phi)$.

Consider a complete solution ϕ to $\mathcal{H}$ starting from $\phi(0, 0) \in K_o$. Let y be the maximal solution to $\dot{y} = f_c(y)$ starting from $y(0) = v(\phi(0, 0)) \in v(K_o)$ and let z be the complete solution to the system $z^+ = f_d(z)$ starting from $z(0) = w(\phi(0, 0)) \in w(K_o)$.

- Using Lemmas A.1, A.2, and A.3 under (16), we conclude that $v(\phi(t, j)) \leq y(t)$ for all $(t, j) \in \operatorname{dom} \phi$; on the other hand, under (18), we conclude that $w(\phi(t, j)) \leq z(j)$ for all $(t, j) \in \operatorname{dom} \phi$.
- Since the solution y starting from $v(K_o)$ will converge to $(-\infty, r_1]$ in finite time and the solution z starting from $w(K_o)$ will converge to $(-\infty, r_2]$ in finite time, we conclude the existence of $(t_y, j_z) \in \mathbb{R}_{\geq 0} \times \mathbb{N}$ such that $y(t) \in (-\infty, r_1]$ for all $t \geq t_y$ and $z(j) \in (-\infty, r_2]$ for all $j \geq j_z$.
- Since the solution ϕ is complete, $(\{t_y\} \times \mathbb{N}) \cap \operatorname{dom} \phi \neq \emptyset$; hence,

  $$v(\phi(t, j)) \leq r_1 \qquad \forall t \geq t_y : (t, j) \in \operatorname{dom} \phi$$

  or $(\mathbb{R}_{\geq 0} \times \{j_z\}) \cap \operatorname{dom} \phi \neq \emptyset$; hence,

  $$w(\phi(t, j)) \leq r_2 \qquad \forall j \geq j_z : (t, j) \in \operatorname{dom} \phi.$$

  As a consequence, we conclude that, for all $(t, j) \in \operatorname{dom} \phi$ such that $t + j \geq t_y + j_z$, it follows that $\phi(t, j) \in K$. □

Remark 3.12. *It is important to notice that, in Theorem 3.11, it is possible to conclude pre-eventual conditional invariance of* K *with respect to* K_o *using only condition 1) (or only condition 2), respectively) provided that we have the knowledge that the solutions from* K_o *reach the set* K *only via flowing (or only jumping, respectively). Indeed, in many applications of hybrid systems, the state variable is composed of both continuous and discrete variables, see the thermostat hybrid model in Example 3.6. Furthermore, when the sets* K_o *and* K *are defined only in terms of the continuous state variables (respectively, only in terms of the discrete state variables), it is possible to conclude that the solutions from* K_o *reach the set* K *only by flowing (respectively, only by jumping).*

Remark 3.13. *In Theorem 3.11, one could think of unifying conditions 1) and 2) as follows:*

$$\begin{aligned} &\langle \nabla v(x), \eta \rangle \leq f_c(v(x)) && \forall \eta \in F(x) \cap T_C(x),\ \forall x \in C, \\ &v(\eta) \leq f_d(v(x)) && \forall \eta \in G(x),\ \forall x \in D, \end{aligned} \tag{20}$$

where the functions f_c *and* f_d *are defined in Theorem 3.11. Furthermore, one could think of concluding the pre-enventually conditionally invariant of* K *with respect to* K_o *by showing that the set* $(-\infty, r]$ *is pre-enventually conditionally invariant with respect to* $v(K_o)$ *for the reduced system given by*

$$\begin{aligned} &\dot{y} = f_c(y) && y \in v(C) \\ &y^+ = f_d(y) && y \in v(D). \end{aligned} \tag{21}$$

Such a comparison-based reasoning is very useful to analyze purely continuous-time or purely discrete-time systems. In general, a key step for such a reasoning to hold consists in showing that (20) *and* (21) *imply that*

$$v(\phi(t, j)) \leq y(t, j) \qquad (t, j) \in \operatorname{dom} \phi. \tag{22}$$

However, (22) *does not necessarily hold under* (20) *and* (21) *due to the possible mismatch in the instant of jumps between the solutions* ϕ *to* $\mathcal{H}$ *and* y *to* (21). *It holds, however, if we replace the inequalities in* (20) *by equalities (the latter is in general very restrictive). As a consequence, the comparison arguments, in general, do not extend directly to the context of hybrid systems. Hence, it would be interesting to investigate a general version of the comparison lemma for hybrid*

[2] A solution has finite escape time inside a given set if the solution diverges while remaining inside the set within a bounded (hybrid) time domain; see [12, Chapter 3].
[3] The solutions to $\dot{y} = f_c(y)$ from $v(K_o)$ exist at least until they reach the set $(-\infty, r_1]$.

systems as it would simplify considerably the conditions in Theorem 3.11. This direction will pursued in future work.

Example 3.14. *Consider a hybrid system $\mathcal{H} = (C, F, D, G)$ with the state $x = (x_1, x_2) \in \mathbb{R}^2$ and the data*

$$F(x) := \begin{bmatrix} -x_1 - x_2 \\ -x_2 + x_1 \end{bmatrix} \quad \forall x \in C := \{x \in \mathbb{R}^2 : x_1 \geq 0,\ x_2 \geq -1,\ x_1 \geq x_2\}$$
$$G(x) := \begin{bmatrix} 0 \\ -x_2 \end{bmatrix} \quad \forall x \in D := \{x \in \mathbb{R}^2 : x_1 = 0,\ x_2 \leq 0\}.$$

Consider the sets K_o and K given by $K_o = [0, 1] \times (-\infty, -1]$ and $K = \mathbb{R}_{\geq 0} \times [-1/2, +\infty)$. Next, to conclude that the set K is pre-eventually conditionally invariant with respect to the set K_o for $\mathcal{H}$, will show that the conditions in Theorem 3.11 are satisfied. Indeed, for the candidate $v(x) = -|x|^2$, we conclude that for $f_c(y) := -2y$, item 1a) holds. Furthermore, we notice that $v(K_o) = (-\infty, -1]$ and that for, $r_1 = 1/2$, (17) holds trivially since $S_1 = \emptyset$. Finally, for the system $\dot{y} = f_c(y) = -2y$, it is easy to see that the solutions starting from $v(K_o) = (-\infty, -1]$ reach the set $(-\infty, 1/2]$. Hence, item 1b) is satisfied.

On the other hand, for the candidate $w(x) = -x_2$ and for

$$f_d(z) := \begin{cases} -z & \text{if } z \in w(D) \\ z & \text{otherwise,} \end{cases}$$

we conclude that item 2a) holds since $-\dot{x}_2 = x_2 - x_1 \leq 0$ for all $x \in C$ and, for all $x \in D$, $w(G(x)) = -w(x)$. Finally, item 2b) holds for $r_2 = 1/2$ and the solutions to $z^+ = f_d(z)$ starting from $[1, +\infty)$ reaches $(-\infty, 1/2]$.

Remark 3.15. *As we illustrated in Example 3.14, once we propose the candidate functions v and w, we find the functions f_c, f_d and the constants r_1, r_2 such that the conditions in Theorem 3.11 hold. That is, for a particular expression of the data of the hybrid system and the sets K_o and K, we can automate the process of generating the functions and parameters satisfying the conditions in Theorem 3.11 as in [21, 24].*

Remark 3.16. *It is important to notice that the conditions in item 1) in Theorem 3.11 can be removed when the following hold:*

- *The set K is forward pre-invariant for $\mathcal{H}$.*
- *The solutions to $\mathcal{H}$ starting from K_o achieve the necessary amount of jumps such that the solutions to $z^+ = f_d(z)$ from $w(K_o)$ reach $(-\infty, r_2]$.*

In the following, we propose sufficient conditions for eventual conditional invariance for hybrid systems.

Theorem 3.17 (Eventual Conditional Invariance). *Consider a hybrid system $\mathcal{H} = (C, F, D, G)$. Consider two sets $K_o, K \subset \mathbb{R}^n$ such that $K_o \subset C \cup D$ and K is pre-eventually conditionally invariant with respect to K_o. Then, the set K is eventually conditionally invariant with respect to the set K_o for $\mathcal{H}$ if the following property holds:*

- *There exists a set $S \subset C \cup D \cup K$ such that $K_o \cup K \subset S$ and S is forward invariant for $\mathcal{H}_m = (C_m, F_m, D_m, G_m)$ in (7).*

Sketch of Proof. Since the set K is pre-eventually conditionally invariant with respect to the set K_o for $\mathcal{H}$, to complete the proof, it remains only to show that the solutions to $\mathcal{H}$ starting from $K_o \setminus K$ always reach the set K. Proceeding by contradiction, assume the existence of a maximal solution ϕ to $\mathcal{H}$ starting from $K_o \setminus K$ that never reaches the set K. We notice that each solution to $\mathcal{H}$ starting from $K_o \setminus K$ is a solution to $\mathcal{H}_m$ provided that it does not reach the set K. Hence, since the set S is forward invariant for $\mathcal{H}_m$, we conclude that the solution ϕ is complete. The aforementioned fact contradicts the fact that K is pre-eventually conditionally invariant with respect to the set K_o for $\mathcal{H}$. □

Example 3.18. *We reconsider the hybrid system in Example 3.14. It is easy to see that the set $S := K_o \cup K$ is forward invariant for $\mathcal{H}_m$. Indeed, all the solutions to $\mathcal{H}_m$ starting from K_o flow in K_o until they reach K. Once in K they reduce the constant discrete solutions that are complete.*

3.3 Sufficient Conditions for Until Operators

Due to the equivalence we provide in Section 3.1, sufficient conditions that guarantee the needed invariance properties of the sets guarantee the satisfaction of the formulas in (4) and (5).

Theorem 3.19 (Weak Until). *Consider a hybrid system $\mathcal{H} = (C, F, D, G)$ satisfying (SA). Given atomic propositions p and q, let the sets P and Q be as in (6) such that $P \subset C \cup D$. Then, the formula $f = p\,\mathcal{U}_w q$ is satisfied for each solution ϕ to $\mathcal{H}$ at $(t, j) = (0, 0)$ with $(\phi, (0, 0)) \vDash p \vee q$ if there exists a C^1 barrier function candidate B with respect to the sets $(P \setminus Q, \mathbb{R}^n \setminus (P \cup Q))$ for $\mathcal{H}$ as in (14) such that $K := \{x \in C \cup D \cup Q : B(x) \leq 0\}$ is closed and the following hold:*

1) *For all $x \in (C \setminus Q) \cap (U(\partial K) \setminus K)$, $\langle \nabla B(x), \eta \rangle \leq 0$ for all $\eta \in F(x) \cap T_{C \setminus Q}(x)$.*
2) *For all $x \in K \cap (D \setminus Q)$, $B(\eta) \leq 0$ for all $\eta \in G(x)$.*
3) *For all $x \in K \cap (D \setminus Q)$, $G(x) \subset C \cup D \cup Q$.*

Sketch of Proof. Let the system $\mathcal{H}_m = (C_m, F_m, D_m, G_m)$ be as in (7). Since $K = \{x \in C \cup D \cup Q\} : B(x) \leq 0\}$ and the barrier function candidate B satisfies

$$B(x) \leq 0 \qquad \forall x \in P \setminus Q$$
$$B(x) > 0 \qquad \forall x \in (\overline{C} \cup D) \setminus (P \cup Q) = (\overline{C} \cup D \cup Q) \setminus (P \cup Q),$$

we conclude that B is a barrier candidate with respect to $(P \setminus Q, \mathbb{R}^n \setminus (P \cup Q))$ for $\mathcal{H}_m$. Furthermore, item 1) implies that $\langle \nabla B(x), \eta \rangle \leq 0$ for all $x \in (U(\partial K) \setminus K) \cap C_m$ and all $\eta \in F(x) \cap T_{C_m}(x)$. Item 2) implies that $B(\eta) \leq 0$ for all $x \in K \cap (D \setminus Q)$ and all $\eta \in G_m(x)$. When $x \in K \cap Q$, $G_m(x) = x$ and $B(x) \leq 0$; and thus, $B(\eta) \leq 0$ for all $x \in K \cap (D \cup Q)$ and all $\eta \in G_m(x)$. Item 3) implies that $G_m(K \cap (D \setminus Q)) \subset C_m \cup D_m$. Furthermore, $G_m(K \cap Q) = K \cap Q \subset C_m \cup D_m$. Hence, $G_m(K \cap D_m) \subset C_m \cup D_m$. Therefore, using Proposition 3.8, we conclude that $P \cup Q$ is conditionally invariant with respect to $P \setminus Q$ for $\mathcal{H}_m$. Hence, using Theorem 3.2, we conclude that the formula $f = p\,\mathcal{U}_w q$ is satisfied for each solution ϕ to $\mathcal{H}$ at $(t, j) = (0, 0)$. □

Example 3.20 (Bouncing ball). *We reconsider the bouncing-ball hybrid model in Example 3.3 in order to confirm the conclusions therein using Theorem 3.19. Indeed, consider the barrier candidate $B(x) := x_1 - \varepsilon$. It is easy to see that B is a barrier candidate with respect to $(P \setminus Q, \mathbb{R}^n \setminus (P \cup Q))$ for $\mathcal{H}$. Furthermore, for all $x \in C \setminus Q = \mathbb{R}_{\geq 0} \times \mathbb{R}_{\leq 0}$, we have $\langle \nabla B(x), F(x) \rangle = x_2 \leq 0$; hence, item 1) holds. Furthermore, for all $x \in K \cap D = D$, $B(G(x)) = B(x) \leq 0$; hence, item 2) holds. Finally, for all $x \in D$, $G(x) \in \{0\} \times \mathbb{R}_{\geq 0} \subset C$; hence, item 3) holds. As a consequence, using Theorem 3.19, we conclude*

that the formula $f = p\,\mathcal{U}_w q$ is satisfied for each solution ϕ to $\mathcal{H}$ at $(t,j) = (0,0)$ with $(\phi,(0,0)) \vDash p \vee q$.

Example 3.21 (Thermostat). *We reconsider the thermostat hybrid model in Example 3.6 in order to show that the formula $f = p\,\mathcal{U}_w q$ is satisfied for each solution ϕ to $\mathcal{H}$ at $(t,j) = (0,0)$ with $(\phi,(0,0)) \vDash p \vee q$ using Theorem 3.19. Indeed, consider the barrier candidate $B(x) := (2h-1)(z - z_{\max})$. It is easy to see that B is a barrier candidate with respect to $(P \setminus Q, \mathbb{R}^n \setminus (P \cup Q))$ for $\mathcal{H}$. Furthermore, for all $x \in C \setminus Q = (\{1\} \times \mathbb{R}) \cup (\{0\} \times (-\infty, z_{\max}))$, we have $\langle \nabla B(x), F(x)\rangle = (2h-1)(-z + z_0 + z_\triangle h) \leq 0$ under (9); hence, item 1) holds. Furthermore, for all $x \in K \cap D = [1 \quad z_{\max}]^\top$, $B(G(x)) = B([0 \quad z_{\max}]^\top) \leq 0$; hence, item 2) holds. Finally, for all $x \in D$, $G(x) \in C$; hence, item 3) holds. As a consequence, using Theorem 3.19, we conclude that the formula $f = p\,\mathcal{U}_w q$ is satisfied for each solution ϕ to $\mathcal{H}$ at $(t,j) = (0,0)$ with $(\phi,(0,0)) \vDash p \vee q$.*

Theorem 3.22 (Strong Until). *Consider a hybrid system $\mathcal{H} = (C,F,D,G)$ satisfying (SA). Given atomic propositions p and q, let the sets P and Q as in (6) such that $P \subset C \cup D$. Then, the formula $f = p\,\mathcal{U}_s q$ is satisfied for each solution ϕ to $\mathcal{H}$ at $(t,j) = (0,0)$ with $(\phi,(0,0)) \vDash p \vee q$ if the following hold:*

1) *The formula $p\,\mathcal{U}_w q$ is satisfied for each solution ϕ to $\mathcal{H}$ at $(t,j) = (0,0)$ with $(\phi,(0,0)) \vDash p \vee q$.*
2) *There exist a C^1 function $v : \mathbb{R}^n \to \mathbb{R}$, a locally Lipschitz function $f_c : \mathbb{R} \to \mathbb{R}$, and a constant $r_1 > 0$ such that the following hold:*
   2.1) *$\langle \nabla v(x), \eta\rangle \leq f_c(v(x))$ for all $\eta \in F(x) \cap T_{C\setminus Q}(x)$ and for all $x \in (C \cap P) \setminus Q$;*
   2.2) *$v(\eta) \leq v(x)$ for all $\eta \in G(x)$ and all $x \in D \cap P$;*
   2.3) *$S_1 := \{x \in C \cap P : v(x) < r_1\} \subset Q$ and the solutions to $\dot{y} = f_c(y)$ starting from $v(P \setminus Q)$ converge to $(-\infty, r_1]$ in finite time.*
3) *There exist a C^1 function $w : \mathbb{R}^n \to \mathbb{R}$, $f_d : \mathbb{R} \to \mathbb{R}$, and $r_2 > 0$ such that the following hold:*
   3.1) *$\langle \nabla w(x), \eta\rangle \leq 0$ for all $\eta \in F(x) \cap T_{C\setminus Q}(x)$ and all $x \in (C \cap P) \setminus Q$;*
   3.2) *$w(\eta) \leq f_d(w(x))$ for all $\eta \in G(x)$ and all $x \in D \cap P$;*
   3.3) *$S_2 := \{x \in D \cap P : w(x) < r_2\} \subset Q$ and the solutions to $z^+ = f_d(z)$ starting from $w(P \setminus Q)$ converge to $(-\infty, r_2]$ in finite time.*
4) *No maximal solution starting from P has a finite time escape within $P \cap (C \setminus Q)$ and every maximal solution from $(P \cap \partial C) \setminus (D \cup Q)$ is nontrivial.*

Sketch of Proof. Let the system $\mathcal{H}_m = (C_m, F_m, D_m, G_m)$ be as in (7). Using item 1) and Theorem 3.2, we conclude that $Q \cup P$ is conditionally invariant with respect to $P \setminus Q$ for $\mathcal{H}_m$. Furthermore, since the solutions starting from Q are discrete, we conclude that $P \cup Q$ is forward pre-invariant for $\mathcal{H}_m$. Next, under item 4) and using Proposition 3.9, we conclude that $P \cup Q$ is forward invariant for $\mathcal{H}_m$. As a last step using items 2) and 3), we show that Q is pre-eventually conditionally invariant with respect to $P \setminus Q$ for $\mathcal{H}_m$.

Indeed, consider the hybrid system $\mathcal{H}_m' = (C_m \cap P, F_m, D_m \cap (P \cup Q), G_m)$ which is the restriction of $\mathcal{H}_m$ to $P \cup Q$. Using Theorem 3.11 for $\mathcal{H}_m'$ under items 2) and 3) we conclude that Q is pre-eventually conditionally invariant with respect to $P \setminus Q$ for $\mathcal{H}_m'$. However, the solutions to $\mathcal{H}_m'$ are the solutions to $\mathcal{H}_m$ since $P \cup Q$ is forward invariant for $\mathcal{H}_m$. Hence, Q is pre-eventually conditionally invariant with respect to $P \setminus Q$ for $\mathcal{H}_m$. □

Example 3.23 (Thermostat). *We reconsider the thermostat hybrid model in Example 3.6 in order to show that the formula $f = p\,\mathcal{U}_s q$ is satisfied for each solution ϕ to $\mathcal{H}$ at $(t,j) = (0,0)$ with $(\phi,(0,0)) \vDash p \vee q$ using Theorem 3.22. Indeed, we already showed in Example 3.21 that the formula $f = p\,\mathcal{U}_w q$ is satisfied for each solution ϕ to $\mathcal{H}$ at $(t,j) = (0,0)$ with $(\phi,(0,0)) \vDash p \vee q$; item 1) is satisfied. Furthermore, for the candidate $v(x) = z_{\max} - z$, we conclude that for $f_c(y) := -y - a$ for some $a \in (0, z_{\max} - z_o - z_\triangle)$, items 2.1) and 2.2) hold. The constant a always exists under (9). Furthermore, we notice that $v(P \setminus Q) = v(P) = [0, +\infty)$ and that, for $r_1 = 0$, the inclusion in item 2.3) holds trivially since $S_1 = \emptyset$. Finally, for the system $\dot{y} = f_c(y) = -y - a$, it is easy to see that the solutions starting from $v(K_o) = [0, +\infty)$ reach the set $(-\infty, 0]$. Hence, item 2.3) is satisfied. On the other hand, for the candidate $w(x) = q$ and for*

$$f_d(z) := \begin{cases} 1 - z & \text{if } z \in w(D) \\ z & \text{otherwise,} \end{cases}$$

we conclude that items 3.1) and 3.2) hold since $\dot{q} = 0$ for all $x \in C$ and, for all $x \in D$, $w(G(x)) = 1 - w(x)$. Furthermore, for $r_2 = 0$ the inclusion in item 3.3) holds trivially since $S_2 = \emptyset$. Finally, the solutions to $z^+ = f_d(z)$ starting from $\{1\}$ reach $(-\infty, 0]$; hence, item 3.3) holds. Finally, in order to conclude item 4), we notice that F is linear; hence, there is no possibility of finite-time escape inside C. Moreover, the solution starting from $C \setminus D$ are nontrivial.

4 CONCLUSION

In this paper, tools are introduced for certifying temporal logic specifications involving until operators for hybrid systems. For such systems, equivalence relationships are established between the satisfaction of formulas having until operators and some of the invariance notions studied in control literature. In particular, conditional invariance and eventual conditional invariance notions are revisited in this paper in the context of hybrid systems. Furthermore, sufficient conditions certifying these invariance properties are proposed. As a consequence, sufficient conditions (not involving the computation of the systems' solutions) guaranteeing the satisfaction of temporal logic specifications with the until operators are proposed. Future research direction may include the relaxation of the proposed sufficient conditions for the eventual conditional invariance notion along the lines of Remark 3.13. Furthermore, another extension consists in the analysis proposed in this paper to handle more complex specifications where the until operator is involved in addition to other operators as in [9].

ACKNOWLEDGMENTS

This research has been partially supported by the National Science Foundation under Grant no. ECS-1710621 and Grant no. CNS-1544396, by the Air Force Office of Scientific Research under Grant no. FA9550-16-1-0015, Grant no. FA9550-19-1-0053, and Grant no. FA9550-19-1-0169, and by CITRIS and the Banatao Institute at the University of California.

REFERENCES

[1] Rajeev Alur, Thomas A Henzinger, and Orna Kupferman. 2002. Alternating-time temporal logic. *Journal of the ACM (JACM)* 49, 5 (2002), 672–713.

[2] Jean-Pierre Aubin and Hélène Frankowska. 2009. *Set-valued Analysis*. Springer Science & Business Media.

[3] Andrea Bisoffi and Dimos V Dimarogonas. 2018. A hybrid barrier certificate approach to satisfy linear temporal logic specifications. In *2018 Annual American Control Conference (ACC)*. IEEE, 634–639.

[4] Edmund M Clarke Jr, Orna Grumberg, Daniel Kroening, Doron Peled, and Helmut Veith. 2018. *Model checking*. MIT press.

[5] Cindy Eisner, Dana Fisman, and John Havlicek. 2005. A topological characterization of weakness. In *Proceedings of the twenty-fourth annual ACM symposium on Principles of distributed computing*. 1–8.

[6] Georgios E Fainekos, Antoine Girard, Hadas Kress-Gazit, and George J Pappas. 2009. Temporal logic motion planning for dynamic robots. *Automatica* 45, 2 (2009), 343–352.

[7] Antoine Girard and George J Pappas. 2006. Verification using simulation. In *International Workshop on Hybrid Systems: Computation and Control*. Springer, 272–286.

[8] Rafal Goebel, Ricardo G Sanfelice, and Andrew R Teel. 2012. *Hybrid Dynamical Systems: modeling, stability, and robustness*. Princeton University Press.

[9] Hyejin Han and Ricardo G Sanfelice. 2020. Linear temporal logic for hybrid dynamical systems: Characterizations and sufficient conditions. *Nonlinear Analysis: Hybrid Systems* 36 (2020), 100865.

[10] Gerard J. Holzmann. 1997. The model checker SPIN. *IEEE Transactions on software engineering* 23, 5 (1997), 279–295.

[11] Sertac Karaman, Ricardo G Sanfelice, and Emilio Frazzoli. 2008. Optimal control of mixed logical dynamical systems with linear temporal logic specifications. In *2008 47th IEEE Conference on Decision and Control*. IEEE, 2117–2122.

[12] Hassan K Khalil. 2002. *Nonlinear systems* (3rd ed.). Prentice Hall.

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

[14] Ron Koymans. 1990. Specifying real-time properties with metric temporal logic. *Real-time systems* 2, 4 (1990), 255–299.

[15] YoungMin Kwon and Gul Agha. 2008. LTLC: Linear temporal logic for control. *Hybrid Systems: Computation and Control* (2008), 316–329.

[16] Gangaram S Ladde and S Leela. 1972. Analysis of invariant sets. *Annali di Matematica Pura ed Applicata* 94, 1 (1972), 283–289.

[17] Mohamed Maghenem and Ricardo G Sanfelice. 2019. Characterization of Safety and Conditional Invariance for Nonlinear Systems. In *2019 American Control Conference (ACC)*. 5039–5044.

[18] Mohamed Maghenem and Ricardo G Sanfelice. 2019. Characterizations of safety in hybrid inclusions via barrier functions. In *Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control (HSCC)*. 109–118.

[19] Mohamed Maghenem and Ricardo G Sanfelice. 2019. Sufficient conditions for forward invariance and contractivity in hybrid inclusions using barrier functions. *arXiv preprint:1908.03980* (2019).

[20] Oded Maler, Zohar Manna, and Amir Pnueli. 1991. Prom timed to hybrid systems. In *Workshop/School/Symposium of the REX Project (Research and Education in Concurrent Systems)*. Springer, 447–484.

[21] Jens Oehlerking, Henning Burchardt, and Oliver Theel. 2007. Fully automated stability verification for piecewise affine systems. In *International Workshop on Hybrid Systems: Computation and Control*. Springer, 741–745.

[22] Nir Piterman and Amir Pnueli. 2018. Temporal logic and fair discrete systems. In *Handbook of Model Checking*. Springer, 27–73.

[23] Amir Pnueli. 1977. The temporal logic of programs. In *18th Annual Symposium on Foundations of Computer Science (sfcs 1977)*. IEEE, 46–57.

[24] Stephen Prajna and Ali Jadbabaie. 2004. Safety verification of hybrid systems using barrier certificates. In *International Workshop on Hybrid Systems: Computation and Control*. Springer, 477–492.

[25] Vasumathi Raman, Alexandre Donzé, Dorsa Sadigh, Richard M Murray, and Sanjit A Seshia. 2015. Reactive synthesis from signal temporal logic specifications. In *Proceedings of the 18th international conference on hybrid systems: Computation and control*. 239–248.

[26] Sayan Saha and A Agung Julius. 2016. An MILP approach for real-time optimal controller synthesis with Metric Temporal Logic specifications. In *American Control Conference (ACC), 2016*. IEEE, 1105–1110.

[27] Ricardo G. Sanfelice. 2015. *Analysis and Design of Cyber-Physical Systems: A Hybrid Control Systems Approach*. CRC Press, 3–31. https://doi.org/10.1201/b19290-3

[28] JG Thistle and WM Wonham. 1986. Control problems in a temporal logic framework. *Internat. J. Control* 44, 4 (1986), 943–976.

[29] Jana Tumova and Dimos V Dimarogonas. 2016. Multi-agent planning under local LTL specifications and event-based synchronization. *Automatica* 70 (2016), 239–248.

[30] Eric M Wolff, Ufuk Topcu, and Richard M Murray. 2014. Optimization-based trajectory generation with linear temporal logic specifications. In *Robotics and Automation (ICRA), 2014*. IEEE, 5319–5325.

[31] Tichakorn Wongpiromsarn, Ufuk Topcu, and Richard M Murray. 2010. Receding horizon control for temporal logic specifications. In *Proceedings of the 13th ACM international conference on Hybrid systems: computation and control*. 101–110.

A APPENDIX

The following result is a version of the well-known comparison Lemma that can be found in [12, Lemma 3.4].

Lemma A.1. *Consider the scalar differential equation given by*

$$\dot{u} = f(t,u), \qquad u(t_0) = u_0, \tag{23}$$

where for all $t \geq 0$ and all $u \in S \subset \mathbb{R}$, $f(t,u)$ is continuous in t and locally Lipschitz in u. Furthermore, let $[t_0, T)$ be the maximal interval, T can be infinity, of existence of the solution $u(t)$. Moreover, suppose that $u(t) \in S$ for all $t \in [t_0, T)$.

On the other hand, let $v(t)$ be a continuous function such that $v(t_0) \leq u_0$, $v(t) \in S$ for all $t \in [t_0, T)$, and its upper right-hand derivative $D^+v(t)$ satisfies the following differential inequality, for almost all $t \in [t_0, T)$,

$$D^+v(t) := \limsup_{s \to 0^+} \frac{v(t+s) - v(t)}{s} \leq f(t, v(t)). \tag{24}$$

Then, $v(t) \leq u(t)$ for all $t \in [t_0, T)$.

Lemma A.2. *Assume that the function $t \mapsto v(t)$ in Lemma A.1 satisfies $v(t) = v(x(t))$ for all $t \in [t_0, T)$ with $t \mapsto x(t)$ a solution to the system*

$$\dot{x} \in F(x) \qquad \forall x \in C \subset \mathbb{R}^n,$$

and $v \in C^1$, it follows that, for almost all $t \in [t_0, T)$,

$$D^+v(t) = \dot{v}(t) = \langle \nabla v(x(t)), \dot{x}(t) \rangle.$$

Proof. Since the solution x is absolutely continuous, it follows that $\dot{x}(t)$ exists for almost all $t \in [t_0, T)$. Furthermore, since $v \in C^1$. Hence, $\dot{v}(t)$ exists for almost all $t \in [t_0, T)$. Let $t \in [t_0, T)$ such that $\dot{v}(t)$ exists, then, by definition of the time derivative, we conclude that

$$\dot{v}(t) = \lim_{s \to 0} \frac{v(t+s) - v(t)}{s} = \limsup_{s \to 0^+} \frac{v(t+s) - v(t)}{s} = D^+v(t).$$

Furthermore, using the classical chain rule for composition of differentiable functions, we conclude that

$$\dot{v}(t) = \langle \nabla v(x(t)), \dot{x}(t) \rangle.$$

□

Lemma A.3. *Let $x : [t_0, T) \to \mathbb{R}^n$ be a solution to the following constrained differential inclusion*

$$\dot{x} \in F(x) \qquad \forall x \in C \subset \mathbb{R}^n.$$

Then, for almost all $t \in [t_0, T)$,

$$\dot{x}(t) \in T_C(x(t)).$$

Proof. Let $t \in [t_0, T)$ such that $\dot{x}(t)$ exists; thus, $\dot{x}(t) \in F(x(t,j))$. Furthermore, let a sequence $\{t_n\}_{n \in \mathbb{N}} \subset (t_0, T - t)$ such that $t_n \to 0$. That is, for $v_n(t) := (x(t_n) - x(t))/t_n$, we have $\lim_n v_n(t) = \dot{x}(t)$ and at the same time $x(t) + t_n v_n(t) = x(t_n) \in C$. Hence, using (13), we conclude that $\dot{x}(t) \in T_C(x(t))$. □