On simulations and bisimulations of general flow systems*

J.M. Davoren[1] and Paulo Tabuada[2]

[1] Department of Electrical & Electronic Engineering
The University of Melbourne, VIC 3010 AUSTRALIA
davoren@unimelb.edu.au
[2] Department of Electrical Engineering
The University of California at Los Angeles, CA 90095 USA
tabuada@ee.ucla.edu

Abstract. We introduce a notion of bisimulation equivalence between general flow systems, which include discrete, continuous and hybrid systems, and compare it with similar notions in the literature. The interest in the proposed notion is based on our main result, that the temporal logic $\mathbf{GFL}^\star$ – an extension to general flows of the well-known computation tree logic $\mathbf{CTL}^\star$ – is semantically preserved by this equivalence.

1 Introduction

There is growing interest in the study of simulation and bisimulation relationships within general classes of dynamical and control systems including hybrid systems [1–6]. A core motivation is the potential for using these relationships, whenever they preserve significant structural and behavioral properties, as a means to reduce complexity in the analysis and design of systems.

In this paper, we define a notion of bisimulation equivalence that is sufficient to preserve the semantics of the general flow logic $\mathbf{GFL}^\star$, introduced in [7], and thus to preserve all system properties expressible in that logic. $\mathbf{GFL}^\star$ extends the discrete-time semantics of the well-known temporal logic $\mathbf{CTL}^\star$ to the class of *general flow systems* [7], which offer a unified treatment of discrete-time transition systems, continuous-time differential inclusions, hybrid-time systems such as hybrid automata and stochastic hybrid systems, as well as more complex systems requiring higher-dimensional time lines; e.g., a "meta-hybrid automaton" as a finite state machine with a hybrid automaton at each discrete state [8].

The framework of general flow systems is given in general set-theoretic terms, and builds on the notion of a *time line* as a suitably structured linear order, and of *finite paths* as functions from bounded and finite-duration subsets of a time line into some value space. A general flow system Φ over a state space X associates with each initial state $x \in X$ the set $\Phi(x)$ of all possible finite paths or trajectories starting from x, and satisfies a generalized version of the *semigroup*

* First author partially supported by Australian Research Council grant DP0208553; second author partially supported by NSF CAREER award 0446716.

property or "Axiom of State" from *Behavioural Systems theory* [9]. The system class is essentially Aubin's model of an *Evolutionary System* [10], generalized from discrete or continuous time to arbitrary time lines, and "deconstructed", so that the basic objects are finite, bounded duration paths, rather than functions from the whole time line. In moving to the hybrid time line, this perspective simply fails to transfer: if we take the limit of any infinite sequence of longer and longer finite hybrid trajectories, then we do not end up with a function defined on the whole hybrid time line, but rather with a function whose time domain is the union of a finite or infinite sequence of disjoint intervals, separated by infinite gaps in the time line. Revising the treatment in [7, 11], we develop a theory of *maximal extensions* of finite paths by taking the limit of infinite sequences of longer and longer finite paths, where those sequences are indexed by transfinite ordinals, up to the ordinal length of the underlying time line (so in the case of continuous or hybrid time, up to the ordinal of the cardinality of the continuum). The payoff from this apparent transfinite generosity is the crucial equivalence, expressed in Theorem 1, between the finitary system property of being deadlock-free or non-blocking, and the infinitary property of being maximally extendible, in the sense that every finite path of the system has a maximal extension.

The maximal extension property is essential for the semantics of the logic $\mathbf{GFL}^\star$, which straight-forwardly generalize the semantics of the logic $\mathbf{CTL}^\star$ with respect to ω-length execution sequences of non-blocking transition systems or state machines, with the singular and crucial exception of the *next-time* operator. To cover general time lines, we introduce a generalized *next-times* operator that behaves as the discrete successor if there is one, and otherwise, in the presence of a dense sub-interval of time, has the meaning "*immediately after now*". This operator is also a key ingredient in our new notions of simulation and bisimulation, and in our semantic preservation theorem for the logic $\mathbf{GFL}^\star$.

The body of the paper is organized as follows. Section 2 consists of preliminary theory of time lines and paths. Section 3 briefly reviews general flow systems and develops the theory of maximal extensions. In Section 4, we give three, progressively stronger, concepts of simulation and bisimulation between general flow systems, allowing *differing* time lines in the systems compared for the first two of these. The new notion we call *p-simulation* is strictly intermediate between two other concepts of simulation found in the current literature [1–6], and we illustrate the differences with some simple examples. Section 5 reviews the syntax and semantics of Full General Flow Logic $\mathbf{GFL}^\star$ and discusses its expressibility. The main result is in Section 6, where we establish that our notion of p-bisimulation preserves the semantics of $\mathbf{GFL}^\star$.

2 Preliminaries: time lines and paths

We use relations/set-valued maps $r : X \rightsquigarrow Y$, with $r(x) \subseteq Y$ for $x \in X$, and let $[\, X \rightsquigarrow Y \,]$ denote the set of all such maps, so $[\, X \rightsquigarrow Y \,] = 2^{X \times Y}$. A map $r : X \rightsquigarrow Y$ has a converse $r^{-1} : Y \rightsquigarrow X$; domain $\mathrm{dom}(r) := \{x \in X \mid r(x) \neq \varnothing\}$; range $\mathrm{ran}(r) := \mathrm{dom}(r^{-1}) \subseteq Y$; and r is *total on* X if $\mathrm{dom}(r) = X$. Writing

$r : X \to Y$ means r is a single-valued function total on X, with values $r(x) = y$, and $[\, X \to Y \,]$ is the set of all such functions. For partial functions, writing $r : X \dashrightarrow Y$ means that on $\mathrm{dom}(r) \subseteq X$, r is single-valued; we write $r(x) = y$ when $x \in \mathrm{dom}(r)$ with value y, and $r(x) = \textsc{undef}$ when $x \notin \mathrm{dom}(r)$, and $[\, X \dashrightarrow Y \,]$ is the set of all such maps. So $[\, X \to Y \,] \subseteq [\, X \dashrightarrow Y \,] \subseteq [\, X \rightsquigarrow Y \,]$.

Let $(L, <, 0)$ be a *linear order* with least element 0 and no largest element. We will call L a (future) *time line* if the following three conditions are satisfied:
(i) L is Dedekind-complete, i.e. sup's and inf's exist for non-empty bounded subsets;
(ii) there exists a *linearly ordered abelian group* $(\overline{L}, <, +, 0)$ such that $(L, <, +, 0)$ is a linearly ordered sub-semigroup of $\overline{L}$, and $L \subseteq \{l \in \overline{L} \mid l \geqslant 0\}$;
(iii) L is equipped with an extended metric function $d_L : (L \times L) \to \mathbb{R}_0^{+\infty}$ together with a continuous order-preserving total function (a *fibering map*) $p : L \to M$ into a countable linear order $(M, <_M)$ such that,
(a) for each $m \in M$, the *fibre* $p^{-1}(m) \subseteq L$ is a metric space under d_L;
(b) for all $m, m' \in M$, $a \in p^{-1}(m)$, $b \in p^{-1}(m') :\ d_L(a, b) < \infty$ iff $m = m'$;
(c) for all $a, b, c \in L$, $a \leqslant c$, $d_L(a, c) < \infty :\ d_L(a, c) = d_L(a, b) + d_L(b, c)$ iff $a \leqslant b \leqslant c$;
(d) for all $a, b, c \in L$, $\quad d_L(b, c) = d_L(a + b, a + c)$.
From the group $\overline{L}$, a time line L has a family of order-isomorphisms $\{\sigma^{+a}\}_{a \in L}$ such that $\sigma^{+0} = \mathrm{id}_L$ and for each $a \in L$, the *right a-shift* $\sigma^{+a} \colon L \to L$ is given by $\sigma^{+a}(l) := l + a$, and with inverse $\sigma^{-a} := (\sigma^{+a})^{-1} \colon [a, \infty) \to L$ the *left a-shift*. A subset $T \subseteq L$ will be called *$<$-unbounded* if for all $a \in L$, there exists $t \in T$ such that $t > a$, and it will be called *$<$-bounded* otherwise. For any subset $T \subseteq L$, define the set's *total duration* $\mathrm{dur}(T) \in \mathbb{R}_0^{+\infty}$ as follows:

$$\mathrm{dur}(T) \;:=\; \sum_{m \in M} \sup \big\{\, d_L(t, t') \;\mid\; t \in T \cap p^{-1}(m) \;\wedge\; t' \in T \cap p^{-1}(m) \,\big\}$$

where for $S \subseteq \mathbb{R}_0^+$, we take $\sup(S) = 0$ if $S = \varnothing$. A subset $T \subseteq L$ will be called *duration-bounded* if $\mathrm{dur}(T) < \infty$, and *duration-unbounded* otherwise.

Basic examples are the discrete time line $\mathbb{N}$, and the dense continuum time line $\mathbb{R}_0^+ := [0, \infty)$, whose linearly ordered abelian groups under addition are $\mathbb{Z}$ and $\mathbb{R}$ respectively. For $L = \mathbb{N}$ and $L = \mathbb{R}_0^+$, the group operation also gives a suitable metric: take $d_L(a, b) := \max\{a - b, b - a\}$, and take $p : L \to \{0\}$ constant, so there is only one fibre, $p^{-1}(0) = L$. For these standard time lines, the metric is finite everywhere and for all subsets $T \subseteq L$, we have the following equivalences: T is $<$-bounded iff T is duration-bounded iff $T \subseteq [0, b]$ for some $b \in L$.

The hybrid time set $L = \mathbb{H} := \mathbb{N} \times \mathbb{R}_0^+$ is linearly ordered *lexicographically*: $(i, t) <_{\mathrm{lex}} (j, s)$ iff $i < j$ or else both $i = j$ and $t < s$. The least element is $\mathbf{0} := (0, 0)$ and the ordering is Dedekind-complete. The linear order $\mathbb{H}$ is the non-negative *quarter* of the abelian group $\mathbb{Z} \times \mathbb{R}$, defined by: $(i, t) + (j, s) := (i + j, t + s)$; with the lexicographic ordering, $\mathbb{Z} \times \mathbb{R}$ is a linearly ordered abelian group. For the extended metric on $L = \mathbb{H}$, the fibering map $p_{\mathbb{H}} : \mathbb{H} \to \mathbb{N}$ is simply $p_{\mathbb{H}}(i, t) := i$ for all $(i, t) \in \mathbb{H}$, and for each $i \in \mathbb{N}$, the fibre under $p_{\mathbb{H}}$ is $p_{\mathbb{H}}^{-1}(i) = \{i\} \times \mathbb{R}_0^+$. We only assign a finite distance between time positions $a = (k, r)$ and $b = (i, t)$ with discrete time coordinates $k = i$ the same; define $d_{\mathbb{H}} : (\mathbb{H} \times \mathbb{H}) \to \mathbb{R}_0^{+\infty}$ such that, for all $a = (k, r)$ and $b = (i, t)$ in $\mathbb{H}$, $d_{\mathbb{H}}(a, b) := d_{\mathbb{R}}(r, t)$ if $k = i$, and $d_{\mathbb{H}}(a, b) := \infty$ if $k \neq i$. Thus $(\mathbb{H}, <_{\mathrm{lex}}, \mathbf{0}, +, d_{\mathbb{H}}, p_{\mathbb{H}})$ is a time line. In $L = \mathbb{H}$, the

two concepts of boundedness are not equivalent: the interval $T = \{42\} \times [0, \infty)$ is $<$-bounded but duration-unbounded, while the time domain of a *Zeno* infinite hybrid trajectory is duration-bounded but $<$-unbounded.

For any linear order $(L, <)$, and for any subset $T \subseteq L$, the T-*successor* partial function $\mathrm{succ}_T : T \dashrightarrow T$ is defined by:

$$\forall a, b \in T, \qquad \mathrm{succ}_T(a) = b \quad \Leftrightarrow \quad [\ a < b \ \wedge \ (\forall t \in T)\, t \leqslant a \ \vee \ b \leqslant t \ ]\,.$$

For example, for $T = L = \mathbb{N}$, we have $\mathrm{dom}(\mathrm{succ}_L) = L$, which means L is *everywhere discrete*, while for $T = L = \mathbb{R}_0^+$, the map succ_L is defined nowhere, which means L is *everywhere dense*. If $T \subset \mathbb{H}$ is the domain of a hybrid trajectory, then the partial function succ_T will be defined only at the switching times in T. For the purpose of formulating a new concept of bisimulation later in the paper, as well as for giving a semantics to a "*next-times*" operator in temporal logic, we have the need for a *progress* operator acting on initial subsets T of time lines.

Definition 1. (***Progress operator on initial subsets of time lines***)
For any time line L, and any initial subset $T \subseteq L$ with $0 \in T$, define:

$$\mathrm{Pro}(T) \ := \ \{\, t \in T \mid t > 0 \ \wedge \ (\forall s \in \mathrm{ran}(\mathrm{succ}_T))\ t \leqslant s \,\}$$

Hence if $0 \in \mathrm{dom}(\mathrm{succ}_T)$ then $\mathrm{Pro}(T) = \{\mathrm{succ}_T(0)\}$; if $0 \notin \mathrm{dom}(\mathrm{succ}_T)$ but $\mathrm{ran}(\mathrm{succ}_T) \neq \varnothing$ then $\mathrm{Pro}(T) = (0, s_T]$ where $s_T := \min(\mathrm{ran}(\mathrm{succ}_T))$, while if T is everywhere dense, so $\mathrm{ran}(\mathrm{succ}_T) = \varnothing$, then $\mathrm{Pro}(T) = T - \{0\}$.

For the usual time lines $L = \mathbb{N}$ and $L = \mathbb{R}_0^+$, the basic form of a time domain for a *path* is a closed bounded interval $[0, b]$, which in $\mathbb{N}$ evaluates to $\{0, 1, \ldots, b\}$. For the hybrid time line $L = \mathbb{H}$, finite hybrid trajectories are typically functions taking values in a space $X \subseteq Q \times \mathbb{R}^n$, with Q a finite set, and we can represent their time domains as disjoint unions of the form:

$$T \ = \ \bigcup_{i<N} \{i\} \times [s_i, s_i + \Delta_i] \ = \ \bigcup_{i<N} [\,(i, s_i),\, (i, s_{i+1})\,] \tag{1}$$

where $s_0 := 0$ and $s_{i+1} := s_i + \Delta_i$ and $(\Delta_0, \Delta_1, \ldots, \Delta_{N-1})$ is a finite sequence of *interval durations* $\Delta_i \in \mathbb{R}_0^+$ for $i < N$, and $(s_1, \ldots, s_{N-1}, s_N)$ is the corresponding sequence of *switching times*. Along a hybrid trajectory, for $i < N - 1$, we have $\mathrm{succ}_T(i, s_{i+1}) = (i + 1, s_{i+1})$, but relative to the underlying ordering $\mathbb{H}$, there is a distinct **gap** between these two time positions, in the form of the interval $\{i\} \times (s_{i+1}, \infty)$ followed by the interval $\{i + 1\} \times [0, s_{i+1})$.

Definition 2. (***Bounded time domains and paths***)
Given a time line L, define a bounded time domain *in L to be a subset $T \subset L$ such that $T = \bigcup_{n<N}[a_n, b_n]$ with $N \in \mathbb{N}^+$, $a_0 = 0$, $b_{N-1} = b_T := \max(T)$, and $a_n \leqslant b_n < a_{n+1} \leqslant b_{n+1}$ for all $n < N - 1$, and $d(a_n, b_n) < \infty$ for all $n < N$. Let $\mathsf{BT}(L) \subset 2^L$ be the set of all bounded time domains in L, and let $\mathsf{BI}(L) := \{T \in \mathsf{BT}(L) \mid (\exists b \in L)\, T = [0, b]\,\}$ be the interval time domains. Over any set $X \neq \varnothing$, define:*

$$\mathsf{Path}(L, X) := \{\, \gamma : L \dashrightarrow X \mid \mathrm{dom}(\gamma) \in \mathsf{BT}(L)\,\}$$
$$\mathsf{IPath}(L, X) := \{\, \gamma : L \dashrightarrow X \mid \mathrm{dom}(\gamma) \in \mathsf{BI}(L)\,\}$$

For $\gamma \in \mathsf{Path}(L,X)$*, define* $b_\gamma := \max(\mathrm{dom}(\gamma))$*, so that* $\gamma(0) \in X$ *is* γ*'s start-point, and* $\gamma(b_\gamma) \in X$ *is* γ*'s end-point. The* total duration *of* γ *is* $\mathrm{dur}(\gamma) := \mathrm{dur}(\mathrm{dom}(\gamma)) < \infty$ *(so* $\mathrm{dom}(\gamma)$ *is both duration-bounded and* $<$*-bounded). Let* $\epsilon \in [L \dashrightarrow X]$ *denote the empty path; for any* $\mathcal{P} \subseteq \mathsf{Path}(L,X)$*, let* $\mathcal{P}_\epsilon := \mathcal{P} \cup \{\epsilon\}$*.*

Given a time line L, the set $\mathsf{BT}(L)$ is *partially ordered* via the linear ordering on L: for $T, T' \in \mathsf{BT}(L)$, we say T' is an *ordered extension* of T, and (re-using notation) we write $T < T'$, iff $T \subset T'$ and $t < t'$ for all $t \in T$ and all $t' \in T' - T$. Likewise, the path set $\mathsf{Path}_\epsilon(L,X)$ is partially ordered: $\gamma < \gamma'$ iff $\gamma \subset \gamma'$ and $\mathrm{dom}(\gamma) < \mathrm{dom}(\gamma')$, in which case we say the path γ' is a (proper) *extension* of γ. For any set of paths $\mathcal{P} \subseteq \mathrm{Path}_\epsilon(L,X)$, $\mathcal{P}$ is $<$*-unbounded* (or *extension-unbounded*) if for all $\gamma \in \mathcal{P}$, there exists $\gamma' \in \mathcal{P}$ such that $\gamma < \gamma'$.

We use the following operations; for $\gamma, \gamma' \in \mathsf{Path}_\epsilon(L,X)$, $t \in \mathrm{dom}(\gamma)$, $x \in X$:

- the *trivial path* $\theta_x : [0,0] \to X$ given by $\theta_x(0) = x$.
- *restriction* or *prefix* ending at t: $\gamma|_t \in \mathsf{Path}_\epsilon(L,X)$ where $(\gamma|_t)(l) := \gamma(l)$ for all $l \in \mathrm{dom}(\gamma|_t) := [0,t] \cap \mathrm{dom}(\gamma)$.
- *translation* or *suffix* starting at t: ${}_t|\gamma \in \mathsf{Path}_\epsilon(L,X)$ where $({}_t|\gamma)(l) := \gamma(l+t)$ for all $l \in \mathrm{dom}({}_t|\gamma) := \sigma^{-t}([t, b_\gamma] \cap \mathrm{dom}(\gamma))$.
- *point-concatenation* at $x \in X$: $\gamma *_x \gamma' \in \mathsf{Path}_\epsilon(L,X)$ where, for all $l \in L$:

$$(\gamma *_x \gamma')(l) := \begin{cases} \gamma(l) & \text{if } \ l \in \mathrm{dom}(\gamma) \ \wedge \ \gamma'(0) = \gamma(b_\gamma) = x \\ \gamma'(l - b_\gamma) & \text{if } \ l \in \sigma^{+b_\gamma}(\mathrm{dom}(\gamma')) \ \wedge \ \gamma'(0) = \gamma(b_\gamma) = x \\ \text{UNDEF} & \text{otherwise} \end{cases}$$

and $\mathrm{dom}(\gamma *_x \gamma') = \mathrm{dom}(\gamma) \cup \sigma^{+b_\gamma}(\mathrm{dom}(\gamma'))$ [3].

The path extension ordering and point-concatenation are related as follows:

$$\gamma < \gamma' \quad \text{iff} \quad \gamma' = \gamma *_x \gamma'' \text{ for some } \gamma'' \in \mathsf{Path}(L,X) \text{ and } x \in X \text{ with } \gamma'' \neq \theta_x \quad (2)$$

3 General flow systems, and their infinitary extensions

Introduced in [7], and further developed in [11], the class of general flow systems generalizes to arbitrary time lines Aubin's model of an *Evolutionary System* [10].

Definition 3. (***General flow systems and finitary properties***)
Let L *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* $x \in \mathrm{dom}(\Phi)$*, for all* $\gamma \in \Phi(x)$*, and for all* $t \in \mathrm{dom}(\gamma)$*:*

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

(**GF1**) time-invariance *or* suffix-closure*:* ${}_t|\gamma \in \Phi(\gamma(t))$*;*

(**GF2**) point-concatenation*:* $\gamma|_t *_y \gamma' \in \Phi(x)$ *for all* $\gamma' \in \Phi(y)$ *with* $y = \gamma(t)$*.*

[3] For the discrete time line $L = \mathbb{N}$, the interval path set $\mathrm{IPath}_\epsilon(\mathbb{N}, X) = X^*$ is the set of all finite *words* or sequences over X. The usual operation of *word-concatenation* from automata theory equips X^* as a total monoid with identity ϵ; word-concatenation can be readily defined in terms of point-concatenation using length-2 connecting words formed from the end-value of the first word and the start-value of the second.

• Φ *is* deadlock-free *if* $\Phi(x) \neq \{\theta_x\}$, *for every* $x \in \mathrm{dom}(\Phi)$*;*
• Φ *is* $<$-unbounded *if the path set* $\Phi(x)$ *is* $<$*-unbounded, for every* $x \in \mathrm{dom}(\Phi)$*;*
• Φ *is* deterministic *if* $\Phi(x)$ *is linearly-ordered by* $<$*, for every* $x \in \mathrm{dom}(\Phi)$*;*
• Φ *is* point-controllable [9] *if for all* $x', x'' \in \mathrm{dom}(\Phi)$*, there exists* $\gamma \in \Phi(x')$ *and* $t \in \mathrm{dom}(\gamma)$ *such that* $\gamma(t) = x''$*;*
• Φ *is* path-controllable [9] *if for all* $x, x', x'' \in \mathrm{dom}(\Phi)$ *and for all* $\gamma' \in \Phi(x)$*, if* $x' = \gamma'(b_{\gamma'})$*, then for all* $\gamma'' \in \Phi(x'')$*, there exists* $\gamma \in \Phi(x')$ *and* $t \in \mathrm{dom}(\gamma)$ *such that* $(\gamma' *_{x'} \gamma|_t *_{x''} \gamma'') \in \Phi(x)$*.*

The following results are readily established [7, 11]: Φ is point-controllable iff Φ is path-controllable; Φ is deadlock-free iff Φ is $<$-unbounded. In terms of *Behavioural Systems theory* [9], condition **GF1** corresponds to the *time invariance* property, while condition **GF2** corresponds to the "Axiom of State" principle.

Example 1. Let L be any time line, and consider the map $\Phi_L : L \rightsquigarrow \mathsf{Path}(L, L)$ given by $\Phi_L(a) := \{\gamma \in \mathsf{Path}(L, L) \mid (\exists s \in L)\ \gamma = (\sigma^{+a})|_s\}$. Then Φ_L is an interval-path, deterministic and deadlock-free general flow system over L, but it is not point-controllable (being only uni-directional since L is a semigroup).

Further examples of general flow systems include automata and state transition systems over $L = \mathbb{N}$, differential equations and inclusions over $L = \mathbb{R}_0^+$, and hybrid automata and impulse differential inclusions over hybrid time $L = \mathbb{H}$ [7], as well as stochastic hybrid and continuous time systems.

In order to directly represent hybrid trajectories, and their constituent parts, we choose to take as our primitive objects paths of finite duration, with a start-point and an end-point. However, we still have many reasons to "go to infinity" by finding "maximal extensions" of finite duration paths, including formalizing asymptotic properties of systems such as stability, as well as the eventuality and *until* type properties expressible in temporal logics [7], and also comparing and utilizing work on existing system-theoretic models, e.g. *Evolutionary Systems* [10]; *Behavioural Systems* [9]; and various hybrid system classes [12, 1–3, 6].

A general flow Φ is deadlock-free iff it is $<$-unbounded, so for each $x \in dom(\Phi)$ and finite path $\gamma \in \Phi(x)$, we can recursively construct an ω-length extending sequence of paths $\{\gamma_n\}_{n<\omega}$ starting from $\gamma_0 = \gamma$ with $\gamma_n \in \Phi(x)$ and $\gamma_n < \gamma_{n+1}$ for all $n < \omega$. Motivated by this fact, we view "maximal extensions" or "completions" of paths as infinitary objects, arising as limits of infinite sequences of finite paths. Revising earlier work in [7, 11], we now work with ν-length infinite sequences of paths $\{\gamma_n\}_{n<\nu}$, for all limit ordinals $\nu \leq \kappa$, where $\kappa = |L|$, the cardinality of the time line L and the initial limit ordinal of that cardinality. The crucial pay-off from this transfinite generosity is Theorem 1.

Definition 4. (κ***-extension of path sets***)
For a time line L*, let* $\kappa = |L|$*, and let* $\mathrm{LO}(\kappa)$ *be the set of all limit ordinals* $\nu \leq \kappa$ *with* $\nu \neq 0$*. For any path set* $\mathcal{P} \subseteq \mathsf{Path}_\epsilon(L, X)$*, define the* κ-extension *of* $\mathcal{P}$*:*

$$\begin{aligned}\mathsf{Ext}(\mathcal{P}) := \{\, \beta \in [L \dashrightarrow X] \mid (\exists \nu \in \mathrm{LO}(\kappa))\,(\exists\, \overline{\gamma} \in [\nu \to \mathsf{Path}(L, X)]\,)\,(\forall n < \nu)\\ \gamma_n := \overline{\gamma}(n) \ \wedge\ \gamma_n \in \mathcal{P} \ \wedge\ (\forall n' < \nu)\,(n < n' \ \Rightarrow\ \gamma_n < \gamma_{n'})\\ \wedge\ \beta = \textstyle\bigcup_{m<\nu} \gamma_m \,\}\end{aligned}$$

Define $\mathsf{EPath}(L, X) := \mathsf{Ext}\,(\,\mathsf{Path}_\epsilon(L, X)\,)$*,* $\mathsf{EIPath}(L, X) := \mathsf{Ext}\,(\,\mathsf{IPath}_\epsilon(L, X)\,)$*.*

The κ-extension $\mathsf{Ext}(\mathcal{P})$ contains all the partial functions $\beta : L \dashrightarrow X$ that can arise as the limit of a ν-length chain of paths in $\mathcal{P}$, for some limit ordinal $\nu \in \mathrm{LO}(\kappa)$. The *total duration* of a limit path $\alpha \in \mathsf{EPath}(L, X)$ is defined $\mathrm{dur}(\alpha) := \mathrm{dur}(\mathrm{dom}(\alpha))$, where $\mathrm{dur}(T)$ is as defined in Section 2 for any $T \subseteq L$. The path extension ordering $<$ on bounded paths induced by the linear order on L can also be lifted to limit paths, and if $\alpha < \alpha'$ then we must have $\mathrm{dur}(\alpha) < \infty$.

For reasoning about the *asymptotic* behaviour of a path set or general flow, the Ext operation will not quite do, as the set of limit paths $\mathsf{Ext}(\mathcal{P})$ also includes limit paths α that are *too short* to be of *maximal* extension or duration, as witnessed by there being some actual, finite-duration path $\gamma \in \mathcal{P}$ that properly extends α. For general flows Φ, we want to additionally require the limit paths in $\mathsf{M}\Phi(x)$ to be not only maximal w.r.t. the extension partial ordering, but also collectively *complete* in their representation of Φ, in that for every finite path $\gamma \in \Phi(x)$, there is at least one limit path $\alpha \in \mathsf{M}\Phi(x)$ properly extending γ.

Definition 5. (***Maximal extension & infinitary properties of path sets***)
Let L be a time line and let $X \neq \varnothing$ be any value space.
For any path set $\mathcal{P} \subseteq \mathsf{Path}_\epsilon(L, X)$, define the maximal extension *of $\mathcal{P}$ to be the limit path set $\mathsf{M}(\mathcal{P})$, with $\mathsf{M}(\mathcal{P}) \subseteq \mathsf{Ext}(\mathcal{P}) \subseteq \mathsf{EPath}(L, X)$ defined by:*

$$\mathsf{M}(\mathcal{P}) := \{\, \alpha \in \mathsf{Ext}(\mathcal{P}) \mid (\forall \gamma \in \mathcal{P})\ \alpha \not< \gamma \,\}$$

A path set $\mathcal{P} \subseteq \mathsf{Path}_\epsilon(L, X)$ will be called maximally extendible *if for all $\gamma \in \mathcal{P}$, there exists $\alpha \in \mathsf{M}(\mathcal{P})$ such that $\gamma < \alpha$.*
Given a general flow system $\Phi\colon X \rightsquigarrow \mathsf{Path}(L, X)$, define the maximal extension *of Φ to be the map $\mathsf{M}\Phi\colon X \rightsquigarrow \mathsf{EPath}(L, X)$ given by $(\mathsf{M}\Phi)(x) := \mathsf{M}(\Phi(x))$ for all $x \in \mathrm{dom}(\mathsf{M}\Phi) := \mathrm{dom}(\Phi)$. A general flow system Φ will be called* maximally extendible *if for all $x \in \mathrm{dom}(\Phi)$, the path set $\Phi(x)$ is maximally extendible.*

Theorem 1. [Assume the Axiom of Choice.] *For any set $\mathcal{P} \subseteq \mathsf{Path}_\epsilon(L, X)$,*
$\mathcal{P}$ is maximally extendible iff $\mathcal{P}$ is $<$-unbounded.
Hence for any general flow system $\Phi\colon X \rightsquigarrow \mathsf{Path}(L, X)$,
Φ is maximally extendible iff Φ is $<$-unbounded iff Φ is deadlock-free;
if Φ is deadlock-free, then: Φ is deterministic iff $\mathsf{M}\Phi$ is a partial function.

4 Bisimulation relations between general flow systems

The most basic notion of simulation and bisimulation is reachability-preserving but not time-preserving or path-matching. This is what is known as "*time-abstract*" simulation and bisimulation for the case of *transition systems* (including transition system representations of hybrid and continuous systems [1]), which are general flow systems over time $L = \mathbb{N}$.

Definition 6. *Given time lines L_1 and L_2, possibly different, and general flows $\Phi_1\colon X_1 \rightsquigarrow \mathsf{Path}(L_1, X_1)$, $\Phi_2\colon X_2 \rightsquigarrow \mathsf{Path}(L_2, X_2)$, a relation $R : X_1 \rightsquigarrow X_2$ is a* reachability simulation (*or* r-simulation) *of Φ_1 by Φ_2 if $\mathrm{dom}(\Phi_1) \subseteq \mathrm{dom}(R)$ and for all $x_1, x_1' \in X_1$ and for all $x_2 \in X_2$ such that $(x_1, x_2) \in R$,*
if *there exists $\gamma_1 \in \Phi_1(x_1)$ and $t_1 \in \mathrm{dom}(\gamma_1)$ such that $t_1 > 0$ and $x_1' = \gamma_1(t_1)$,*

then *there exists* $x_2' \in X_2$ *and* $\gamma_2 \in \Phi_2(x_2)$ *and a time point* $t_2 \in \mathrm{dom}(\gamma_2)$ *such that* $t_2 > 0$ *and* $x_2' = \gamma_2(t_2)$ *and* $(x_1', x_2') \in R$.
A map $R : X_1 \rightsquigarrow X_2$ *is a* reachability bisimulation (*or* r-bisimulation) *between* Φ_1 *and* Φ_2 *if both* R *and* R^{-1} *are r-simulations.*

For general flows Φ_i, $i = 1, 2$, let $Q_i : X_i \rightsquigarrow X_i$ be the (strict) *reachability relation* of the system: for all $x, x' \in X_i$, define $(x, x') \in Q_i$ iff $x' = \gamma(t)$ for some $\gamma \in \Phi_i(x)$ and $t \in \mathrm{dom}(\gamma)$ with $t > 0$. So $\mathrm{dom}(Q_i) \subseteq \mathrm{dom}(\Phi_i)$, and for sets $A \subseteq X_i$, the Φ_i-reachable region from A is the $\exists$-post-image of relation Q_i applied to A; that is, $\mathrm{Reach}_i(A) := Q_i^{\exists}(A) = \{x' \in X_i \mid (\exists x \in A)\,(x, x') \in Q_i\}$. This is at the heart of any transition system representation of hybrid or continuous dynamical systems. For any map/relation $R : X_1 \rightsquigarrow X_2$, the $\exists$-pre-image operator $R^{-\exists}$ is given by $R^{-1}(B) := \{x_1 \in X_1 \mid (\exists x_2 \in B)\,(x_1, x_2) \in R\}$ for sets $B \subseteq X_2$. The following results are straight-forward, and motivate our choice of name "reachability simulation" (alternatively, "time abstract simulation").

Proposition 1. *Given time lines* L_1 *and* L_2*, possibly different, and general flows* $\Phi_1 \colon X_1 \rightsquigarrow \mathsf{Path}(L_1, X_1)$ *and* $\Phi_2 \colon X_2 \rightsquigarrow \mathsf{Path}(L_2, X_2)$*, and a map* $R : X_1 \rightsquigarrow X_2$*, suppose that* $\mathrm{dom}(\Phi_1) \subseteq \mathrm{dom}(R)$*. Then the following are equivalent:*
(1.) R *is an r-simulation of* Φ_1 *by* Φ_2*;*
(2.) $R^{-1} \circ Q_1 \subseteq Q_2 \circ R^{-1}$*;*
(3.) $\mathrm{Reach}_1(R^{-\exists}(B)) \subseteq R^{-\exists}(\mathrm{Reach}_2(B))$ *for all* $B \subseteq X_2$.
If R *is an r-bisimulation and* $Q_i^{-1} = Q_i$ *for* $i = 1, 2$ (*e.g. if both flows* Φ_i *are point-controllable*)*, then* $R^{\exists}(\mathrm{Reach}_1(A)) = \mathrm{Reach}_2(R^{\exists}(A))$ *for all* $A \subseteq X_1$.

Proposition 2. *Given* L_1 *and* L_2*, and general flows* $\Phi_1 \colon X_1 \rightsquigarrow \mathsf{Path}(L_1, X_1)$ *and* $\Phi_2 \colon X_2 \rightsquigarrow \mathsf{Path}(L_2, X_2)$*, suppose that* $R : X_1 \rightsquigarrow X_2$ *is an r-simulation of* Φ_1 *by* Φ_2*, and* $\mathrm{dom}(\Phi_2) \subseteq \mathrm{ran}(R)$*. If* Φ_1 *is deadlock-free, then* Φ_2 *is deadlock-free.*

Next, we introduce a slightly stronger notion of simulation and bisimulation which requires some "matching" of time points along paths, but not an exact matching, thus relating systems defined over different time lines.

Definition 7. *Given time lines* L_1 *and* L_2*, possibly different, and general flows* $\Phi_1 \colon X_1 \rightsquigarrow \mathsf{Path}(L_1, X_1)$*,* $\Phi_2 \colon X_2 \rightsquigarrow \mathsf{Path}(L_2, X_2)$*, a relation* $R : X_1 \rightsquigarrow X_2$ *is a* progress simulation (*or* p-simulation) *of* Φ_1 *by* Φ_2 *if* $\mathrm{dom}(\Phi_1) \subseteq \mathrm{dom}(R)$ *and for all* $x_1, x_1' \in X_1$ *and for all* $x_2 \in X_2$ *such that* $(x_1, x_2) \in R$,
if *there exists* $\gamma_1 \in \Phi_1(x_1)$ *and* $t_1 \in \mathrm{Pro}(\mathrm{dom}(\gamma_1))$ *such that* $x_1' = \gamma_1(t_1)$,
then *there exists* $x_2' \in X_2$ *and* $\gamma_2 \in \Phi_2(x_2)$ *and* $t_2 \in \mathrm{Pro}(\mathrm{dom}(\gamma_2))$ *such that* $x_2' = \gamma_2(t_2)$ *and* $(x_1', x_2') \in R$*, and for all intermediate times* $s_2 \in (0, t_2] \cap \mathrm{dom}(\gamma_2)$*, there exists* $s_1 \in (0, t_1] \cap \mathrm{dom}(\gamma_1)$ *such that* $(\gamma_1(s_1), \gamma_2(s_2)) \in R$.
Map $R : X_1 \rightsquigarrow X_2$ *is a* progress bisimulation (p-bisimulation) *between* Φ_1 *and* Φ_2 *if both* R *and* R^{-1} *are p-simulations.*

As we show in the main result, Theorem 2 below, this notion of p-bisimulation is strong enough to yield a semantic-presevation bisimulation theorem for the logic $\mathbf{GFL}^\star$ of general flow systems, yet is still flexible enough to allow that the time lines of the two general flows be different. Note that, in the case that both

time lines are discrete, with $L_1 = L_2 = \mathbb{N}$, and both general flows are determined by a (one-step) transition relation on the state space, then a p-simulation is a (standard) simulation relation in the original sense of Milner [13].

Definition 8. *Given general flow systems* $\Phi_1 \colon X_1 \rightsquigarrow \mathsf{Path}(L, X_1)$ *and* $\Phi_2 \colon X_2 \rightsquigarrow \mathsf{Path}(L, X_2)$ *over the same time line* L*, a relation* $R : X_1 \rightsquigarrow X_2$ *is a* timed simulation (t-simulation) *of* Φ_1 *by* Φ_2 *if* $\mathrm{dom}(\Phi_1) \subseteq \mathrm{dom}(R)$*, and for all* $x_1, x_1' \in X_1$*, and* $x_2 \in X_2$ *such that* $(x_1, x_2) \in R$*, and for all times* $t > 0$*,*
if *there exists* $\gamma_1 \in \Phi_1(x_1)$ *such that* $x_1' = \gamma_1(t)$*,*
then *there exists* $x_2' \in X_2$ *and* $\gamma_2 \in \Phi_2(x_2)$ *such that* $x_2' = \gamma_2(t)$ *and*
$\mathrm{dom}(\gamma_2) = \mathrm{dom}(\gamma_1)$ *and* $(\gamma_1(s), \gamma_2(s)) \in R$ *for all* $s \in \mathrm{dom}(\gamma_2) \cap [0, t]$.
A relation $R : X_1 \rightsquigarrow X_2$ *is a* timed bisimulation (*or* t-bisimulation) *between* Φ_1 *and* Φ_2 *if both* R *and* R^{-1} *are t-simulations.*

It follows directly from the definitions that when $L_1 = L_2$ and R is a t-simulation, R is also a p-simulation, and for any L_1 and L_2, if R is a p-simulation, then R is an r-simulation. Other notions of simulation and bisimulation have been recently investigated in the context of continuous [5, 6] and hybrid systems [1, 2]. All of them require an exact matching between the time parameterizing trajectories and thus are t-bisimulations between the general flow systems defined by the corresponding continuous or hybrid systems. Notions of bisimulation not requiring exact time matching were implicitly considered in [4]. Although [4] is based on the standard Milner notion of bisimulation between transition systems, different embeddings of linear control systems into transition systems resulted in different notions of bisimulation: t-bisimulation and r-bisimulation. The notions of simulation and bisimulation developed for hybrid I/O automata in [3] come out as intermediate between the r-simulations and p-simulations here.

We conclude this section with a brief discussion of some examples. We deliberately choose systems with simple deterministic dynamics so as to keep the focus on illustrating the various simulation relationships.

Example 2. Consider a discrete-time deterministic system with general flow map $\Phi_1 : X_1 \rightsquigarrow \mathsf{Path}(\mathbb{N}, X_1)$ over state space $X_1 := \{q_1, q_2, q_3, q_4\}$ generated by the transition function $\delta : X_1 \to X_1$ with $\delta(q_k) := q_{k+1}$ for $k = 1, 2, 3$ and $\delta(q_4) = q_1$. Next, consider a continuous-time deterministic system with general flow map $\Phi_2 : X_2 \rightsquigarrow \mathsf{Path}(\mathbb{R}_0^+, X_2)$ over the state space $X_2 := \mathbb{R}^2 - \{(0, 0)\}$ given by the differential equation: $\dot{x}_1 = x_2$ and $\dot{x}_2 = -x_1$. So $\Phi_2(x_1, x_2) = \{\gamma : [0, b] \to X_2 \mid b \geq 0 \wedge (\forall t \in \mathrm{dom}(\gamma))\, \gamma(t) = (x_1 \cos(t) + x_2 \sin(t), x_2 \cos(t) - x_1 \sin(t))\}$, and the paths correspond to circular motion in clockwise direction, with radius of the circle $r = \sqrt{x_1^2 + x_2^2}$. Then consider the relation $R : X_1 \rightsquigarrow X_2$ given by:

$$R(q_1) = \{(x_1, x_2) \in X_2 \mid x_1 \leqslant 0 \wedge x_2 > 0\},\ R(q_2) = \{(x_1, x_2) \in X_2 \mid x_1 > 0 \wedge x_2 \geqslant 0\}$$
$$R(q_3) = \{(x_1, x_2) \in X_2 \mid x_1 \geqslant 0 \wedge x_2 < 0\},\ R(q_4) = \{(x_1, x_2) \in X_2 \mid x_1 < 0 \wedge x_2 \leqslant 0\}$$

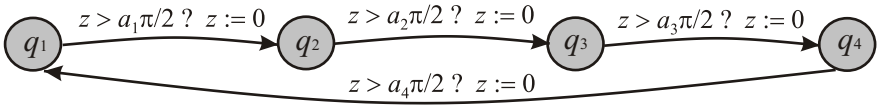
It is clear that $\mathrm{dom}(\Phi_1) = X_1 = \mathrm{dom}(R)$ and $\mathrm{dom}(\Phi_2) = X_2 = \mathrm{ran}(R)$, and it is readily established that R is an r-simulation of the discrete system Φ_1 by the continuous system Φ_2, but it is not a p-simulation. To see why p-similarity fails, consider $(q_2, (\frac{1}{2}, \frac{1}{2})) \in R$ and note that, in Φ_1, along the unique discrete path

$\gamma_1 \in \Phi_1(q_2)$ with $\mathrm{dom}(\gamma_1) = \{0,1,2,3,4\}$, we have $q_3 = \gamma_1(1)$ with time $t_1 = 1 \in \mathrm{Pro}(\mathrm{dom}(\gamma_1))$, and this is matched in reachability terms by the unique continuous path $\gamma_2 \in \Phi_2(\frac{1}{2}, \frac{1}{2})$ with $\mathrm{dom}(\gamma_2) = [0, 2\pi]$, at time $t_2 = \frac{\pi}{2} \in \mathrm{Pro}(\mathrm{dom}(\gamma_2))$ and state $(\frac{1}{2}, -\frac{1}{2}) = \gamma_2(\frac{\pi}{2})$, since $(q_3, (\frac{1}{2}, -\frac{1}{2})) \in R$. However, if we pick the intermediate time point $s_2 = \frac{\pi}{4} \in (0, t_2] \cap \mathrm{dom}(\gamma_2) = (0, \frac{\pi}{2}]$, and the state $(\frac{1}{\sqrt{2}}, 0) = \gamma_2(\frac{\pi}{4})$, then we *cannot* find any matching time point $s_1 \in (0, t_1] \cap \mathrm{dom}(\gamma_1) = \{1\}$ such that $\gamma_1(s_1) = q_2$ – because $\gamma_1(1) = q_3$, and thus we cannot satisfy $(\gamma_1(s_1), \gamma_2(s_2)) = (\gamma_1(s_1), (\frac{1}{\sqrt{2}}, 0)) \in R$.

We can, however, easily construct a variant map $\hat{R} : X_1 \rightsquigarrow X_2$ such that $\hat{R}$ is a p-simulation of Φ_1 by Φ_2. Let $\hat{R} : X_1 \rightsquigarrow X_2$ be given by:

$$\hat{R}(q_1) = \{(x_1, x_2) \in X_2 \mid x_1 = 0 \wedge x_2 > 0\},\ \hat{R}(q_2) = \{(x_1, x_2) \in X_2 \mid x_1 > 0 \wedge x_2 = 0\}$$
$$\hat{R}(q_3) = \{(x_1, x_2) \in X_2 \mid x_1 = 0 \wedge x_2 < 0\},\ \hat{R}(q_4) = \{(x_1, x_2) \in X_2 \mid x_1 < 0 \wedge x_2 = 0\}$$

While we have chosen for illustrative purposes to simulate a discrete-time system by a continuous-time system, the process of temporal sampling and spatial quantization would go the other way, simulating continuous by discrete.



Example 3. Consider the hybrid system defined by the timed automaton H over state space $X_3 := \bigcup_{k \in K} \{q_k\} \times [0, (a_k + 1)\frac{\pi}{2}]$ represented in the figure above, where z is the (sole) clock variable and for $k \in K = \{1,2,3,4\}$, $a_k > 0$ are fixed real constants; let $\Phi_3 : X_3 \rightsquigarrow \mathsf{Path}(\mathbb{H}, X_3)$ be its general flow. Then consider the relation $S : X_3 \rightsquigarrow X_2$ defined for all $z \in \mathbb{R}_0^+$ by:

$$S(q_1, z) = \{(x_1, x_2) \in X_2 \mid x_1 \leq 0 \ \wedge\ x_2 > 0 \ \wedge\ \ z = a_1 \tfrac{\pi}{2} \arctan(\tfrac{x_1}{x_2})\}$$
$$S(q_2, z) = \{(x_1, x_2) \in X_2 \mid x_1 > 0 \ \wedge\ x_2 \geq 0 \ \wedge\ \ z = a_2 \tfrac{\pi}{2} \arctan(\tfrac{-x_2}{x_1})\}$$
$$S(q_3, z) = \{(x_1, x_2) \in X_2 \mid x_1 \geq 0 \ \wedge\ x_2 < 0 \ \wedge\ \ z = a_3 \tfrac{\pi}{2} \arctan(\tfrac{-x_2}{x_1})\}$$
$$S(q_4, z) = \{(x_1, x_2) \in X_2 \mid x_1 < 0 \ \wedge\ x_2 \leq 0 \ \wedge\ \ z = a_4 \tfrac{\pi}{2} \arctan(\tfrac{x_1}{x_2})\}$$

Then S is a p-bisimulation between the hybrid system Φ_3 and the continuous-time system Φ_2, but it cannot be a t-bisimulation since the time-lines are different. However, we can give a continuous-time model Φ_3' of the timed automaton H such that, if $a_1 = a_2 = a_3 = a_4 = 1$, S is a t-bisimulation between Φ_3' and Φ_2.

5 Full General Flow Logic GFL*

The logic *Full General Flow Logic*, **GFL***, first introduced in [7], extends to general flow models the semantics of *Full Computation Tree Logic*, **CTL***, introduced by Emerson and Halpern in 1983 [14, 15] for formalizing reasoning about executions of concurrent systems (hardware or software) in discrete time. The syntax here is a labelled variant of that of **CTL***, the labelling allowing for semantic models consisting of a family of deadlock-free general flow systems.

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

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

for atomic propositions $p \in \mathrm{Prp}$, and system labels $a \in \mathrm{Sys}$. Define logical constants *true*, $\top \stackrel{\text{def}}{=} p \vee \neg p$, for any $p \in \mathrm{Prp}$, and *false*, $\bot \stackrel{\text{def}}{=} \neg\top$. The other propositional (Boolean) connectives are defined in a standard way, and the path quantifiers $\forall_a$ have classical negation duals $\exists_a$, as follows:

$$\varphi_1 \wedge \varphi_2 \stackrel{\text{def}}{=} \neg(\neg\varphi_1 \vee \neg\varphi_2) \qquad \varphi_1 \to \varphi_2 \stackrel{\text{def}}{=} \neg\varphi_1 \vee \varphi_2$$
$$\varphi_1 \leftrightarrow \varphi_2 \stackrel{\text{def}}{=} (\varphi_1 \to \varphi_2) \wedge (\varphi_2 \to \varphi_1) \qquad \exists_a\varphi \stackrel{\text{def}}{=} \neg\forall_a\neg\varphi$$

The *next-times* temporal operators, $\mathbf{X}_a$, for $a \in \mathrm{Sys}$, will be given their semantics using the progress operator (Definition 1). The formula $\mathbf{X}_a\varphi$, read "at *next* times, φ, along $\mathsf{M}\Phi_a$-paths", will hold along any maximal limit path $\eta \in \mathrm{ran}(\mathsf{M}\Phi_a)$ if for some time $t \in \mathrm{Pro}(\mathrm{dom}(\eta))$, φ holds at all time points $s \in (0, t]$. This means that if 0 has a discrete sucessor within $\mathrm{dom}(\eta)$, then φ will hold at that (unique) time, while if 0 does not have a discrete sucessor within $\mathrm{dom}(\eta)$, then φ will hold "immediately after now", throughout the left-open interval $(0, t]$. With this construction, we recover the standard meaning of *next* in discrete time, the same at that for $\mathbf{CTL}^\star$, while if 0 is followed by a dense interval within $\mathrm{dom}(\eta)$, then we gain a rather useful notion of "dense next".

In earlier work on the logic $\mathbf{GFL}^\star$, in [7], we worked with the strictest version of the *until* operator, and used a well-known method to *define* a discrete "next-time" operator as well as a separate dense "immediately after now" operator both in terms of this strictest *until*. Here, we take both *until* and *next* as syntactic and semantic primitives, as is standard in the presentation of $\mathbf{CTL}^\star$ [14, 15], but give new semantics for *next* to allow for denseness in the time domains of paths. This is better for the formulation and proof of preservation of semantics by suitable bisimulations, but still gives a logic equivalent in expressive power to the original.

Definition 9. *A* general flow logic model *of signature* $\Sigma = (\mathrm{Sys}, \mathrm{Prp})$ *is a structure* $\mathfrak{M} = (X, \mathcal{L}, \mathcal{S}, \mathcal{P})$*, where:*
- $X \neq \varnothing$ *is the state space, of arbitrary non-zero 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 a deadlock-free 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 maximal path space *of a model* $\mathfrak{M}$ *is* $\mathsf{MPath}(\mathfrak{M}) := \bigcup_{a\in\mathrm{Sys}} \mathrm{ran}(\mathsf{M}\Phi_a)$.

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 $\Phi_S : X \rightsquigarrow \mathsf{IPath}(\mathbb{N}, X)$ from a total transition relation $S : X \rightsquigarrow X$ [14, 15]).

Definition 10. *For $\varphi \in \mathcal{F}(\Sigma)$ and maximal limit path $\eta \in \mathsf{MPath}(\mathfrak{M})$, the relation "$\varphi$* is satisfied along path η in model $\mathfrak{M}$*", written $\mathfrak{M}, \eta \models \varphi$, is defined by induction on the structure of formulas, with $p \in$ Prp and $a \in$ Sys:*

$$
\begin{array}{lll}
\mathfrak{M}, \eta \models p & \text{iff} & \eta(0) \in \mathcal{P}(p) \\
\mathfrak{M}, \eta \models \neg\, \varphi & \text{iff} & \mathfrak{M}, \eta \not\models \varphi \\
\mathfrak{M}, \eta \models \varphi_1 \vee \varphi_2 & \text{iff} & \mathfrak{M}, \eta \models \varphi_1 \text{ or } \mathfrak{M}, \eta \models \varphi_2 \\
\mathfrak{M}, \eta \models \varphi_1\, \mathbf{U}_a\, \varphi_2 & \text{iff} & \eta \in \mathrm{ran}(\mathsf{M}\Phi_a) \text{ and } \exists\, t \in \mathrm{dom}(\eta),\, t \geqslant 0 \text{ such that} \\
 & & \mathfrak{M},\, {}_t|\eta \models \varphi_2 \text{ and } \forall s \in [0, t) \cap \mathrm{dom}(\eta),\, \mathfrak{M},\, {}_s|\eta \models \varphi_1 \\
\mathfrak{M}, \eta \models \mathbf{X}_a\, \varphi & \text{iff} & \eta \in \mathrm{ran}(\mathsf{M}\Phi_a) \text{ and } \exists\, t \in \mathrm{Pro}(\mathrm{dom}(\eta)) \text{ such that} \\
 & & \forall s \in (0, t] \cap \mathrm{dom}(\eta),\ \ \mathfrak{M},\, {}_s|\eta \models \varphi \\
\mathfrak{M}, \eta \models \forall_a\, \varphi & \text{iff} & \forall \eta' \in \mathsf{M}\Phi_a(\eta(0)),\ \ \mathfrak{M}, \eta' \models \varphi
\end{array}
$$

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

$$[\![\, \varphi \,]\!]^{\mathfrak{M}} := \{\, \eta \in \mathsf{MPath}(\mathfrak{M}) \mid \mathfrak{M}, \eta \models \varphi \,\}$$

$$[\![\, \varphi \,]\!]^{\mathfrak{M}}_{\mathsf{st}} := \{\, x \in X \mid \exists \eta \in \mathsf{MPath}(\mathfrak{M}) : \mathfrak{M}, \eta \models \varphi \ \textit{and}\ x = \eta(0) \,\}$$

For a logic model $\mathfrak{M} \in \mathbb{GF}(\Sigma)$, state x in the state space of $\mathfrak{M}$, class of logic models $C \subseteq \mathbb{GF}(\Sigma)$, and for formulas $\varphi \in \mathcal{F}(\Sigma)$, we say:
• *φ is* satisfied *in $\mathfrak{M}$ at state x, if $x \in [\![\, \varphi \,]\!]^{\mathfrak{M}}_{\mathsf{st}}$, and* 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 $\eta \in \mathsf{MPath}(\mathfrak{M})$;*
• *φ is C-*valid*, written $\models_C \varphi$, if $\mathfrak{M} \models \varphi$ for every $\mathfrak{M} \in C$.*
Define $\mathbf{Valid}(C) := \{\psi \in \mathcal{F}(\Sigma) \mid \models_C \psi\}$ to be the set of all C-valid formulas, and define $\mathbf{GFL}^{\star}(L, \Sigma) := \mathbf{Valid}(\, \mathbb{GF}(L, \Sigma)\,)$, for any given time line L.

It is immediate that when restricting to discrete-time systems in $\mathbb{TR}(\mathbb{N})$, we have $\mathbf{Valid}(\, \mathbb{TR}(\mathbb{N})\,) = \mathbf{CTL}^{\star}$ [14, 15]. For each system label $a \in$ Sys, the one-place operators for *eventually* $\Diamond_a$ and *always* $\Box_a$ are definable in the standard way from the two-place $\mathbf{U}_a$ plus $\top$, and the range of $\mathsf{M}\Phi_a$ is also definable:

$\Diamond_a\, \varphi \stackrel{\text{def}}{=} \top\, \mathbf{U}_a\, \varphi$	paths in $\mathrm{ran}(\mathsf{M}\Phi_a)$ along which φ is *eventually* true
$\Box_a\, \varphi \stackrel{\text{def}}{=} \neg(\top\, \mathbf{U}_a\, (\neg\, \varphi))$	paths in $\mathrm{ran}(\mathsf{M}\Phi_a)$ along which φ is *always* true, plus all the limit paths in $\mathsf{MPath}(\mathfrak{M}) - \mathrm{ran}(\mathsf{M}\Phi_a)$
$\mathsf{Beh}_a \stackrel{\text{def}}{=} \mathbf{X}_a \top$	set of all paths in $\mathrm{ran}(\mathsf{M}\Phi_a)$ = the *behaviour* of Φ_a

As is the case for $\mathbf{CTL}^{\star}$ [14], properties expressible in $\mathbf{GFL}^{\star}$ include safety, invariance, eventuality and "return infinitely often" fairness-type properties. Other properties of interest that can be expressed include:
• *Safety with event sequence behaviour* [16]: suppose the finite family of regions $\{S_1, \ldots, S_k\}$ forms a cover of the designated *Safe* portion of the state space X, and $K = \{1, \ldots, M\}$ and *next* : $K \rightsquigarrow K$ is a total map describing the permitted

sequence orderings of traversal through the regions. The requirement is that every maximal Φ_a trajectory that enters a region S_k remains in S_k until it enters into $S_{k'} - S_k$ for some $k' \in next(k)$. This can by expressed by:

$$\mathfrak{M} \models ((\bigvee_{k\in K} \mathsf{S}_k) \leftrightarrow \mathsf{Safe}) \ \wedge \ \bigwedge_{k\in K} \forall_a(\,\mathsf{S}_k \ \rightarrow \ \bigvee_{k'\in next(k)} (\mathsf{S}_k \,\mathbf{U}_a(\mathsf{S}_{k'} \wedge \neg \mathsf{S}_k))\,)$$

• Aubin's notion of *viability with target* [10, 12] is a "weak until" concept which is expressible in the logic, as is the dual notion of *invariance with target*. The set of maximal Φ_a trajectories that are *viable* within state set $K = [\![\, \mathsf{K} \,]\!]^{\mathfrak{M}}_{\mathsf{st}}$ until capturing target $C = [\![\, \mathsf{C} \,]\!]^{\mathfrak{M}}_{\mathsf{st}}$ can be defined in the logic as follows:

$$\mathsf{K}\,\mathbf{V}_a\,\mathsf{C} \ \stackrel{\text{def}}{=} \ \mathsf{Beh}_a \ \wedge \ (\,\Box_a \mathsf{K} \ \vee \ \mathsf{K}\,\mathbf{U}_a(\mathsf{K} \wedge \mathsf{C})\,)$$

• Fix $\Sigma = (\mathrm{Sys}, \mathrm{Prp})$ with $\alpha \in \mathrm{Sys}$ and Prp having at least two distinct symbols. Given an interval-path deadlock-free general flow Φ, Φ is *deterministic* iff $\mathfrak{M} \models \exists_\alpha \varphi \rightarrow \forall_\alpha \varphi$ for every formula $\varphi \in \mathcal{F}(\Sigma)$ and every model $\mathfrak{M} = (X, \mathfrak{L}, \mathfrak{S}, \mathcal{P})$ of signature Σ over the space X such that $\mathfrak{L}(\alpha) = L$ and $\mathfrak{S}(\alpha) = \Phi$.
• The properties of *point-controllability* (and hence of *path-controllability*) for deadlock-free general flows are expressible in the logic by an inference rule which is valid in every model which includes that flow.

6 Bisimulation theorem for the logic GFL*

In this section, we announce that the notion of p-bisimulation, intermediate between "time-abstract" reachability-preserving and exact time- and path-matching, is adequate for preservation of the semantics of **GFL***.

Definition 11. *Fix a signature $\Sigma = (\mathrm{Sys}, \mathrm{Prp})$, and for $i = 1, 2$, let $\mathfrak{M}_i = (X_i, \mathfrak{L}_i, \mathfrak{S}_i, \mathcal{P}_i)$ be two logic models of signature Σ, and for each system label $a \in \mathrm{Sys}$ and $i = 1, 2$, let $L_{ia} := \mathfrak{L}_i(a)$ be the time line in the model $\mathfrak{M}_i$ for the (deadlock-free) general flow system $\Phi_{ia} := \mathfrak{S}_i(a) \colon X_i \rightsquigarrow \mathsf{Path}(L_{ia}, X_i)$.*
A relation $R : X_1 \rightsquigarrow X_2$ is a p-simulation *of model $\mathfrak{M}_1$ by model $\mathfrak{M}_2$ if:*
(i) *for each system label $a \in \mathrm{Sys}$, relation R is a p-simulation of Φ_{1a} by Φ_{2a}; and*
(ii) *for each atomic proposition $p \in \mathrm{Prp}$, and for all $x_1 \in X_1$ and $x_2 \in X_2$,*
if $x_1 \, R \, x_2$ and $x_1 \in \mathcal{P}_1(p)$, then $x_2 \in \mathcal{P}_2(p)$.
A relation $R : X_1 \rightsquigarrow X_2$ is a p-bisimulation *between model $\mathfrak{M}_1$ and model $\mathfrak{M}_2$ if R is a p-simulation of $\mathfrak{M}_1$ by $\mathfrak{M}_2$, and R^{-1} is a p-simulation of $\mathfrak{M}_2$ by $\mathfrak{M}_1$.*

Recall from the definition of p-bisimulations for general flow systems that if R is a p-bisimulation between $\mathfrak{M}_1$ and $\mathfrak{M}_2$, then we have $\mathrm{dom}(\Phi_{1a}) \subseteq \mathrm{dom}(R)$ and $\mathrm{dom}(\Phi_{2a}) \subseteq \mathrm{ran}(R)$ for each system label $a \in \mathrm{Sys}$.

Theorem 2. [Semantic preservation of **GFL*** for p-bisimulations]
Fix a signature $\Sigma = (\mathrm{Sys}, \mathrm{Prp})$, and for $i = 1, 2$, let $\mathfrak{M}_i = (X_i, \mathfrak{L}_i, \mathfrak{S}_i, \mathcal{P}_i)$ be

two logic models of signature Σ, and suppose $B : X_1 \rightsquigarrow X_2$ is a p-bisimulation between $\mathfrak{M}_1$ and $\mathfrak{M}_2$. Then for all $x_1 \in X_1$ and $x_2 \in X_2$,

$$\text{if} \quad x_1 \, B \, x_2, \quad \text{then} \quad \textit{for all } \varphi \in \mathcal{F}(\Sigma), \quad \Big[\, x_1 \in [\![\, \varphi \,]\!]_{\mathsf{st}}^{\mathfrak{M}_1} \;\Leftrightarrow\; x_2 \in [\![\, \varphi \,]\!]_{\mathsf{st}}^{\mathfrak{M}_2} \, \Big].$$

Corollary 1. *If $B : X_1 \rightsquigarrow X_2$ is a p-bisimulation between $\mathfrak{M}_1$ and $\mathfrak{M}_2$, and both B and B^{-1} are total maps (on X_1 and X_2, respectively), then for all formulas $\varphi \in \mathcal{F}(\Sigma)$, $\mathfrak{M}_1 \models \varphi$ iff $\mathfrak{M}_2 \models \varphi$.*

A journal-length paper covering this material, with detailed proofs and more examples, is available from the authors.

References

1. Haghverdi, E., Tabuada, P., Pappas, G.: Bisimulation relations for dynamical, control and hybrid systems. Theoretical Computer Science **342** (2005) 229–261
2. Julius, A.: On Interconnection and Equivalences of Continuous and Discrete Systems: A Behavioural Perspective. The University of Twente (2005) PhD thesis.
3. Lynch, N., Segala, R., Vaandrager, F.: Hybrid I/O Automata. Information and Computation **185** (2003) 105–157
4. Pappas, G.: Bisimilar linear systems. Automatica **39** (2003) 2035–2047
5. Tabuada, P., Pappas, G.: Bisimilar control affine systems. Systems and Control Letters **52** (2004) 49–58
6. van der Schaft, A.: Equivalence of dynamical systems by bisimulation. IEEE Trans. Automatic Control **49** (2004) 2160–2172
7. Davoren, J., Coulthard, V., Markey, N., Moor, T.: Non-deterministic temporal logics for general flow systems. In: Hybrid Systems: Computation and Control (HSCC'04). LNCS 2993, Springer-Verlag (2004) 280–295
8. Davoren, J.: On hybrid systems and the modal mu-calculus. In: Hybrid Systems V. LNCS 1567, Springer-Verlag (1999) 38–69
9. Willems, J.: Models for dynamics. Dynamics Reported **2** (1989) 171–269
10. Aubin, J.P., Dordan, O.: Dynamical qualitative analysis of evolutionary systems. In: Hybrid Systems: Computation and Control (HSCC'02). LNCS 2289, Springer-Verlag (2002) 62–75
11. Davoren, J., Moor, T.: Non-deterministic reactive systems, from hybrid systems and behavioural systems perspectives. In: Proc. 2nd IFAC Conference on Analysis and Design of Hybrid Systems (ADHS'06), IFAC (2006) 409–416
12. Aubin, J.P., Lygeros, J., Quincampoix, M., Sastry, S., Seube, N.: Impulse differential inclusions: A viability approach to hybrid systems. IEEE Trans. on Automatic Control **47** (2002) 2–20
13. Milner, R.: Communication and Concurrency. Prentice Hall (1989)
14. Emerson, E.: Temporal and modal logic. In van Leeuwen, J., ed.: Handbook of Theoretical Computer Science. Elsevier Science (1990) 997–1072
15. Emerson, E., Halpern, J.: "Sometimes" and "Not Never" revisited: on branching versus linear time. Journal of the ACM **33** (1986) 151–178
16. Moor, T., Davoren, J.: Robust controller synthesis for hybrid systems using modal logic. In: Hybrid Systems: Computation and Control (HSCC'01). LNCS 2034, Springer-Verlag (2001) 433–446