Non-deterministic temporal logics for general flow systems ⋆

J.M. Davoren[1], V. Coulthard[1,2], N. Markey[3], and T. Moor[4]

[1] Department of Electrical & Electronic Engineering
The University of Melbourne, VIC 3010 AUSTRALIA
davoren@unimelb.edu.au
[2] Computer Sciences Laboratory, RSISE
The Australian National University, Canberra ACT 0200 AUSTRALIA
vaughan@discus.anu.edu.au
[3] Département d'Informatique
Université Libre de Bruxelles, 1050 BELGIUM
markey@lsv.ens-cachan.fr
[4] Lehrstuhl für Regelungstechnik
Friedrich-Alexander-Universität, Erlangen D-91058 GERMANY
thomas.moor@rt.eei.uni-erlangen.de

Abstract. In this paper, we use the constructs of branching temporal logic to formalize reasoning about a class of general flow systems, including discrete-time transition systems, continuous-time differential inclusions, and hybrid-time systems such as hybrid automata. We introduce Full General Flow Logic, **GFL***, which has essentially the same syntax as the well-known Full Computation Tree Logic, **CTL***, but generalizes the semantics to general flow systems over arbitrary time-lines. We propose an axiomatic proof system for **GFL*** and establish its soundness w.r.t. the general flow semantics.

1 Introduction

Recent work in set-valued dynamical systems [4, 5], investigates a general class known as *evolutionary systems*. These are described by a set-valued map $\mathcal{S}$ which maps each state $x \in X$ to the *set* $\mathcal{S}(x)$ of all possible *future evolutions* γ from initial state x, where $\gamma : [0, \infty) \to X$, $\gamma(0) = x$. These systems are *non-deterministic*: from an initial state, there may be none, exactly one, or many possible futures. The defining condition of these systems is that the family of sets $\mathcal{S}(x)$ must be closed under the operations of taking a *suffix* of an evolution, and of taking the *fusion* of the two evolutions at a common state. It includes as examples the solution maps over real time of differential equations with inputs, and of differential inclusions and their impulse/hybrid extensions [4, 7]. In the discrete time case, these same closure properties come up in the study of sets *computation sequences*, in automata theory and the semantics of branching temporal

⋆ Research support from Australian Research Council, Grants DP0208553 & LX0242359, and CNRS France, Embassy of France in Australia, & Aust. Academy of Science, Grant DEMRIX236. The work has benefited from discussions with participants of the Logic Seminar at the University of Melbourne, particularly B. Humberstone, L. Humberstone and G. Restall.

logics such as **CTL*** [1, 17, 16]. The same closure properties appear again in Willems' *Behavioural Systems theory* [18], under the names *time invariance* and *axiom of state*, with the time domain the reals *or* the integers. In the analysis of evolutionary systems, there is particular interest in the area of *Viability Theory* [7, 4], where a central concept is that of an evolution being "*viable in K until capturing target C*", which means that the path starts at a state in K, and *either* remains in K for all time, *or* it reaches C in finite time, and remains within K until it does so. From a computer science perspective, this concept corresponds to the *Until* construct on paths in temporal logic.

The purpose of this paper is to generalize the class of evolutionary systems to give an adequate semantics for non-deterministic temporal logic that is uniform for discrete-time transition systems, continuous-time differential inclusions, and hybrid systems, where the time domains of evolutions lie in the lexicographically ordered $L = \mathbb{N} \times \mathbb{R}^+_\circ$. There are three novelties in our work. ***First***, we take a minimalist approach to the notion of a time-line: for the suffix and fusion-closure properties, the minimal structure needed on a linear order are translation or shift maps, which is weaker than a semi-group. ***Second***, we don't take as primitive objects evolutions or paths defined on the entire time line; that perspective gives something of a "god's eye" view of the system, looking forward from now to eternity. Instead, our basic object of a *path* describes a *bounded-time* segment of a possible evolution of or signal within a system; it *starts somewhere*, at relative time 0 with some value $x \in X$, and then progresses with an ordering given by the underlying time-line L to *end somewhere*, at some time-point $\tau \geqslant 0$, with a value $x' \in X$. We then build up a theory of infinitary extensions with unbounded time domains. ***Third***, we don't restrict to paths $\gamma : T \to X$ with bounded *interval* time domains $T = [0, \tau] \subseteq L$, but rather allow "gaps" in T. Over $L = \mathbb{N} \times \mathbb{R}^+_\circ$, finite hybrid trajectories are functions taking values in some X, with time domains $T \subseteq L$ of the form $T = \bigcup_{i<N} [\,(i, 0),\ (i, \Delta_i)\,]$, with $\Delta_i \in \mathbb{R}^+_\circ$ the duration of the i-th interval. Within T, time $(i + 1, 0)$ is the immediate *discrete successor* of time (i, Δ_i), but in the underlying line L, there is a continuum-length open interval "gap" in between.

The body of the paper is as follows. Section 2 covers preliminaries on set-valued maps and linear orders, and develops some basic theory of paths with "gappy" time domains. We introduce general flow systems in Section 3, and give examples in discrete, continuous and hybrid time. In Section 4, we give an infinitary completion construction, and relate our model class to evolutionary systems and behavioural systems. Section 5 introduces Full General Flow Logic, **GFL***, with basically the same syntax as the well-known Full Computation Tree Logic, **CTL***, developed for discrete-time models, but semantics w.r.t. general flow systems over arbitrary time. In Section 6, we propose an axiomatic proof system for **GFL*** and sketch soundness w.r.t. general flow semantics.

2 Preliminaries: set-valued maps, time-lines and paths

When we write $Y \subset X$ for sets X, Y, we will mean Y is a *proper* subset of X, and so $Y \subseteq X$ iff $Y \subset X$ or $Y = X$. We write $r : X \rightsquigarrow Y$ to mean $r : X \to 2^Y$ is a *set-valued map*, with set-values $r(x) \subseteq Y$ for every $x \in X$ (possibly $r(x) = \varnothing$); equivalently, $r \subseteq X \times Y$ is a *relation*. Let $[\,X \rightsquigarrow Y\,] := 2^{X \times Y}$ denote the set of all maps, partially ordered by $\subseteq$, so $r \subseteq r'$ iff $r(x) \subseteq r'(x)$ for all $x \in X$, with least element the empty map $\varnothing$. Every map $r : X \rightsquigarrow Y$ has a *converse* $r^{-1} : Y \rightsquigarrow X$ given by $x \in r^{-1}(y)$ iff $y \in r(x)$. The *domain* of a set-valued map is $dom(r) := \{x \in X \mid r(x) \neq \varnothing\}$, and the *range* is $ran(r) := dom(r^{-1}) \subseteq Y$. A map $r : X \rightsquigarrow Y$ is *total on* X if $dom(r) = X$. We distinguish several sub-classes of maps. We write $r : X \to Y$ to mean r is a (total) *function*, with values written $r(x) = y$. We also distinguish *partial functions*, and write $r : X \dashrightarrow Y$ to mean that r is single-valued on its domain $dom(r) \subseteq X$, and write $r(x) = y$ when $x \in dom(r)$, and $r(x) = \text{UNDEF}$ when $x \notin dom(r)$.

Let $(L, <, 0)$ be a *linear order* with least element 0 and no largest element, and $\leqslant$ the reflexive closure of $<$. For elements $a, b \in L$, the set $[a, b] := \{l \in L \mid a \leqslant l \leqslant b\}$ is a *closed, bounded interval* in L, and $(a, b) := \{l \in L \mid a < l < b\}$ is an *open bounded interval*; similarly for half-open/half-closed bounded intervals $[a, b)$ and $(a, b]$. For right *unbounded intervals*, we write $[a, \infty) := \{l \in L \mid a \leqslant l\}$. Any subset $T \subseteq L$ gives a linear order $(T, <_T)$, where $<_T := < \cap (T \times T)$. Define a partial function $\mathbf{succ}_L : L \dashrightarrow L$, for $a, b \in L$, by $\mathbf{succ}_L(a) := b$ iff $a < b$ and there does *not* exists an $l \in L$ such that $a < l < b$. A linear order L is called *discrete* if $\mathbf{succ}_L$ is a *total* function ($dom(\mathbf{succ}_L) = L$), and is *dense* if $\mathbf{succ}_L$ if $dom(\mathbf{succ}_L) = \varnothing$. Given two linear orders $(L, <)$ and $(L', <')$, a function $g : L \to L'$ is called: *strictly order-preserving* if $(\forall l, k \in L)$, $l < k$ implies $g(l) <' g(k)$; and an *order isomorphism* if it bijective and both g and g^{-1} are strictly order-preserving.

Definition 1. *Let* $(L, <, 0)$ *be a* linear order *with least element* 0 *and no largest element. We call* L *a* (future) time line *if* L *is* shift invariant, *in the sense that if for each* $a \in L$, *there exists an order isomorphism* $\sigma^{-a} : [a, \infty) \to L$, *with inverse* $\sigma^{+a} := (\sigma^{-a})^{-1} : L \to [a, \infty)$, *and* $\sigma^{-0} = id_L$. *We call the functions* σ^{-a} left a-shift maps, *and the inverses* σ^{+a} right a-shift maps.

The discrete time line $\mathbb{N}$, and the dense continuum time line $\mathbb{R}^+_\circ := [0, \infty)$, are considered with their usual orderings. The hybrid time space $\mathbb{N} \times \mathbb{R}^+_\circ$ is linearly ordered *lexicographically*: i.e. $(i, t) <_{\text{lex}} (j, s)$ iff $i < j$ or $i = j$ and $t < s$. The least element is $\mathbf{0} := (0, 0)$. This ordering does not admit any natural addition operation to make it a linearly ordered semi-group, but its shift invariance is witnessed by the following order isomorphisms: for each $a = (k, r) \in L$, define $\sigma^{-a} : [a, \infty) \to L$ by $\sigma^{-a}(i, t) := (0, t - r)$ if $i = k$ and $\sigma^{-a}(i, t) := (i - k, t)$ if $i > k$, for $l = (i, t) \in [a, \infty)$. Then $\sigma^{+a} : L \to [a, \infty)$ satisfies $\sigma^{+a}(i, t) = (k, t + r)$ if $i = 0$ and $\sigma^{+a}(i, t) = (i + k, t)$ if $i > 0$. The full hybrid time line $\mathbb{N} \times \mathbb{R}^+_\circ$ is everywhere dense. In the "gappy" time domains $T \subset L$ considered below, the partial function $\mathbf{succ}_T$ may be defined at some time points in T and not at others, so T is a "hybrid" of discrete and dense.

Definition 2. *Let* $(L, <, 0)$ *be a time line. A* bounded time domain *in* L *is a proper subset* $T \subset L$ *with least element* 0 *and a largest element* b_T *such that* T *is a finite union of closed intervals in* L, *of the form* $T = \bigcup_{i<N} [a_i, b_i]$, *where* $N \in \mathbb{N}$ *and* $a_0 = 0$ *and* $a_i \leqslant b_i < a_{i+1}$ *for* $i < N - 1$, *and* $b_{N-1} = b_T$. *Let* $\mathsf{BT}(L) \subset 2^L$ *denote the set of all bounded time domains in* L. *Also define* $\mathsf{BI}(L) := \{T \in \mathsf{BT}(L) \mid (\exists b \in L)\, T = [0, b]\}$ *to be the subset of interval time domains. Over any set (signal space)* $X \neq \varnothing$, *define the set of* L-paths *in* X, *by* $\mathsf{Path}(L, X) := \{\gamma : L \dashrightarrow X \mid dom(\gamma) \in \mathsf{BT}(L)\}$, *and define* $\mathrm{IPath}(L, X)$ *to be the subset* interval paths *with* $dom(\gamma) \in \mathsf{BI}(L)$. *For*

$\gamma \in \mathsf{Path}(L,X)$, define $b_\gamma := b_{dom(\gamma)}$ to be the largest element in $dom(\gamma)$, so that $\gamma(0) \in X$ is the start-value of γ and $\gamma(b_\gamma) \in X$ is the end-value of γ.

Proposition 1. *For L any time line, the set $\mathsf{BT}(L)$ is closed under the following operations: for $T, T' \in \mathsf{BT}(L)$ and $t \in L$,*
- *intersection: $T \cap T' \in \mathsf{BT}(L)$; in particular, $[0,t] \cap T \in \mathsf{BT}(L)$ if $t \in T$;*
- *left t-shift: $\sigma^{-t}([t, b_T] \cap T) \in \mathsf{BT}(L)$ if $t \in T$;*
- *union with right t-shift: $T \cup \sigma^{+t}(T) \in \mathsf{BT}(L)$ if $t \geqslant b_T$.*

The subset $\mathsf{BI}(L)$ of bounded initial closed intervals is closed under the first two operations, and is also closed under union with right shift restricted to $t = b_T$.

For X any value space, the following operations are well-defined in $\mathsf{Path}(L,X)$: for $\gamma, \gamma' \in \mathsf{Path}(L,X)$ and $t \in dom(\gamma)$,
- *t-end prefix: $\gamma|_t \in \mathsf{Path}(L,X)$, where $\gamma|_t := \gamma\restriction_{[0,t]\cap dom(\gamma)}$*
- *t-start suffix: ${}_t|\gamma \in \mathsf{Path}(L,X)$, where $({}_t|\gamma)(l) := \gamma(\sigma^{+t}(l))$ for all $l \in dom({}_t|\gamma) := \sigma^{-t}([t, b_\gamma] \cap dom(\gamma))$*
- *fusion: $\gamma * \gamma' \in \mathsf{Path}(L,X)$, provided that $\gamma'(0) = \gamma(b_\gamma)$, where*
  $(\gamma * \gamma')(l) := \gamma(l)$ for $l \in dom(\gamma)$ and
  $(\gamma * \gamma')(l) := \gamma'(\sigma^{-b_\gamma}(l))$ for $l \in \sigma^{+b_\gamma}(dom(\gamma'))$.

For each value $x \in X$, define the *trivial path* $\theta_x : [0,0] \to X$ by $\theta_x(0) = x$. In $\mathsf{Path}(L,X)$, the trivial path θ_x functions as a point-wise identity with respect to fusion: $\theta_x * \gamma = \gamma$ iff γ starts at value $x = \gamma(0)$, and $\gamma * \theta_x = \gamma$ iff γ ends at value $x = \gamma(b_\gamma)$.

Definition 3. *Let $(L, <, 0)$ be a time line and X a value space. Define a partial order on $\mathsf{Path}(L,X)$ from the underlying linear order on L (re-using notation) by: $\gamma < \gamma'$ iff $\gamma \subset \gamma'$ and $t < t'$ for all $t \in dom(\gamma)$ and $t' \in dom(\gamma') - dom(\gamma)$. If $\gamma < \gamma'$, we say the path γ' is a (proper)* extension *of γ, or γ is a proper* prefix *of γ'.*

In general, the path extension ordering $<$ is a proper subordering of the subset relation, but when restricted to the set $\mathrm{IPath}(L,X)$, it collapses to the subset relation. The following proposition characterizes the path extension partial order in terms of the fusion operation.

Proposition 2. *For L a time line, X a value space, and for all $\gamma, \gamma' \in \mathsf{Path}(L,X)$, $\gamma < \gamma'$ iff $\gamma' = \gamma * \gamma''$ for some $\gamma'' \in \mathsf{Path}(L,X)$ with $\gamma'' \neq \theta_x$ and $\gamma''(0) = \gamma(b_\gamma)$.*

We now return to the hybrid time line $L = \mathbb{N} \times \mathbb{R}^+_\circ$ for a more detailed discussion of some of its paths. Define $DS := \mathrm{IPath}(\mathbb{N}, \mathbb{R}^+_\circ)$ to be the set of all (finite) *duration sequences*; i.e. $\Delta \in DS$ is a finite sequence of values $\Delta_i := \Delta(i) \in \mathbb{R}^+_\circ$ for $i < N$ for $N = \mathrm{length}(\Delta) \in \mathbb{N}$. For duration sequences $\Delta \in DS$, define $HT(\Delta)$ to be the *hybrid time domain* determined by Δ:

$$\begin{aligned} HT(\Delta) &:= \textstyle\bigcup_{i<\mathrm{length}(\Delta)} [\,(i,0),\,(i,\Delta_i)\,] \\ \mathsf{HT} &:= \{\, HT(\Delta) \in \mathsf{BT}(L) \mid \Delta \in DS \,\} \\ \mathsf{HPath}(X) &:= \{\, \gamma \in \mathsf{Path}(\mathbb{N} \times \mathbb{R}^+_\circ,\, X) \mid dom(\gamma) \in \mathsf{HT} \,\} \end{aligned} \tag{1}$$

For hybrid paths $\gamma \in \mathsf{HPath}(X)$, define the *duration sequence* of γ by $\mathrm{ds}(\gamma) = \Delta$ iff $dom(\gamma) = HT(\Delta)$ for $\Delta \in DS$, and define the *discrete length* of γ by $\mathrm{dl}(\gamma) := \mathrm{length}(\mathrm{ds}(\gamma)) \in \mathbb{N}$. Also define the *total duration* of γ by $\mathrm{td}(\gamma) := \sum_{i<\mathrm{dl}(\gamma)} \Delta_i$.

Proposition 3. *For all* $\gamma, \gamma' \in \mathsf{HPath}(X)$,

$$\gamma \leqslant_{\text{lex}} \gamma' \textit{ iff } \mathrm{dl}(\gamma) \leqslant \mathrm{dl}(\gamma') \textit{ and } (\forall i < N := \mathrm{dl}(\gamma) - 1\,)\ \gamma_i = \gamma_i' \textit{ and } \gamma_N \leqslant \gamma_N'$$

With hybrid paths, we have to deal with the product structure on the time line. We also encounter product structure on the value space. Let $\pi_X : (X \times Y) \to X$ and $\pi_Y : (X \times Y) \to Y$ be the standard coordinate projection functions on a product of sets $X \times Y$. These can be lifted to give projection functions on paths $\pi_X : \mathsf{Path}(L, X \times Y) \to \mathsf{Path}(L, X)$ and to projections on functions $\pi_X : [\,L \to (X \times Y)\,] \to [\,L \to X\,]$, by defining $(\pi_X \zeta)(t) := \pi_X(\zeta(t))$ for $t \in \mathit{dom}(\zeta)$ and $\zeta \in \mathsf{Path}(L, X \times Y)$ or $\zeta : L \to (X \times Y)$; and symmetrically for π_Y in the other coordinate.

3 General flow systems

The general dynamical system model we develop here is essentially Aubin's model of an evolutionary system, generalized to arbitrary time lines L, and "deconstructed", so that the basic objects are bounded length paths, having $\mathit{dom}(\gamma) \subseteq [0, b_\gamma]$.

Definition 4. *Let* $(L, <, 0)$ *be a time line, and let* $X \neq \varnothing$ *be an arbitrary value space. A* general flow system *over* X *with time line* L *is a map* $\Phi\colon X \rightsquigarrow \mathsf{Path}(L, X)$ *satisfying, for all* $x \in \mathit{dom}(\Phi)$*, for all* $\gamma \in \Phi(x)$*, and for all* $t \in \mathit{dom}(\gamma)$*:*

(GF0) initialization: $\gamma(0) = x$

(GF1) suffix-closure: ${}_t|\gamma \in \Phi(\gamma(t))$

(GF2) fusion-closure: $\gamma|_t * \gamma' \in \Phi(x)$ *for all* $\gamma' \in \Phi(\gamma(t))$

- Φ *has* interval paths *if* $\mathit{ran}(\Phi) \subseteq \mathsf{IPath}(L, X)$*;*
- Φ *has* hybrid paths *if* $\mathit{ran}(\Phi) \subseteq \mathsf{HPath}(X)$ *and* $L = \mathbb{N} \times \mathbb{R}^+_{\circ}$*;*
- Φ *is* reflexive *if* $\theta_x \in \Phi(x)$ *for all* $x \in \mathit{dom}(\Phi)$*;*
- Φ *is* blocked at x *if* $\Phi(x) = \{\theta_x\}$*, and* non-blocking *if not blocked at any* $x \in X$*;*
- Φ *is* prefix-closed *if* $\gamma|_t \in \Phi(x)$ *for all* $x \in \mathit{dom}(\Phi)$*,* $\gamma \in \Phi(x)$ *and* $t \in \mathit{dom}(\gamma)$*;*
- Φ *is* deterministic *if for all* $x \in \mathrm{dom}(\Phi)$*, the set* $\Phi(x)$ *is linearly ordered by* $<$*.*

In terms of *Behavioural Systems theory* [18], the suffix-closure condition $(\mathbf{GF1})$ corresponds to the *time invariance* property, while the fusion-closure condition $(\mathbf{GF2})$ corresponds to the so-called *"axiom of state"* principle, that *"the state should contain sufficient information about the past so as to determine the future behaviour"*, because the various possible extensions of a trajectory at time t are exactly those which would have been possible if we had observed only the state at time t, and not the past of the trajectory prior to that point.

Proposition 4. *Let* $(L, <, 0)$ *be a time line, let* $X \neq \varnothing$ *be a value space, and let* $\Phi\colon X \rightsquigarrow \mathsf{Path}(L, X)$ *be a general flow system over* X *with respect to* L*. Then:*

$(1.)$ *The set* $\mathit{dom}(\Phi) \subseteq X$ *is closed under reachability by* Φ*-paths:*
if $x \in \mathit{dom}(\Phi)$ *and* $\gamma \in \Phi(x)$*, and* $t \in \mathit{dom}(\gamma)$*, then* $\gamma(t) \in \mathit{dom}(\Phi)$*.*

$(2.)$ Φ *is reflexive iff* Φ *is prefix-closed.*

$(3.)$ Φ *is non-blocking iff for all* $x \in \mathit{dom}(\Phi)$*,* $\gamma \in \Phi(x)$*, there is a* $\gamma' \in \Phi(x) : \gamma < \gamma'$*.*

Example 1. If $g : L_1 \to L_2$ is an order embedding, and $\Phi : X \rightsquigarrow \mathsf{Path}(L_1, X)$ is a general flow system, then the map $\Phi_g : X \rightsquigarrow \mathsf{Path}(L_2, X)$ is also a general flow, where for $x \in dom(\Phi_g) := dom(\Phi)$, define $\Phi_g(x) := \{\eta \in \mathsf{Path}(L_2, X) \mid \exists \gamma \in \Phi(x) : dom(\eta) = g(dom(\gamma)) \wedge (\forall t \in dom(\eta))\ \eta(t) = \gamma(g^{-1}(t))\}$.

Example 2. A (basic) *state transition system* is a structure (X, R) where $X \neq \varnothing$ is the state space, and $R : X \rightsquigarrow X$ is any set-valued map (the one-step transition relation). The map R determines a general flow system with interval paths over time-line $L = \mathbb{N}$: $\Phi_R(x) := \{\gamma \in \mathrm{IPath}(\mathbb{N}, X) \mid \gamma(0) = x \wedge (\forall i < b_\gamma - 1)\ \gamma(i+1) \in R(\gamma(i))\}$. It is easily verified that $\Phi_R(x) = \{\theta_x\}$ iff $x \notin dom(R)$. Hence Φ_R is non-blocking iff the map R is total on X, and Φ_R is deterministic iff the map R is a partial function.

Example 3. A *differential inclusion* is a structure (X, F) where $X \subseteq \mathbb{R}^n$ is a finite dimensional vector space with the Euclidean norm, and $F : X \rightsquigarrow \mathbb{R}^n$ is a set-valued map. Define $\mathsf{AC}(X) := \{\gamma \in \mathrm{IPath}(\mathbb{R}^+_\circ, X) \mid \gamma$ *absolutely continuous on* $[0, b_\gamma]\}$. Solutions to the inclusion $\dot{x}(t) \in F(x(t))$ starting at a state x are defined by: $\mathsf{Sol}_F(x) := \{\gamma \in \mathsf{AC}(X) \mid \gamma(0) = x \wedge \left(\frac{d}{dt}\gamma\right)(l) \in F(\gamma(l))$ a.e. for $l \in [0, b_\gamma]\}$. It is immediate that Sol_F is reflexive and is suffix-closed and fusion, hence is a general flow system with interval paths over $L = \mathbb{R}^+_\circ$. For the non-blocking property, to ensure the existence of non-trivial solutions from each $x \in \mathrm{cl}(dom(F))$, one needs to impose some regularity assumptions (e.g. *Lipschitz* or *Marchaud* conditions) on the map F [7, 3, 6]. If $F : X \to \mathbb{R}^n$ is actually a function and the differential equation $\dot{x}(t) = F(x(t))$ has a unique maximal solution $\eta : [0, c_x) \to X$ starting from each $x \in X$, with $c_x \in \mathbb{R}^+_\circ \cup \{\infty\}$, then $\mathsf{Sol}_F(x) = \{\eta|_t \mid t \in [0, c_x)\}$ is linearly ordered, hence deterministic at every $x \in X$.

Example 4. A *hybrid automaton* [15, 2, 14, 1] is a structure $H = (Q, E, X, F, D, R)$:

- Q is a finite set of control modes;
- $E : Q \rightsquigarrow Q$ is the discrete transition relation;
- $X \subseteq \mathbb{R}^n$ is the continuous state space;
- $F : Q \to [X \rightsquigarrow \mathbb{R}^n]$ maps each $q \in Q$ to a set-valued vector field $F(q) : X \rightsquigarrow \mathbb{R}^n$ with differential inclusion solution map $\mathsf{Sol}_q := \mathsf{Sol}_{F(q)} : X \rightsquigarrow \mathrm{IPath}(\mathbb{R}^+_\circ, X)$;
- $D : Q \rightsquigarrow X$ maps each $q \in Q$ to a set $D_q := D(q) \subseteq X$, the domain of mode q;
- $R : E \to [X \rightsquigarrow X]$ maps $(q, q') \in E$ to a reset map $R_{q,q'} := R(q, q') : X \rightsquigarrow X$.

Define a map $\mathsf{Traj}_H : (Q \times X) \rightsquigarrow \mathsf{HPath}(Q \times X)$ by:

$$\begin{aligned}
\mathsf{Traj}_H\,(q, x) := \{\, &\gamma \in \mathsf{HPath}(Q \times X) \mid \\
&{\scriptstyle (0)}\ \gamma(0,0) = (q, x) \ \wedge\ (\forall i < \mathrm{dl}(\gamma))\,[\text{ for } \Delta_i := \mathrm{ds}(\gamma)(i) \ \wedge\ q_i := \pi_Q\gamma_i(0) \\
&{\scriptstyle (1)}\ \pi_X\gamma_i \in \mathsf{Sol}_{q_i}(\pi_X\gamma_i(0)) \ \wedge ran(\gamma_i) \subseteq \{q_i\} \times D_{q_i} \ \wedge \\
&{\scriptstyle (2)}\ (q_i, q_{i+1}) \in E \ \wedge\ \pi_X\gamma_{i+1}(0) \in R_{q_i,\,q_{i+1}}\big(\pi_X\gamma_i(\Delta_i)\big) \ \text{ if } i < \mathrm{dl}(\gamma) - 1\,]\,\}
\end{aligned}$$

Paths in Traj_H are called (*finite*) *trajectories* of H. Direct from the definition, we can see that $dom(\mathsf{Traj}_H) = D = \{(q, x) \in Q \times X \mid x \in D_q\}$.

We will say a hybrid automaton H is *well-constituted* if all of the following hold:

(A) $Q \neq \varnothing$, and $E : Q \rightsquigarrow Q$ is total;

(B) $X \subseteq \mathbb{R}^n$ is a non-empty finite dimensional vector space with the Euclidean norm;

(C) $D : Q \rightsquigarrow X$ is total, so $D_q \neq \varnothing$ for each $q \in Q$;
(D) for each $q \in Q$, domain $D_q \subset dom(\mathsf{Sol}_q)$ and Sol_q is not blocked at any $x \in D_q$;
(E) for each transition pair $(q, q') \in E$, the reset relation $R_{q,q'} : X \rightsquigarrow X$ satisfies the constraints $dom(R_{q,q'}) \neq \varnothing$ and $dom(R_{q,q'}) \subseteq D_q$ and $ran(R_{q,q'}) \subseteq D_{q'}$.

Any assumptions will do on the set-valued vector fields $F(q) : X \rightsquigarrow \mathbb{R}^n$, provided they give non-trivial solution paths in Sol_q on the mode domains D_q.

Proposition 5. *Let $H = (\, Q, E, X, F, D, R\,)$ be a hybrid automaton. Then the trajectory map $\mathsf{Traj}_H : (Q \times X) \rightsquigarrow \mathsf{HPath}(Q \times X)$ is a general flow system over $Q \times X$ with time line $\mathbb{N} \times \mathbb{R}^+_\circ$. If H is well-constituted then Traj_H is also prefix-closed.*

The conditions on H being well-constituted rule out all "trivial" ways that Traj_H may become blocked: Sol_q is not blocked at any $x \in D_q \subseteq dom(\mathsf{Sol}_q)$; since E is total, every $q \in Q$ has a discrete successor; and for each discrete transition $(q, q') \in E$, the *transition guard* set $dom(R_{q,q'})$ is non-empty and contained in D_q, and under the reset relation, the image set $ran(R_{q,q'})$ lies in $D_{q'}$. So in attending to the possibility of blocking, we need to focus only on states $x \in D_q$ that are not in any transition guard set, so no discrete transition is possible from (q, x), and states $x \in D_q$ from which every non-trivial q-solution leaves D_q "immediately after now", so there are no hybrid trajectories from (q, x) with non-trivial continuous evolution in mode q.

Proposition 6. *If a hybrid automaton H is well-constituted, and*

$$\begin{aligned} Out_q &:= \big\{ x \in D_q \mid (\forall \gamma \in \mathsf{Sol}_q(x))(\forall t \in dom(\gamma),\, t > 0\,)(\exists s < t)\;\; \gamma(s) \notin D_q \,\big\} \\ Grd_q &:= \textstyle\bigcup_{q' \in E(q)} \; dom(R_{q,q'}) \end{aligned}$$

then Traj_H is non-blocking on its domain D iff $Out_q \subseteq Grd_q$ for each $q \in Q$.

The sets Out_q and the condition $Out_q \subseteq Grd_q$ are identified in [15], for systems with deterministic continuous dynamics. In virtue of the continuity of paths in $\mathsf{Sol}_q(x)$, the set Out_q is contained in the topological boundary: $Out_q \subseteq \mathrm{bd}(D_q) := \mathrm{cl}(D_q) - \mathrm{int}(D_q)$. An immediate corollary is that for well-constituted systems H, Traj_H will be non-blocking on D if for all $q \in Q$, either $(\mathrm{bd}(D_q) \cap D_q) \subseteq Grd_q$, or D_q is open.

We can also show the *impulse differential inclusion* model of hybrid systems from [7] to be an example of a general flow system over the hybrid time line; this example and others will be discussed in a separate paper.

4 Infinitary extensions of general flow systems

From Proposition 4, we know that if a general flow Φ is non-blocking, then for each $x \in dom(\Phi)$ and $\gamma \in \Phi(x)$, there exists an infinite sequence of paths $\{\gamma_n\}$ with $\gamma_0 = \gamma$ and $\gamma_n \in \Phi(x)$ and $\gamma_n < \gamma_{n+1}$ for all n. Motivated by this fact, we view "maximal extensions" or "completions" of paths as infinitary objects, arising as limits of infinite ordered sequences of finitary bounded paths. In this paper, we take limits over ordered sequences of order type (ordinal) ω, the order type of $\mathbb{N}$, but we want to leave open the possibility, for later work, of dealing with sequences of transfinite length, with ordinals greater than ω (for formalizing the notion of a continuation of a Zeno hybrid trajectory that has discrete stages $\omega, \omega+1, \omega+2, \ldots$ up to some limit ordinal $\nu > \omega$). We need access to maximal length paths in order to formalize the *Until* construct in temporal logic, but we also want to "go to infinity" in order to be able to directly compare our class of dynamical systems with those developed in terms of functions over the whole time line $L = \mathbb{N}$ or $L = \mathbb{R}^{+}_{\circ}$; in particular, Aubin's model of an *evolutionary system* [5, 4], and also Willem's *behavioural systems* model [18].

Definition 5. *For any path set $\mathcal{P} \subseteq \mathsf{Path}(L, X)$, define the* ω-extension *of $\mathcal{P}$ by:*

$$\mathsf{Ext}^{\omega}(\mathcal{P}) := \{ \eta : L \dashrightarrow X \mid (\exists\, \overline{\gamma} : \omega \to \mathsf{Path}(L, X))\, (\forall k < \omega)\, [\ \gamma_k := \overline{\gamma}(k) \ \wedge \ \gamma_k \in \mathcal{P} \ \wedge \ \gamma_k < \gamma_{k+1} \ \wedge \ \eta = \textstyle\bigcup_{k<\omega} \gamma_k \ ] \ \}$$

Define $\mathsf{EPath}^{\omega}(L, X) := \mathsf{Ext}^{\omega}(\, \mathsf{Path}(L, X)\,)$*;* $\mathsf{EIPath}^{\omega}(L, X) := \mathsf{Ext}^{\omega}(\, \mathsf{IPath}(L, X)\,)$. *Paths $\eta \in \mathsf{Ext}^{\omega}(\mathcal{P})$ will be called* ω-paths *of $\mathcal{P}$.*

Thus the ω-extension $\mathsf{Ext}^{\omega}(\mathcal{P})$ contains all the partial functions $\eta : L \dashrightarrow X$ that can arise as the union or limit of an ω-length strictly extending sequence of paths in the set $\mathcal{P}$. The path extension ordering $<$ on bounded paths induced by the linear order on L can be lifted to ω-paths. For paths $\eta, \eta' \in \mathsf{Path}(L, X) \cup \mathsf{EPath}^{\omega}(L, X)$, we extend Definition 3 to define $\eta < \eta'$ if $\eta \subset \eta'$ and $t < t'$ for all $t \in dom(\eta)$ and $t' \in dom(\eta') - dom(\eta)$. If $\eta < \eta'$ then $dom(\eta)$ must be a *bounded* subset of L.

For a general flow system, we want to pick out the ω-paths $\eta \in \mathsf{Ext}^{\omega}(\Phi(x))$ that are *maximal* in the sense that there are no real paths of the system in $\Phi(x)$ extending η.

Definition 6. *Given a general flow system $\Phi\colon X \rightsquigarrow \mathsf{Path}(L, X)$, define the* maximized ω-extension *of Φ to be the set-valued map $\mathsf{E}^{\omega}\Phi\colon X \rightsquigarrow \mathsf{EPath}^{\omega}(L, X)$ given by:*

$$(\mathsf{E}^{\omega}\Phi)(x) := \{ \eta \in \mathsf{Ext}^{\omega}(\Phi(x)) \mid (\forall \gamma \in \Phi(x)) \ \ \eta \not< \gamma \}$$

A system Φ will be called ω-extendible *if for every $x \in dom(\Phi)$ and every $\gamma \in \Phi(x)$, there exists $\eta \in (\mathsf{E}^{\omega}\Phi)(x)$ such that $\gamma < \eta$.*

In general, $dom(\mathsf{E}^{\omega}\Phi) \subseteq dom(\Phi)$; Φ is ω-extendible iff $dom(\mathsf{E}^{\omega}\Phi) = dom(\Phi)$. In reasoning about the behaviour of an ω-extendible system Φ, we can safely replace quantification over all possible paths in $\Phi(x)$, with quantification over $(\mathsf{E}^{\omega}\Phi)(x)$, the maximal ω-paths; this is crucial for the semantics of the temporal *Until* construct.

Proposition 7. *For any general flow $\Phi\colon X \rightsquigarrow \mathsf{Path}(L, X)$,*

(1.) *Φ is ω-extendible iff Φ is non-blocking.*

(2.) *If Φ non-blocking, then Φ is deterministic iff $\mathsf{E}^{\omega}\Phi$ is a partial function.*

The non-trivial direction is: Φ is non-blocking implies Φ is ω-extendible; the proof uses Zorn's Lemma to obtain a maximum of any strictly extending sequence of ω-paths.

We are now in a position to formalize the relationship between Aubin's model of an *evolutionary system* [5, 4], and the general flow systems defined here. An evolutionary system, over time lines $L = \mathbb{R}^{+}_{\circ}$ or $L = \mathbb{N}$, is a map $\Psi : X \rightsquigarrow [\, L \to X\,]$ such that, for whole line paths $\eta : L \to X$, $\eta(0) = x$ for all $\eta \in \Psi(x)$ and Ψ is closed under the suffix and fusion operations (the natural extensions to unbounded paths of the operations in Proposition 1), in the same sense as which general flow systems with bounded paths are closed under these operations, as required by clauses **(GF1)** and **(GF2)** of Definition 4.

Proposition 8. *Let the time line be either $L = \mathbb{N}$ or $L = \mathbb{R}^+_\circ$, and $X \neq \varnothing$.*

$\Psi : X \rightsquigarrow [\,L \to X\,]$ *is an evolutionary system in the sense of Aubin*

iff *there exists an interval path general flow system* $\Phi\colon X \rightsquigarrow \mathsf{IPath}(L, X)$ *that is non-blocking and satisfies* $\Psi = \mathsf{E}^\omega \Phi$.

Thus evolutionary systems are a subclass of non-blocking general flow systems. In Willem's *Behavioural Systems* model [18], with time lines $L = \mathbb{N}$ or $L = \mathbb{R}^+_\circ$, a *behaviour* is a set of functions $\mathfrak{B} \subseteq [\,L \to X\,]$. It can also be established that $\mathfrak{B}$ is a time-invariant and complete state behaviour iff there exists an interval path, non-blocking general flow system $\Phi\colon X \rightsquigarrow \mathsf{IPath}(L, X)$ such that $\mathfrak{B} = ran(\mathsf{E}^\omega \Phi)$.

When $L = \mathbb{N}$, then all ω-paths $\eta \in \mathsf{EPath}^\omega(\mathbb{N}, X)$ have infinite time domain, so we will always have $(\mathsf{E}^\omega \Phi)(x) = \mathsf{Ext}^\omega(\Phi(x))$ for any non-blocking general flow Φ.

When $L = \mathbb{R}^+_\circ$, we know that every ω-path $\eta \in \mathsf{EIPath}^\omega(\mathbb{R}^+_\circ, X)$ must have $dom(\eta) = [0, c)$ for some $c \in \mathbb{R}^+_\circ \cup \{\infty\}$. For a non-blocking flow Φ, suppose $\eta \in \mathsf{Ext}^\omega(\Phi(x))$ is any ω-path. Then $c = \infty$ automatically gives $\eta \in (\mathsf{E}^\omega \Phi)(x)$. If $c < \infty$, then we will have a maximally extended ω-path $\eta \in (\mathsf{E}^\omega \Phi)(x)$ exactly when $\eta|_t \in \Phi(x)$ for all $t \in [0, c)$ but the limit as $t \to c$ of $\eta(t)$ does not exist, or does exist but is not in $dom(\Phi)$; i.e. η has *finite escape time*. The analysis for the ω-extensions of general bounded paths $\eta \in \mathsf{EPath}^\omega(\mathbb{R}^+_\circ, X)$ is similar. For the differential inclusion systems in *Example 3*, the Marchaud conditions on F in [3,7] constitute a property stronger than non-blocking: they imply that $dom(\eta) = [0, \infty)$ for all $\eta \in (\mathsf{E}^\omega \mathsf{Sol}_F)(x)$, so there are no ω-paths with finite escape time.

When $L = \mathbb{N} \times \mathbb{R}^+_\circ$ is the hybrid time line, we can characterize the maximal ω-paths of a non-blocking system as follows.

Proposition 9. *For any $X \neq \varnothing$ and non-blocking general flow $\Phi : X \rightsquigarrow \mathsf{HPath}(X)$, every ω-path $\eta \in (\mathsf{E}^\omega \Phi)(x)$ is of one of two forms:*
(i) *$\eta = \gamma * \upsilon$ where $\gamma \in \Phi(x)$ and $\upsilon : \{0\} \times [0, c) \to X$ with $c \in \mathbb{R}^+_\circ \cup \{\infty\}$ and $\upsilon = \bigcup_{n<\omega} \gamma_n$ and each $\gamma_n \in \Phi(\upsilon(0,0))$ has $\mathrm{dl}(\gamma_n) = 1$, hence η has finite discrete length $\mathrm{dl}(\eta) = \mathrm{dl}(\gamma) \in \mathbb{N}$, and total duration $\mathrm{td}(\eta) = \mathrm{td}(\gamma) + c$, which may be finite or infinite, depending on c; or*
(ii) *$\eta = \bigcup_{n<\omega} \gamma_n$ where $\mathrm{dl}(\gamma_n) < \mathrm{dl}(\gamma_{n+1})$, hence η has infinite discrete length, and total duration $\mathrm{td}(\eta) = \sum_{n<\omega} \mathrm{td}(\gamma_n)$, which may be finite or infinite;*

The non-blocking/ω-extendibility property here allows for two cases among extensions of hybrid paths that are typically considered "pathological": *Zeno* extended hybrid paths $\eta \in (\mathsf{E}^\omega \Phi)(x)$ that have infinite discrete length but finite total duration $\mathrm{td}(\eta) < \infty$; and *livelocked* extended hybrid paths $\eta \in (\mathsf{E}^\omega \Phi)(x)$ that have finite discrete length $\mathrm{dl}(\eta) = k + 1$ *and* finite total duration. Livelocked η are maximal with the last path segment having $dom(\eta_k) = [0, c)$; this Φ path would "die" at k-local time $t = c$ (hybrid time (k, c)) if it ever got there, but it never can, as for every extension of η_k to domain $[0, c]$, the resulting hybrid path is not in $\Phi(x)$. For a non-blocking hybrid automaton H, the general flow Traj_H will exhibit livelock on an extended trajectory $\eta \in (\mathsf{E}^\omega \mathsf{Traj}_H)(x)$ with $\mathrm{dl}(\eta) = k + 1$ iff the last path segment $\eta_k : [0, c) \to (Q \times X)$ is such that, for $q_k := \pi_Q \eta_k(0)$ and $x_k := \pi_X \eta_k(0)$, there exists a solution path $\gamma \in \mathsf{Sol}_{q_k}(x_k)$ such that $dom(\gamma) = [0, b_\gamma]$, with $b_\gamma > c$ and

$\gamma\restriction_{[0,c)} = \pi_X \eta_k$, that eventually leaves the mode domain D_q, but never passes through Grd_q on the way: $\gamma(c) \notin D_q$ and $\gamma(t) \in D_q - Grd_q$ for all $t \in [0, c)$.

5 Full General Flow Logic GFL*: syntax and semantics

We now turn to the syntax and semantics of a logic we call *Full General Flow Logic*, **GFL***, which generalizes to general flow models the semantics of *Full Computation Tree Logic*, **CTL***, introduced by Emerson and Halpern in 1983 [10] for formalizing reasoning about executions of concurrent programs in discrete time. The syntax here is a labelled variant of that of **CTL***, allowing for semantic models consisting of a finite family of non-blocking general flow systems.

Definition 7. *A* signature *is a pair $\Sigma = (\mathrm{Sys}, \mathrm{Prp})$, where* Sys *is a finite set of system labels, and* Prp *is a countable set of atomic propositions. The temporal logic language $\mathcal{L}(\Sigma)$ consists of the set of all formulae φ generated by the grammar:*

$$\varphi \ ::= \ p \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \,\mathcal{U}_a\, \varphi_2 \mid \forall_a \varphi$$

for atomic propositions $p \in \mathrm{Prp}$, and system labels $a \in \mathrm{Sys}$.

The other propositional (Boolean) connectives and logical constants *true*, $\top$, and *false*, $\bot$, are defined in a standard way, and the path quantifiers $\forall_a$ have classical negation duals $\exists_a$, as follows:

$$\begin{aligned} \varphi_1 \wedge \varphi_2 &\stackrel{\text{def}}{=} \neg(\neg\varphi_1 \vee \neg\varphi_2) & \varphi_1 \to \varphi_2 &\stackrel{\text{def}}{=} \neg\varphi_1 \vee \varphi_2 \\ \varphi_1 \leftrightarrow \varphi_2 &\stackrel{\text{def}}{=} (\varphi_1 \to \varphi_2) \wedge (\varphi_2 \to \varphi_1) & \exists_a\varphi &\stackrel{\text{def}}{=} \neg\forall_a\neg\varphi \\ \top &\stackrel{\text{def}}{=} p \vee \neg p \quad \text{for any } p \in \mathrm{Prp} & \bot &\stackrel{\text{def}}{=} \neg\top \end{aligned} \tag{2}$$

The temporal operators, $\mathcal{U}_a$, for $a \in \mathrm{Sys}$, refer to the ω-path space of a non-blocking general flow system Φ_a. The formula $\varphi\mathcal{U}_a\psi$, read "φ *until* ψ, for a-type paths", will hold along any ω-path η of type a if at some time in the future (along η) the formula ψ holds, and at all intermediate times (along η) between now and then, φ holds. The universal quantifier $\forall_a$ applied to a path formula produces a state formula, and $\forall_a(\varphi\mathcal{U}_a\psi)$ holds at a state x if *every* ω-path $\eta \in (\mathsf{E}^\omega\Phi_a)(x)$ satisfies the path formula $\varphi\mathcal{U}_a\psi$. Dually, $\exists_a(\varphi\mathcal{U}_a\psi)$ holds at a state x if *there exists* an ω-path $\eta \in (\mathsf{E}^\omega\Phi_a)(x)$ which satisfies the path formula $\varphi\mathcal{U}_a\psi$. The *until* construct on paths can be formulated in several distinct ways; we shall take as primitive the *strictest* version of *until*, and then define weaker variants in terms of it. In particular, an important *difference* between the logic here, and the usual presentation of **CTL*** developed for discrete time paths, is that instead of taking the *next-time* discrete successor operator as a syntactic and semantic primitive, we use a known method to *define* next-time in terms of the strictest *until* [8, 13]. Our semantics covers arbitrary time lines, so in general the immediate successor map is only a partial function on the domain of a path, and in the case of interval paths in a dense time line, may be everywhere undefined.

Definition 8. *A* general flow logic model *(*logic model*, for short) of signature $\Sigma = (\mathrm{Sys}, \mathrm{Prp})$ is a structure $\mathfrak{M} = (X, \mathfrak{L}, \mathfrak{S}, \mathfrak{P})$, where:*

- $X \neq \varnothing$ *is the state space, of arbitrary cardinality;*
- $\mathcal{L}$ *is a function mapping each symbol* $a \in \mathrm{Sys}$ *to a time line* $L_a := \mathcal{L}(a)$*;*
- $\mathcal{S}$ *is a function mapping each symbol* $a \in \mathrm{Sys}$ *to an non-blocking general flow system* $\Phi_a := \mathcal{S}(a) : X \rightsquigarrow \mathsf{Path}(L_a, X)$ *over the space* X*, with time line* L_a*;*
- $\mathcal{P} : \mathrm{Prp} \rightsquigarrow X$ *maps each* $p \in \mathrm{Prp}$ *to a set* $\mathcal{P}(p) \subseteq X$ *of states.*

The ω-path space *of a model* $\mathfrak{M}$ *is defined by* $\mathsf{EPath}(\mathfrak{M}) := \bigcup_{a \in \mathrm{Sys}} \mathsf{EPath}^{\omega}(L_a, X)$.

Let $\mathbb{GF}(\Sigma)$ denote the class of all general flow logic models of signature Σ, and for the case of a single time line L, let $\mathbb{GF}(L, \Sigma)$ denote the subclass of all logic models $\mathfrak{M}$ such that $\mathcal{L}(a) = L$ for all $a \in \mathrm{Sys}$. For the further special case where $|\mathrm{Sys}| = 1$ and Prp is countably infinite, let $\mathbb{TR}(\mathbb{N})$ denote the subclass of all discrete time logic models $\mathfrak{M}$ with one general flow $\Phi_R : X \rightsquigarrow \mathsf{IPath}(\mathbb{N}, X)$ from a total transition relation $R : X \rightsquigarrow X$ (also called *R-generable models* [12, 10, 16]). For the case of deterministic systems, let $\mathbb{DF}(L)$ denote the subclass of all logic models where the time line L is the non-negative half of a linearly ordered abelian group, and the one general flow $\Phi : X \rightsquigarrow \mathsf{IPath}(L, X)$ is deterministic, total, interval path, and non-blocking [9].

Definition 9. *For* $\varphi \in \mathcal{L}(\Sigma)$ *and* ω*-path* $\eta \in \mathsf{EPath}(\mathfrak{M})$*, the relation "*$\psi$ is satisfied along path η in model $\mathfrak{M}$*", written* $\mathfrak{M}, \eta \models \psi$*, is defined by induction on the structure of formulae, with* $p \in \mathrm{Prp}$ *and* $a \in \mathrm{Sys}$*:*

$$
\begin{array}{lll}
\mathfrak{M}, \eta \models p & \text{iff} & \eta(0) \in \mathcal{P}(p) \\
\mathfrak{M}, \eta \models \neg \psi & \text{iff} & \mathfrak{M}, \eta \not\models \psi \\
\mathfrak{M}, \eta \models \psi_1 \vee \psi_2 & \text{iff} & \mathfrak{M}, \eta \models \psi_1 \ \text{ or } \ \mathfrak{M}, \eta \models \psi_2 \\
\mathfrak{M}, \eta \models \psi_1 \, \mathcal{U}_a \, \psi_2 & \text{iff} & \eta \in \mathsf{EPath}^{\omega}(L_a, X) \ \text{ and } \ \exists\, t \in \mathit{dom}(\eta) \ \text{ with } \ t > 0 \ : \\
 & & \mathfrak{M}, {}_t|\eta \models \psi_2 \ \text{ and } \ \forall s \in (0, t) \cap \mathit{dom}(\eta) : \ \mathfrak{M}, {}_s|\eta \models \psi_1 \\
\mathfrak{M}, \eta \models \forall_a \, \psi & \text{iff} & \forall \xi \in (\mathsf{E}^{\omega} \Phi_a)(\eta(0)) : \ \mathfrak{M}, \xi \models \psi
\end{array}
$$

For formulas $\varphi \in \mathcal{L}(\Sigma)$*, the* ω-path denotation set $[\![\, \varphi \,]\!]^{\mathfrak{M}} \subseteq \mathsf{EPath}(\mathfrak{M})$*, and the* state denotation set $[\![\, \varphi \,]\!]^{\mathfrak{M}}_{\mathsf{st}} \subseteq X$*, are defined by:*

$$
\begin{aligned}
[\![\, \varphi \,]\!]^{\mathfrak{M}} &:= \{\, \eta \in \mathsf{EPath}(\mathfrak{M}) \ | \ \mathfrak{M}, \eta \models \varphi \,\} \\
[\![\, \varphi \,]\!]^{\mathfrak{M}}_{\mathsf{st}} &:= \{\, x \in X \ | \ \exists \eta \in \mathsf{EPath}(\mathfrak{M}) \ : \ \mathfrak{M}, \eta \models \varphi \ \textit{ and } \ x = \eta(0) \,\}
\end{aligned}
$$

For a logic model $\mathfrak{M} \in \mathbb{GF}(\Sigma)$*, class of logic models* $C \subseteq \mathbb{GF}(\Sigma)$*, and for formulas* $\varphi \in \mathcal{L}(\Sigma)$*, we say:*
- φ *is* satisfiable *in* $\mathfrak{M}$*, if* $[\![\, \varphi \,]\!]^{\mathfrak{M}}_{\mathsf{st}} \neq \varnothing$*;*
- φ *is* true *in* $\mathfrak{M}$*, written* $\mathfrak{M} \models \varphi$*, if* $\mathfrak{M}, \eta \models \varphi$ *for every* $\eta \in \mathsf{EPath}(\mathfrak{M})$*;*
- φ *is* C-valid*, written* $\models_C \varphi$*, if* $\mathfrak{M} \models \varphi$ *for every* $\mathfrak{M} \in C$*.*

Define $\mathbf{Valid}(C) := \{\psi \in \mathcal{L}(\Sigma) \mid \ \models_C \psi \,\}$ *to be the set of all* C*-valid formulas, and define* $\mathbf{CTL}^{\star} := \mathbf{Valid}(\, \mathbb{TR}(\mathbb{N}) \,)$ *and* $\mathbf{GFL}^{\star} := \mathbf{Valid}(\, \mathbb{GF}(\Sigma) \,)$.

The *while...always* operator is a negation dual of *until*: $\varphi \, \mathcal{A}_a \, \psi \ \stackrel{\text{def}}{=} \ \neg(\varphi \, \mathcal{U}_a \, (\neg \, \psi))$, which can be read as "if a type-a path, then *while* φ, *always* ψ". The semantics are:

$$
\begin{array}{lll}
\mathfrak{M}, \eta \models \varphi \, \mathcal{A}_a \, \psi & \textit{iff} & \text{if } \ \eta \in \mathsf{EPath}^{\omega}(L_a, X) \ \text{ then } \ \forall\, t \in \mathit{dom}(\eta) \ \text{ with } \ t > 0 \,, \\
 & & \text{if } \ (\forall s \in (0, t) \cap \mathit{dom}(\eta)) \ \mathfrak{M}, {}_s|\eta \models \varphi \quad \text{then } \ \mathfrak{M}, {}_t|\eta \models \psi
\end{array}
$$

Other one-place operators are defined as $\Diamond_a \varphi \stackrel{\text{def}}{=} \top \mathcal{U}_a \varphi$, $\Box_a \varphi \stackrel{\text{def}}{=} \top \mathcal{A}_a \varphi$, $\odot_a \varphi \stackrel{\text{def}}{=} \bot \mathcal{U}_a \varphi$, and $\circledcirc_a \varphi \stackrel{\text{def}}{=} \neg\varphi \mathcal{A}_a \bot$, where

- $\Diamond_a \varphi$ type-a paths along which φ will *eventually* be true in the *future*;
- $\Box_a \varphi$ type-a paths along which φ will *always* be true in the *future*, plus non-type-a paths;
- $\odot_a \varphi$ type-a paths along which time 0 has a discrete successor, and φ is true *then*;
- $\circledcirc_a \varphi$ type a-paths along which φ is true *immediately after now*, plus non-type-a paths.

In particular, the *next-time* operators, $\odot_a$, come out as: $\mathfrak{M}, \eta \models \odot_a \varphi$ *iff*

for $T := dom(\eta)$ and $0 \in dom(\mathbf{succ}_T)$ and $k := \mathbf{succ}_T(0)$ and $\mathfrak{M},\ {}_k|\eta \models \varphi$

Different versions of *until* come by varying the constraints on end-values of the bounded paths that satisfy φ until they satisfy ψ :

$$\varphi \mathcal{U}_a^{\bullet\bullet} \psi \stackrel{\text{def}}{=} \varphi \wedge \varphi \mathcal{U}_a(\varphi \wedge \psi) \qquad \varphi \mathcal{U}_a^{\bullet\circ} \psi \stackrel{\text{def}}{=} \varphi \wedge \varphi \mathcal{U}_a \psi \tag{3}$$

We briefly illustrate the expressivity of the logic in two areas.

***Viability Theory*:** In the recent work of Aubin and co-workers in *Viability Theory* [3, 7, 4], the key concept is of paths being "*viable in K until capturing target C*". Define:

$$\varphi \mathcal{V}_a \psi \stackrel{\text{def}}{=} (\top \mathcal{U}_a \top \ \wedge\ \varphi\ \wedge\ \Box_a \varphi\ \wedge\ \Box_a \Diamond_a \top)\ \vee\ \varphi \mathcal{U}_a^{\bullet\bullet} \psi \tag{4}$$

The formula $\varphi \mathcal{V}_a \psi$ is satisfied by an ω-path $\eta \in \mathsf{EPath}^\omega(L_a, X)$ iff *either* φ is true now and at all times in the future along η, and the time domain of η is unbounded, *or* there is a finite time along η at which ψ becomes true, and φ is true at all times between now and then (inclusive). Thus η is either *viable forever in the set* $[\![\varphi]\!]^{\mathfrak{M}}$ or *viable in* $[\![\varphi]\!]^{\mathfrak{M}}$ *until it captures the target set* $[\![\psi]\!]^{\mathfrak{M}}$ in finite time. Applying the path quantifiers $\exists_a$ and $\forall_a$ restricts to ω-paths of the system $\mathsf{E}^\omega \Phi_a$, and this can be used to formalize in the logic the two-place state set operators known as the *viability kernel with target* and the *invariance kernel with target*.

***Dynamical properties of hybrid automata*:** Given a hybrid automaton H, assume that H is well- constituted, and define a logic model $\mathfrak{M}_X^H$ with state space $X \subseteq \mathbb{R}^n$ the continuous state space of H. Let the system label set $\mathrm{Sys}_X^H := Q$, and for each $q \in Q$, the time line is $\mathcal{L}(q) := \mathbb{R}_\circ^+$ and the general flow systems are $\mathcal{S}(q) = \Phi_q := \mathsf{Sol}_q$. Assume the atomic proposition set Prp^H includes constants $\mathtt{D}_q$ and $\mathtt{G}_q$ for each $q \in Q$, and the valuation $\mathcal{P} : \mathrm{Prp}^H \rightsquigarrow X$ satisfies $\mathcal{P}(\mathtt{D}_q) = D_q$, and $\mathcal{P}(\mathtt{G}_q) = Grd_q$.

- Traj_H is non-blocking iff $\mathfrak{M}_X^H \models \bigwedge_{q \in Q} ((\circledcirc_q \neg \mathtt{D}_q) \to \mathtt{G}_q)$
- If Traj_H is non-blocking, then Traj_H has no livelock iff
$$\mathfrak{M}_X^H \models \bigwedge_{q \in Q} \forall_q ((\mathtt{D}_q \wedge \Diamond_q \neg \mathtt{D}_q) \to (\mathtt{D}_q \mathcal{U}_q (\mathtt{G}_q \wedge \Diamond_q \neg \mathtt{D}_q)))$$

We can, of course, also form a logic model $\mathfrak{M}^H$ with state space $Q \times X$, and have a single system label $\mathrm{Sys}^H := \{0\}$ with the general flow system $\Phi_0 := \mathsf{Traj}_H$, and formalize with the operators $\mathcal{U}_0$ and $\forall_0$ quite sophisticated temporal and dynamic properties of H as a single system. We can also reason about multiple systems over a common state space, and express comparative properties.

Definition 10. *Given a class of logic models $C \subseteq \mathbb{GF}(\Sigma)$, the* validity problem for C *is to determine, for any given formula $\varphi \in \mathcal{L}(\Sigma)$, whether or not $\varphi \in \mathbf{Valid}(C)$. The validity problem for C is* decidable *if there is a recursive procedure for determining membership of $\mathbf{Valid}(C)$ that finitely terminates on all input formulae $\varphi \in \mathcal{L}(\Sigma)$.*

Proposition 10. [12, 11] *The validity problem is decidable $\mathbf{CTL}^\star$ (the class $\mathbb{TR}(\mathbb{N})$ of discrete time models), with complexity double exponential time in the length of the formula.*

We conjecture that the validity problem is decidable for the class $\mathbb{DF}(\mathbb{R}^+_\circ)$ of deterministic, total, interval path, non-blocking flows described by functions $\phi : X \times \mathbb{R} \to X$ satisfying the group action laws. These models are studied in [9], where they are used to give semantics for *until* and *since* (the time-reversal or past tense correlate) in the language of *Linear Temporal Logic* ($\mathbf{LTL}$), with no path quantifiers, and the validity problem for that logic is decidable.

6 Axiomatisation and soundness

We seek formal deductive proof systems for $\mathbf{GFL}^\star := \mathbf{Valid}(\mathbb{GF}(\Sigma))$, or for the validity set of distinguished subclasses of general flow models. The *soundness* or *adequacy* of a proof system Λ for a semantically characterized formula set such as $\mathbf{GFL}^\star$, is the property that if φ is provable in Λ, then $\varphi \in \mathbf{GFL}^\star$. For soundness proofs, the larger the class of semantic models, the stronger the result (so we do rather well here on that score). The technically much more challenging task is to establish *completeness* of a proof system Λ, which in our case is the property: if $\varphi \in \mathbf{GFL}^\star$, then φ is provable in Λ. Proofs of completeness proceed via the contrapositive, and in that form, are essentially a *model realization problem*: if φ is *Λ-consistent* (i.e. the formula $\neg\varphi$ is *not* provable in Λ), then there exists a logic model $\mathfrak{M} \in \mathbb{GF}(\Sigma)$ in which φ is satisfiable. Generally speaking, the smaller the class from which the realization models are drawn, the stronger or tighter the completeness result.

An axiomatic proof system Λ consists of a recursive list of *axioms*, usually given by taking all instances in the language of some finite set of *formula schemes*, together with a finite list of *inference rules*, of the form: **if** φ is provable in Λ, **then** ψ is provable in Λ. A formula is provable in Λ if it is an axiom of Λ or is derivable from provable formulas by a finite sequence of applications of inference rules. We write $\vdash_\Lambda \varphi$ to mean that φ is provable in the system Λ.

A sound and complete axiomatic proof system for the logic $\mathbf{CTL}^\star$ remained an open problem for almost 20 years, and was solved by Reynolds quite recently [16]. That axiomatization lays side by side a list of axioms for path formulae, obtained from axiomatizing $\mathbf{LTL}$ together with a list of axioms for universal quantification over paths. In addition, Reynolds' proof system includes the axiom $\bot\mathcal{U}\top$, which asserts that the underlying time line is discrete, or equivalently, the discrete successor map is total. It also includes an additional inference rule, which is an *induction rule* for "recursively unwinding" *Until* formulae in terms of the *next-time* operator. The axiomatic proof system we present for $\mathbf{GFL}^\star$ consists of Reynolds' system for $\mathbf{CTL}^\star$, *minus* those last two "discrete" items, the axiom and rule.

Let Λ be the proof system having as axioms all formulae of $\mathcal{L}$(Sig) that are instances of propositional tautologies, or are instances of the schemes **(P1)** – **(P6)** and **(Q1)** – **(Q5)** below, and having as rules of inference the propositional rule of *Modus Ponens* (**MP**) along with three monotonicity rules:

$$
\begin{array}{llll}
(\mathbf{Mono}\mathcal{U}\textbf{-1}): & \textbf{if } \vdash_\Lambda \varphi_1 \to \varphi_2 & \textbf{then } \vdash_\Lambda \varphi_1 \mathcal{U}_a \psi \to \varphi_2 \mathcal{U}_a \psi \\
(\mathbf{Mono}\mathcal{U}\textbf{-2}): & \textbf{if } \vdash_\Lambda \psi_1 \to \psi_2 & \textbf{then } \vdash_\Lambda \varphi \mathcal{U}_a \psi_1 \to \varphi \mathcal{U}_a \psi_2 \\
(\mathbf{Mono}\forall): & \textbf{if } \vdash_\Lambda \varphi \to \psi & \textbf{then } \vdash_\Lambda \forall_a \varphi \to \forall_a \psi
\end{array}
$$

$$
\begin{array}{lrcl}
\textbf{(P1):} & & & \bigvee_a (\top \mathcal{U}_a \top) \\
\textbf{(P2):} & & & \neg(\top \mathcal{U}_a \bot) \\
\textbf{(P3):} & (\varphi \mathcal{U}_a \psi_1 \wedge \neg(\varphi \mathcal{U}_a \psi_2)) & \to & \varphi \mathcal{U}_a (\psi_1 \wedge \neg \psi_2) \\
\textbf{(P4):} & (\varphi_1 \mathcal{U}_a \psi \wedge \neg(\varphi_2 \mathcal{U}_a \psi)) & \to & \varphi_1 \mathcal{U}_a (\varphi_1 \wedge \neg \varphi_2 \wedge \varphi_1 \mathcal{U}_a \psi) \\
\textbf{(P5):} & \varphi \mathcal{U}_a \psi & \to & (\varphi \wedge \varphi \mathcal{U}_a \psi) \mathcal{U}_a \psi \\
\textbf{(P6):} & \varphi \mathcal{U}_a (\varphi \wedge \varphi \mathcal{U}_a \psi) & \to & \varphi \mathcal{U}_a \psi \\
\textbf{(P7):} & (\varphi_1 \mathcal{U}_a \psi_1 \wedge \varphi_2 \mathcal{U}_a \psi_2) & \to & ((\varphi_1 \wedge \varphi_2) \mathcal{U}_a (\psi_1 \wedge \psi_2) \\
 & & & \vee (\varphi_1 \wedge \varphi_2) \mathcal{U}_a (\varphi_2 \wedge \psi_1) \\
 & & & \vee (\varphi_1 \wedge \varphi_2) \mathcal{U}_a (\varphi_1 \wedge \psi_2)) \\
\textbf{(Q1):} & & & \forall_a \top \\
\textbf{(Q2):} & \forall_a (\varphi \wedge \psi) & \to & (\forall_a \varphi \wedge \forall_a \psi) \\
\textbf{(Q3):} & \forall_a \varphi & \to & \forall_a \forall_a \varphi \\
\textbf{(Q4):} & \forall_a \varphi & \to & \varphi \\
\textbf{(Q5):} & \varphi & \to & \forall_a \exists_a \varphi
\end{array}
$$

Proposition 11. (Soundness of Axiomatisation) *For every formula $\varphi \in \mathcal{L}$(Sig),*

$$\vdash_\Lambda \varphi \qquad \Rightarrow \qquad \varphi \in \mathbf{GFL}^\star$$

The verification of soundness of an axiom scheme φ consists of showing that $\mathfrak{M} \models \varphi$ for every model $\mathfrak{M} \in \mathbb{GF}(\Sigma)$, and for an inference rule of the form **if** $\vdash_\Lambda \varphi$ **then** $\vdash_\Lambda \psi$, one needs to show that if $\mathfrak{M} \models \varphi$, then $\mathfrak{M} \models \psi$, for all models $\mathfrak{M} \in \mathbb{GF}(\Sigma)$.

We give some verbal explanation for a selection of the axioms. The first axiom, **(P1)**, asserts that the union over a of all type-a paths is equal to the whole ω-path space of the model. To understand **(P5)**, suppose γ is an a-path satisfying $\varphi \mathcal{U}_a \psi$. Then there must be some positive time t along γ at which the suffix path ${}_t|\gamma$ satisfies ψ and at all strictly intermediate points along γ the suffix paths satisfy φ. In particular at all those strictly intermediate points, the suffix paths satisfy φ and $\varphi \mathcal{U}_a \psi$, meaning that γ satisfies $(\varphi \wedge \varphi \mathcal{U}_a \psi) \mathcal{U}_a \psi$. The axiom **(P6)** is sound because of the fusion closure of the ω-path space since the antecedent contains embedded *Until* operators. The axioms **(Q1-Q5)** all follow directly from the meaning of the universal (and existential) quantification. The three rules all express the monotonicity of the operators with respect to subset inclusion.

7 Summary and discussion

In this paper, we propose and develop a quite general class of dynamical system models we call *general flow systems* which include and extend the broad class of evolutionary systems identified by Aubin, and the complete state behaviours of Willems. The advance specifically consists in modelling *hybrid time paths* as entities in their own right. We take the syntactic constructs of the non-deterministic and branching temporal logic $\mathbf{CTL}^\star$ originally developed for discrete time models, and re-interpret them in a semantics over general flow systems and with respect to arbitrary time lines. We propose a first candidate for an axiomatic proof system for the class of general flow models, and establish the soundness or adequacy of the proof system.

References

1. R. Alur, T.A. Henzinger, and P.-H. Ho. Automatic symbolic verification of embedded systems. *IEEE Transactions on Software Engineering*, 22:181–201, 1996.
2. R. Alur, T.A. Henzinger, G. Lafferriere, and G. Pappas. Discrete abstractions of hybrid systems. *Proceedings of the IEEE*, 88, July 2000.
3. J.-P. Aubin. Viability kernels and capture basins of sets under differential inclusions. *Siam Journal of Control*, 40:853–881, 2001.
4. J.-P. Aubin. Viability kernels and capture basins: Lecture notes. Technical report, Universidad Politecnica de Cartagena, Spain, April-May 2002.
5. J.-P. Aubin and O. Dordan. Dynamical qualitative analysis of evolutionary systems. In *Hybrid Systems: Computation and Control*, LNCS 2289, pages 62–75. Springer-Verlag, 2002.
6. J.-P. Aubin and H. Frankowska. *Set-Valued Analysis*. Birkhauser, Boston, 1990.
7. J.-P. Aubin, J. Lygeros, M. Quincampoix, S. Sastry, and N. Seube. Impulse differential inclusions: A viability approach to hybrid systems. *IEEE Transactions on Automatic Control*, 47:2–20, 2002.
8. J.P. Burgess. Axioms for tense logic I: "Since" and "Until". *Notre Dame Journal of Formal Logic*, 23:367–374, 1982.
9. V. Coulthard. *Temporal Logics of Dynamical Systems in Discrete and Dense Time*. PhD thesis, RSISE, The Australian National University, 2004. In preparation.
10. E.A. Emerson and J.Y. Halpern. "Sometimes" and "Not Never" revisited: on branching versus linear time. *Journal of the Association of Computing Machinery*, 33:151–178, 1986.
11. E.A. Emerson and C. Jutla. Complexity of tree automata and modal logics of programs. In *Proc. 29th IEEE Foundations of Computer Science (FOCS'88)*. IEEE, 1988.
12. E.A. Emerson and A. Sistla. Deciding Full Branching Time Logic. *Information and Control*, 61:175–201, 1984.
13. D.M. Gabbay, I. Hodkinson, and M. Reynolds. *Temporal Logic: Mathematical Foundations and Computational Aspects, Volume 1*. Clarendon Press, Oxford, 1994.
14. T.A. Henzinger. The theory of hybrid automata. In *Proc. of 11th Annual IEEE Symposium on Logic in Computer Science*, pages 278–292, 1996.
15. J. Lygeros, K.H. Henrik, S.N. Simić, and S.S. Sastry. Dynamical properties of hybrid automata. *IEEE Transactions on Automatic Control*, 48:2–17, 2003.
16. M. Reynolds. An Axiomatization of Full Computation Tree Logic. *J. Symbolic Logic*, 66:1011–1057, 2001.
17. C. Stirling. Modal and temporal logics. In *Handbook of Logic in Computer Science*, volume 2, pages 477–563. Oxford University Press, 1992.
18. J.C. Willems. Paradigms and puzzles in the theory of dynamical systems. *IEEE Transactions on Automatic Control*, 36:259–294, 1991.