On simulations and bisimulations of general flow systems

Jen Davoren

Department of Electrical & Electronic Engineering
The University of Melbourne, AUSTRALIA

and

Paulo Tabuada

Department of Electrical Engineering
The University of California at Los Angeles, USA

Outline

- Introduction and motivation: logics and systems
- Foundations: time-lines, bounded paths, operations on paths
- General flow systems: definition, properties, examples, maximal extensions
- Relationships between general flow systems
- The logic $\mathbf{GFL}^{\star}$: semantics and examples of expressivity
- Semantic preservation theorem for p-bisimulation relations
- Conclusions and further work

Introduction and motivation

Temporal logics for non-deterministic or “branching” dynamics:

$\star$ On top of classical propositional logic (AND, OR, NOT, IMPLIES)

$\star$ 2-place operator on paths: φ UNTIL ψ

$\star$ 1-place operator on paths: NEXT φ or IMMEDIATELY-AFTER-NOW φ

$\star$ $\forall$ and $\exists$ quantification over paths: $\forall\varphi$ and $\exists\varphi$

In discrete time, logic $\mathbf{CTL}^\star$ = Full Computation Tree Logic with semantics over ω-length state sequences in Kripke models/transition systems, successfully used for hardware and software verification and design.

General dynamical systems

- Want to provide infrastructure for logic-based analysis and design of systems: semantics for the language of “full” non-deterministic temporal logic over paths/trajectories of a class of general dynamical models.
- Want set-theoretic minimalism of Aubin’s evolutionary systems, and Willems’ behavioural systems but not restricted to Time = Integers or Reals, as want to formalize hybrid time domains as sets of time positions $(i, t) \in \mathbb{N} \times \mathbb{R}_0^+$.
- Want to model all variations of hybrid and hierarchical systems, and provide framework in which models of different types can be compared.
- Want finite or bounded paths as basic objects in model.
- Want to express in temporal logic concepts such as Aubin’s notions of viability with target and invariance with target using $\forall$, $\exists$ and UNTIL constructs.
- Want to develop notions of simulation and bisimulation that preserve the semantics of the logic, and also allow comparison of models over differing time lines.

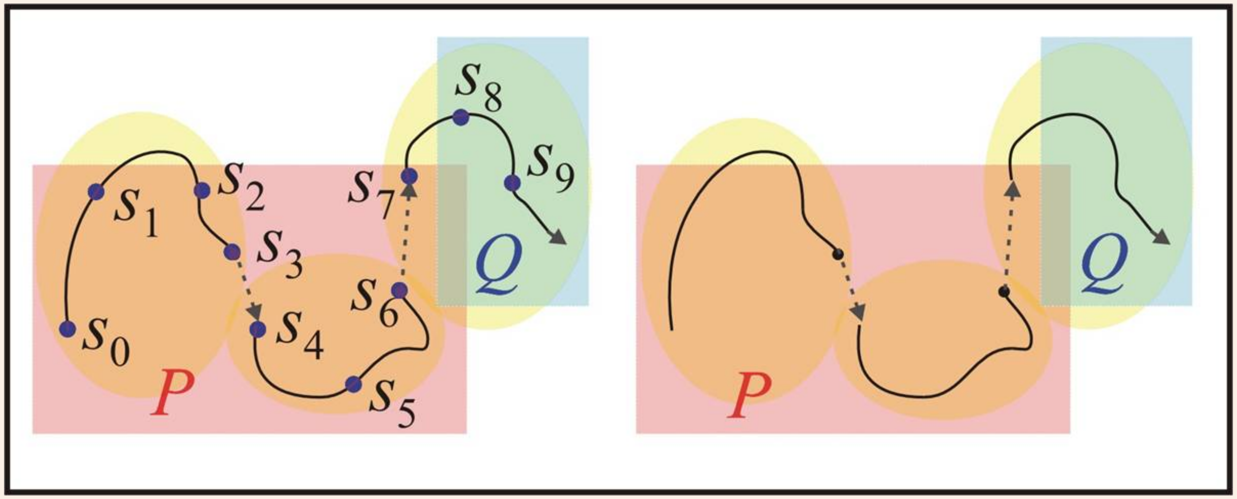
Semantics in hybrid system models

Transition system semantics for hybrid systems:

path = discrete execution sequence

= "sampling" of hybrid trajectory

$$\exists(\, P \,\mathrm{UNTIL}\, Q \,)$$



Outline

- Introduction and motivation: logics and systems
- Foundations: time-lines, bounded paths, operations on paths
- General flow systems: definition, properties, examples, maximal extensions
- Relationships between general flow systems
- The logic $\mathbf{GFL}^\star$: semantics and examples of expressivity
- Semantic preservation theorem for p-bisimulation relations
- Conclusions and further work

Foundations: maps

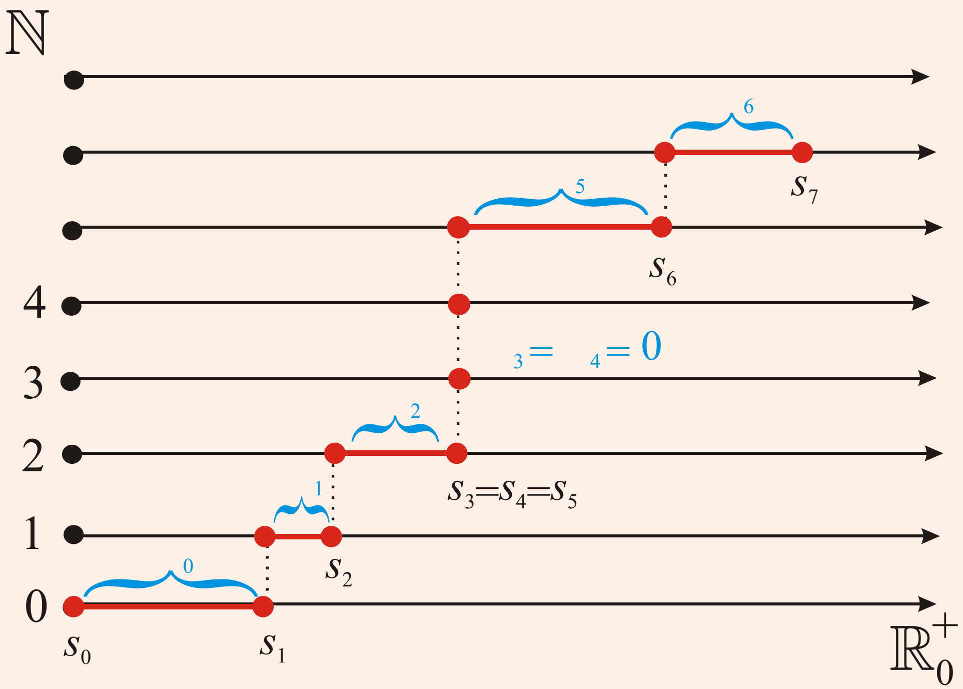
Set-valued maps/relations $r : X \rightsquigarrow Y$ with values $r(x) \subseteq Y$, with converse $r^{-1} : Y \rightsquigarrow X$; domain $\mathrm{dom}(r) := \{x \in X \mid r(x) \neq \varnothing\}$; range $\mathrm{ran}(r) := \mathrm{dom}(r^{-1}) \subseteq Y$; and r is *total on X* if $\mathrm{dom}(r) = X$.

Single-valued functions $r : X \to Y$ with values $r(x) = y$ instead of $r(x) = \{y\}$.

Partial functions $r : X \dashrightarrow Y$, i.e. on $\mathrm{dom}(r) \subseteq X$, r is single-valued. Write $r(x) = y$ when $x \in \mathrm{dom}(r)$ with value y, and $r(x) =$ UNDEF when $x \notin \mathrm{dom}(r)$.

So as sets of maps, $[\,X \to Y\,] \subseteq [\,X \dashrightarrow Y\,] \subseteq [\,X \rightsquigarrow Y\,]$.

Time domain of a bounded hybrid path



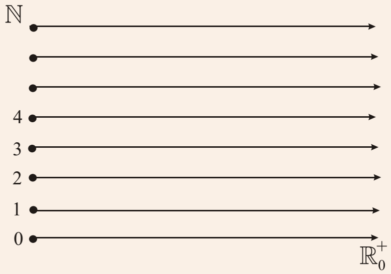
switching times $s_0 := 0$; $\quad s_i := \sum_{j<i} \Delta_j$;
$\mathrm{dom}(\gamma) = \bigcup_{i<N} \{i\} \times [s_i, s_{i+1}]$.

Examples of time lines

Discrete time line $\mathbb{N}$, non-negative half of linearly ordered abelian group $\mathbb{Z}$.

Continuous time line $\mathbb{R}_0^+$, non-negative half of linearly ordered abelian group $\mathbb{R}$.

Hybrid time line $\mathbb{H} := \mathbb{N} \times \mathbb{R}_0^+$, non-negative quarter of $\mathbb{Z} \times \mathbb{R}$, lexicographic order: $(i, t) <_{\text{lex}} (j, s)$ iff $i < j$ or ($i = j$ and $t < s$).



Discrete hybrid time line $\mathbb{N} \times \mathbb{N}$, non-negative quarter of $\mathbb{Z} \times \mathbb{Z}$.

Meta-hybrid time line $\mathbb{N} \times \mathbb{N} \times \mathbb{R}_0^+$ for hierarchical hybrid systems.

Higher-dimensional time lines for systems with multiple time scales.

Foundations: time lines

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 $d_L : (L \times L) \longrightarrow \mathbb{R}_0^{+\infty}$ together with a continuous order-preserving total function (a *fibering map*) $p : L \longrightarrow M$ 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 $a, b, c \in L,\ a \leqslant c,\ d_L(a, c) < \infty$,

$$d_L(a, c) = d_L(a, b) + d_L(b, c) \text{ iff } a \leqslant b \leqslant c;$$

(d) for all $a, b, c \in L$, $\quad d_L(b, c) = d_L(a + b, a + c)$.

Foundations: time lines

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 any time line L, and any initial subset $T \subseteq L$ with $0 \in T$, define the *progress set* $\mathrm{Pro}(T) \subset T$ by:

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

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 $s_T := \min(\mathrm{ran}(\mathrm{succ}_T))$; if T is everywhere dense, so $\mathrm{ran}(\mathrm{succ}_T) = \varnothing$, then $\mathrm{Pro}(T) = T - \{0\}$.

Foundations: time lines

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 *$<$-bounded* otherwise.

For any subset $T \subseteq L$, define the set's *total duration* $\mathrm{dur}(T) \in \mathbb{R}_0^{+\infty}$ as follows:

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

A subset $T \subseteq L$ will be called *duration-bounded* if $\mathrm{dur}(T) < \infty$, and *duration-unbounded* otherwise.

Bounded time domains and paths

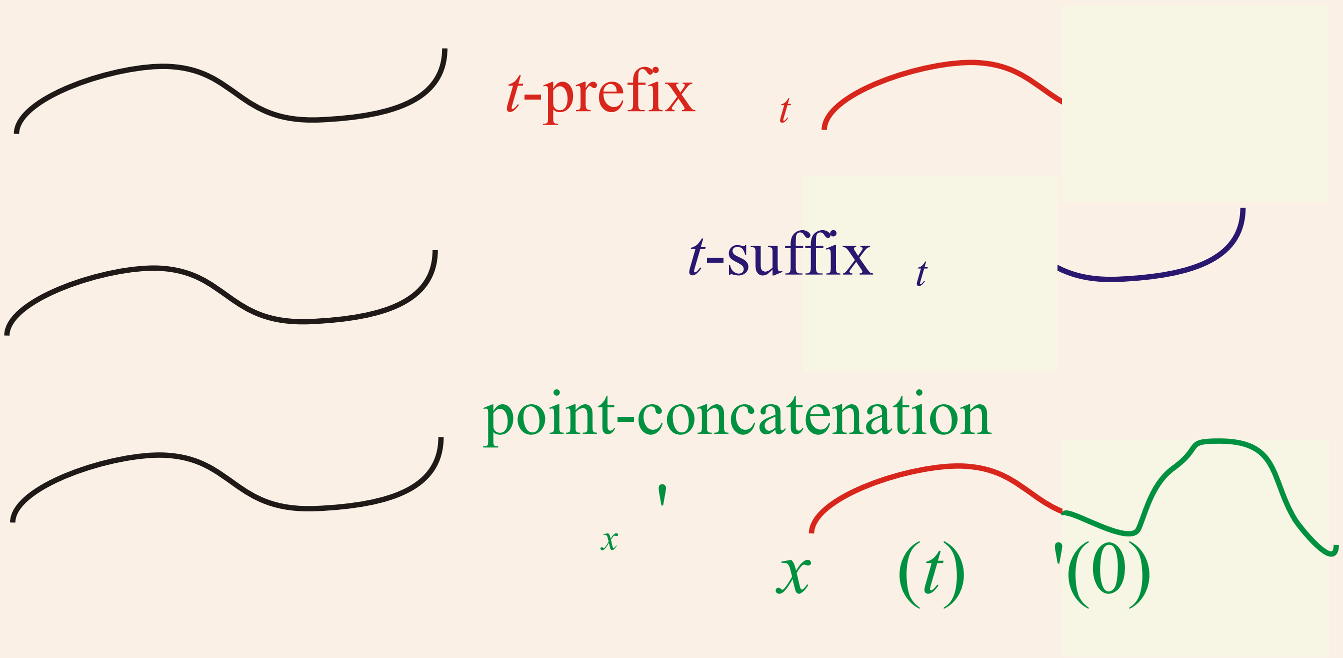
Given a time line L, define a *bounded time domain* in L to be a subset $T \subset L$ such that T is a finite union of closed and duration-bounded intervals, of the form $T = \bigcup_{n<N}[a_n, b_n]$ with $N \in \mathbb{N}^+$, $a_0 = 0$, $b_{N-1} = b_T := \max(T)$, and $a_n \leqslant b_n < a_{n+1} \leqslant b_{n+1}$ 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. Over any set $X \neq \varnothing$, define:

$$\begin{array}{rcl} \mathsf{BI}(L) & := & \{T \in \mathsf{BT}(L) \mid (\exists b \in L)\, T = [0, b]\,\} \\ \mathsf{Path}(L, X) & := & \{\,\gamma : L \dashrightarrow X \mid \mathrm{dom}(\gamma) \in \mathsf{BT}(L)\,\} \\ \mathsf{IPath}(L, X) & := & \{\,\gamma : L \dashrightarrow X \mid \mathrm{dom}(\gamma) \in \mathsf{BI}(L)\,\} \end{array}$$

A path is a partial function whose domain is a bounded time domain.

Operations on paths



identity path at x is θ_x with dom(θ_x) = [0,0], $\theta_x(0) = x$

Partial order on paths

Given a time line L, the set $\mathrm{BT}(L)$ is *partially ordered* via the linear ordering on L: for $T, T' \in \mathrm{BT}(L)$, 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:

$$\gamma < \gamma' \text{ iff } \gamma \subset \gamma' \text{ and } \mathrm{dom}(\gamma) < \mathrm{dom}(\gamma')$$

in which case we say the path γ' is a (proper) *extension* of γ.

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

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

Outline

- Introduction and motivation: logics and systems
- Foundations: time-lines, bounded paths, operations on paths
- General flow systems: definition, properties, examples, maximal extensions
- Relationships between general flow systems
- The logic $\mathbf{GFL}^{\star}$: semantics and examples of expressivity
- Semantic preservation theorem for p-bisimulation relations
- Conclusions and further work

General flow systems

Definition: 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 set-valued map $\Phi\colon X \rightsquigarrow \mathtt{Path}(L, X)$ satisfying, for all $x \in dom(\Phi)$, for all $\gamma \in \Phi(x)$, and for all $t \in dom(\gamma)$:

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

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

(GF2) *point-concatenation-closure*: $\forall\, \gamma' \in \Phi(\gamma(t)),\ \ \gamma|_t * \gamma' \in \Phi(x)$

Examples of general flow systems

- State-machines (discrete-time transition systems), incl. input-state-output (Mealy) state machines
- Differential equations or inclusions (continuous time), incl. input-state-output control systems
- Aubin's evolutionary systems (continuous time or discrete time)
- Willems' time-invariant state behaviours (continuous time or discrete time)
- Hybrid automata, switched continuous systems (hybrid time, discrete hybrid time)
- Impulse differential inclusions (hybrid time)
- Stochastic hybrid systems (hybrid time, discrete hybrid time)
- Meta-hybrid automata (time line $\mathbb{N} \times \mathbb{N} \times \mathbb{R}_0^+$)

Properties of general flow systems

- Φ is *reflexive* if $\theta_x \in \Phi(x)$ for all $x \in dom(\Phi)$;
- Φ is *deadlocked at x* if $\Phi(x) = \{\theta_x\}$;
- Φ is *deadlock-free* if not deadlocked at any $x \in X$;
- Φ is *prefix-closed* if $\gamma|_t \in \Phi(x)$
  for all $x \in dom(\Phi)$, $\gamma \in \Phi(x)$ and $t \in dom(\gamma)$;
- Φ is *deterministic* if $\forall x \in \mathrm{dom}(\Phi)$, set $\Phi(x)$ linearly ordered by $<$;
- Φ is *$<$-unbounded* if $\forall x \in \mathrm{dom}(\Phi)$, path set $\Phi(x)$ is $<$-unbounded;
- Φ is *point-controllable* 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* 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 $(\gamma' *_{x'} \gamma|_t *_{x''} \gamma'') \in \Phi(x)$.

Infinitary extensions

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 *limit-extension* of $\mathcal{P}$:

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

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

Limit paths are unions of strictly-extending chains of paths, where the chains are of limit ordinal length less than or equal to that of line L.

Maximal extensions

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 $\mathsf{M}(\mathcal{P}) \subseteq \mathsf{Ext}(\mathcal{P}) \subseteq \mathsf{EPath}(L,X)$ where:

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

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.

Maximal extensions

Theorem: [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 MΦ is a partial function.

Outline

- Introduction and motivation: logics and systems
- Foundations: time-lines, bounded paths, operations on paths
- General flow systems: definition, properties, examples, maximal extensions
- Relationships between general flow systems
- The logic $\mathbf{GFL}^{\star}$: semantics and examples of expressivity
- Semantic preservation theorem for p-bisimulation relations
- Conclusions and further work

Reachability (bi-)simulations

First, capture the "*time-abstract*" simulation and bisimulation notion for *transition system representations* of hybrid, continuous and discrete systems (used in current finite bisimulation results e.g. o-minimal HA).

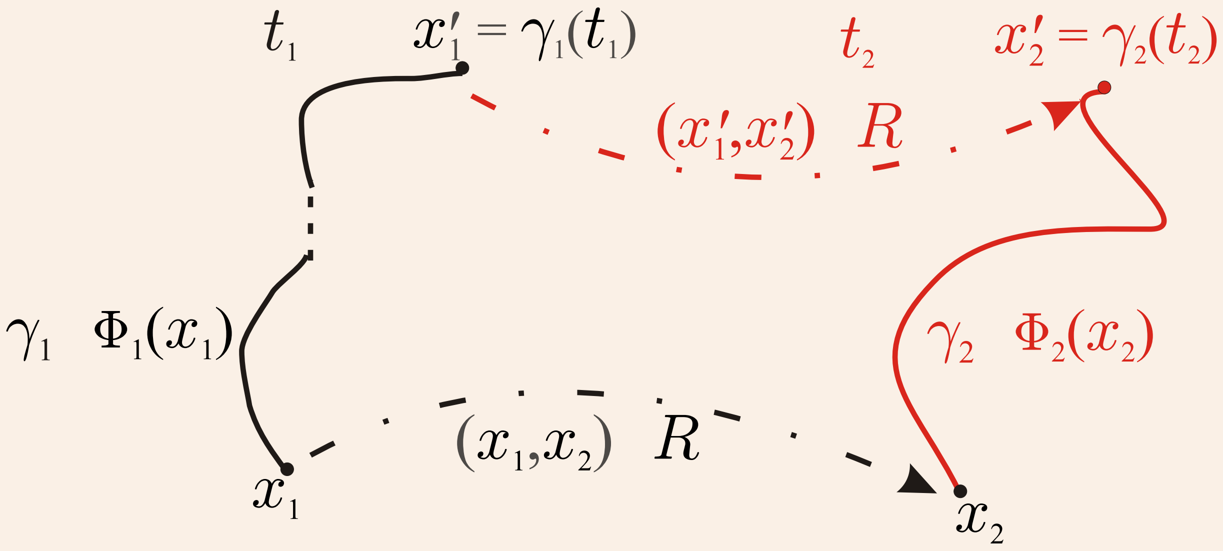
Definition: Given time lines L_1 and L_2, possibly different, and $\Phi_1 \colon X_1 \rightsquigarrow \mathsf{Path}(L_1, X_1)$, $\Phi_2 \colon X_2 \rightsquigarrow \mathsf{Path}(L_2, X_2)$, $R : X_1 \rightsquigarrow X_2$ is a *reachability simulation* (or *r-simulation*) of Φ_1 by Φ_2 if $\mathrm{dom}(\Phi_1)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

Reachability (bi-)simulations

if $(x_1, x_2) \in R$ and $\exists\ \gamma_1 \in \Phi_1(x_1)$ and $t_1 \in \mathrm{dom}(\gamma_1)$ s.t. $t_1 > 0$ and $x'_1 = \gamma_1(t_1)$,
then $\exists\ x'_2 \in X_2$ and $\gamma_2 \in \Phi_2(x_2)$ and a time point $t_2 \in \mathrm{dom}(\gamma_2)$ s.t. $t_2 > 0$ and $x'_2 = \gamma_2(t_2)$ and $(x'_1, x'_2) \in R$.



Progress (bi-)simulations

Next, a slightly stronger notion of simulation and bisimulation which requires some “matching” of time points along paths, but not an exact matching, so still can compare systems over different time lines, like r-(bi-)simulations.

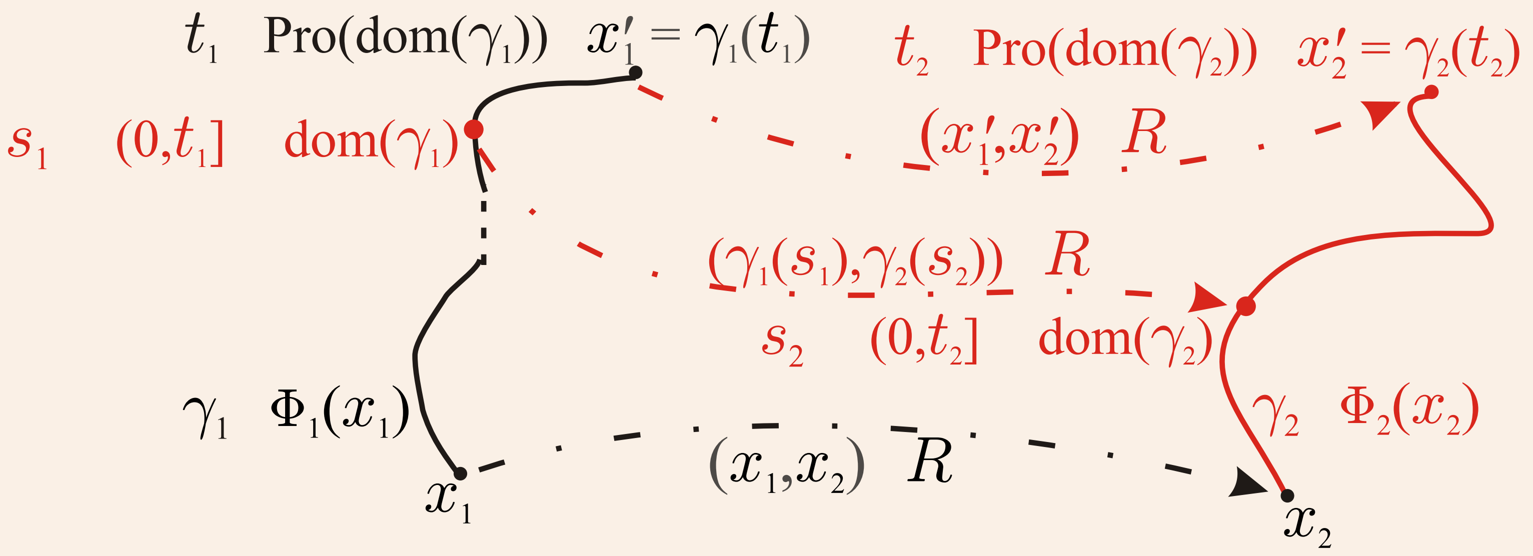
Definition: Given time lines L_1 and L_2, possibly different, and $\Phi_1\colon X_1 \rightsquigarrow \mathsf{Path}(L_1, X_1)$, $\Phi_2\colon X_2 \rightsquigarrow \mathsf{Path}(L_2, X_2)$, $R : X_1 \rightsquigarrow X_2$ is a *progress simulation* (or *p-simulation*) of Φ_1 by Φ_2 if $\mathrm{dom}(\Phi_1)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

Map $R : X_1 \rightsquigarrow X_2$ is a *progress bisimulation* (or *p-bisimulation*) between Φ_1 and Φ_2 if both R and R^{-1} are p-simulations.

Progress (bi-)simulations

if $(x_1, x_2) \in R$ and $\exists\, \gamma_1 \in \Phi_1(x_1)$ and $t_1 \in \mathrm{Pro}(\mathrm{dom}(\gamma_1))$ s.t. $x_1' = \gamma_1(t_1)$,
then $\exists\, x_2' \in X_2$ and $\gamma_2 \in \Phi_2(x_2)$ and $t_2 \in \mathrm{Pro}(\mathrm{dom}(\gamma_2))$ s.t. $x_2' = \gamma_2(t_2)$
and $(x_1', x_2') \in R$, and $\forall\, s_2 \in (0, t_2] \cap \mathrm{dom}(\gamma_2)$, $\exists\, s_1 \in (0, t_1] \cap \mathrm{dom}(\gamma_1)$
such that $(\gamma_1(s_1), \gamma_2(s_2)) \in R$.


t_1 $\mathrm{Pro}(\mathrm{dom}(\gamma_1))$ $x_1' = \gamma_1(t_1)$
t_2 $\mathrm{Pro}(\mathrm{dom}(\gamma_2))$ $x_2' = \gamma_2(t_2)$
s_1 $(0,t_1]$ $\mathrm{dom}(\gamma_1)$
(x_1',x_2') R
$(\gamma_1(s_1),\gamma_2(s_2))$ R
s_2 $(0,t_2]$ $\mathrm{dom}(\gamma_2)$
γ_1 $\Phi_1(x_1)$
γ_2 $\Phi_2(x_2)$
(x_1,x_2) R
x_1
x_2

Timed (bi-)simulations

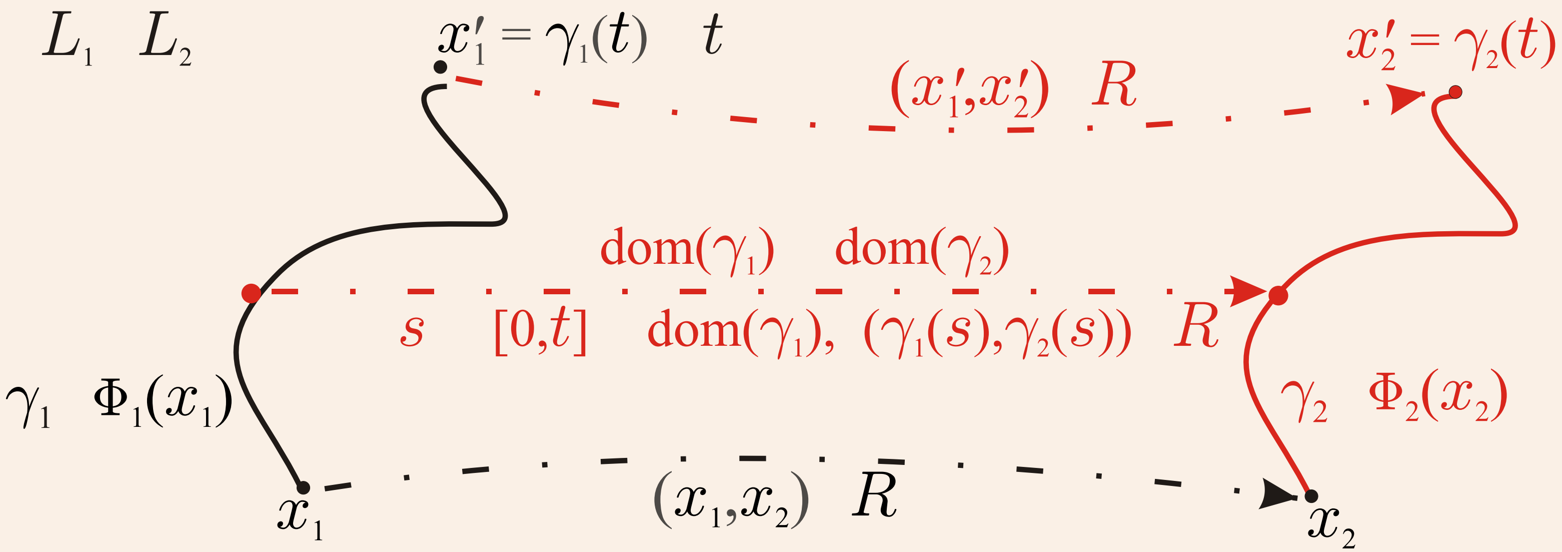
Finally, the strongest notion that requires the two systems to have the same time lines, and exact matching along paths.

Definition: Given $\Phi_1 \colon X_1 \rightsquigarrow \mathsf{Path}(L, X_1)$ 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 $\exists\, \gamma_1 \in \Phi_1(x_1)$ such that $x_1' = \gamma_1(t)$,
then $\exists\, x_2' \in X_2$ 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.

Timed (bi-)simulations

if $(x_1, x_2) \in R$ and $\exists\, \gamma_1 \in \Phi_1(x_1)$ s.t. $x_1' = \gamma_1(t)$,
then $\exists\ x_2' \in X_2$ and $\gamma_2 \in \Phi_2(x_2)$ s.t. $x_2' = \gamma_2(t)$ and $(x_1', x_2') \in R$, and $\mathrm{dom}(\gamma_2) = \mathrm{dom}(\gamma_1)$ and $\forall\, s \in [0, t] \cap \mathrm{dom}(\gamma_1)$, it holds that $(\gamma_1(s), \gamma_2(s)) \in R$.



Examples of simulation relationships

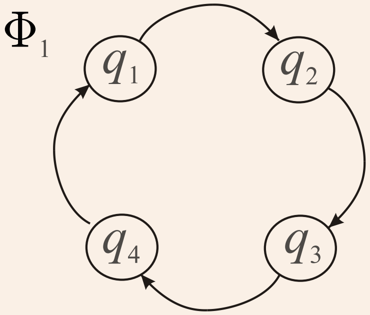
1. Discrete-time det. system $\Phi_1 : X_1 \rightsquigarrow \mathsf{Path}(\mathbb{N}, X_1)$ over space $X_1 := \{q_1, q_2, q_3, q_4\}$ generated by $\delta : X_1 \to X_1$ with $\delta(q_k) := q_{k+1}$ for $k = 1, 2, 3$ and $\delta(q_4) = q_1$.

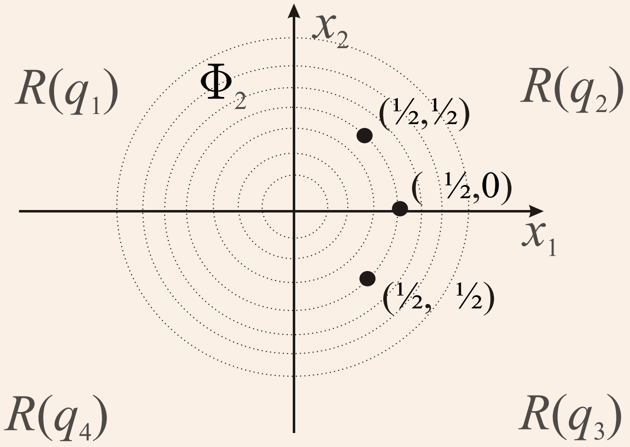
2. Continuous-time det. system $\Phi_2 : X_2 \rightsquigarrow \mathsf{Path}(\mathbb{R}_0^+, X_2)$ over space $X_2 := \mathbb{R}^2 - \{(0, 0)\}$ given by diff. equation: $\dot{x}_1 = x_2$ and $\dot{x}_2 = -x_1$. So $\Phi_2(x_1, x_2) = \{\gamma : [0, b] \to X_2 \mid b \geq 0 \wedge (\forall t \in \mathrm{dom}(\gamma))\, \gamma(t) = (x_1 \cos(t) + x_2 \sin(t), x_2 \cos(t) - x_1 \sin(t))\}$; paths correspond to circular motion in clockwise direction, with radius $r = \sqrt{x_1^2 + x_2^2}$.

Examples of simulation relationships

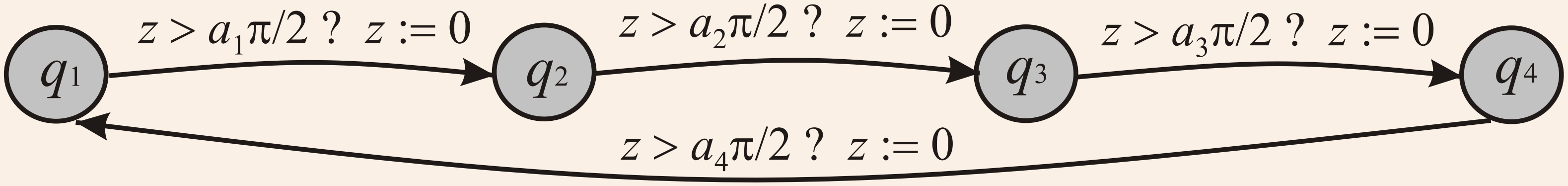
Then consider the relation $R : X_1 \rightsquigarrow X_2$ given by:

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





Then R is r-simulation of discrete Φ_1 by cont. Φ_2, but not p-simulation.


q_1
q_2
q_3
q_4
$z > a_1\pi/2$? $z := 0$
$z > a_2\pi/2$? $z := 0$
$z > a_3\pi/2$? $z := 0$
$z > a_4\pi/2$? $z := 0$

3. Hybrid time system: timed automaton H over space $X_3 := \bigcup_{k\in K}\{q_k\}\times[0,(a_k+1)\frac{\pi}{2}]$, where z is (sole) clock variable and for $k \in K = \{1,2,3,4\}$, $a_k > 0$ are fixed real constants, and $\Phi_3 : X_3 \rightsquigarrow \mathsf{Path}(\mathbb{H}, X_3)$ its general flow.

Then consider the relation $S : X_3 \rightsquigarrow X_2$ defined for all $z \in \mathbb{R}_0^+$ by:

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

Then S is a p-bisimulation between hybrid system Φ_3 and continuous system Φ_2, but it cannot be a t-bisimulation.

Outline

- Introduction and motivation: logics and systems
- Foundations: time-lines, bounded paths, operations on paths
- General flow systems: definition, properties, examples, maximal extensions
- Relationships between general flow systems
- The logic $\mathbf{GFL}^{\star}$: semantics and examples of expressivity
- Semantic preservation theorem for p-bisimulation relations
- Conclusions and further work

Syntax of the logic $\mathbf{GFL}^{\star}$

(Same syntax as $\mathbf{CTL}^{\star}$.) Let Prp be a non-empty countable (finite or infinite) set of atomic propositions. The temporal logic language $\mathcal{F}(\mathrm{Prp})$ consists of the set of all formulas φ generated by the grammar:

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

Define logical constants *true*, $\top \overset{\text{def}}{=} p \vee \neg\,p$, for any $p \in \mathrm{Prp}$, and *false*, $\bot \overset{\text{def}}{=} \neg\top$. The other propositional (Boolean) connectives are defined in a standard way, and the path quantifier $\forall$ has a classical negation dual $\exists$, as follows:

$$\varphi_1 \wedge \varphi_2 \quad \overset{\text{def}}{=} \quad \neg\,(\neg\,\varphi_1 \ \vee \ \neg\varphi_2) \qquad\qquad \varphi_1 \rightarrow \varphi_2 \quad \overset{\text{def}}{=} \quad \neg\,\varphi_1 \ \vee \ \varphi_2$$

$$\varphi_1 \leftrightarrow \varphi_2 \quad \overset{\text{def}}{=} \quad (\varphi_1 \rightarrow \varphi_2) \wedge (\varphi_2 \rightarrow \varphi_1) \qquad\qquad \exists\,\varphi \quad \overset{\text{def}}{=} \quad \neg\,\forall\neg\,\varphi$$

Semantics of $\mathbf{GFL}^{\star}$

A *general flow logic model* for the proposition set Prp is a structure $\mathfrak{M} = (X, L, \Phi, \mathcal{P})$, where:

- $X \neq \varnothing$ is the state space, of arbitrary non-zero cardinality;

- L is a time line;

- Φ is a deadlock-free general flow system $\Phi : X \rightsquigarrow \mathsf{Path}(L, X)$ over the space X, with time line L;

- $\mathcal{P} : \mathrm{Prp} \rightsquigarrow X$ maps each $p \in \mathrm{Prp}$ to a set $\mathcal{P}(p) \subseteq X$ of states.

The *maximal path space* of $\mathfrak{M}$ is $\mathsf{MPath}(\mathfrak{M}) := \mathrm{ran}(\mathsf{M}\Phi)$.

Semantics of $\mathbf{GFL}^\star$

For $\varphi \in \mathcal{F}(\mathrm{Prp})$ 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 $p \in \mathrm{Prp}$:

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

Semantics of $\mathbf{GFL}^\star$

For formulas $\varphi \in \mathcal{F}(\mathrm{Prp})$, 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:

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

For a logic model $\mathfrak{M} \in \mathbb{GF}(\mathrm{Prp})$, state x in the state space of $\mathfrak{M}$, and for formulas $\varphi \in \mathcal{F}(\mathrm{Prp})$, we say:

- φ is *satisfied* in $\mathfrak{M}$ at state x, if $x \in [\![\,\varphi\,]\!]^{\mathfrak{M}}_{\mathsf{st}}$;
- φ is *satisfiable* in $\mathfrak{M}$, if $[\![\,\varphi\,]\!]^{\mathfrak{M}}_{\mathsf{st}} \neq \varnothing$ (equivalently, $[\![\,\varphi\,]\!]^{\mathfrak{M}} \neq \varnothing$);
- φ is *true* in $\mathfrak{M}$, written $\mathfrak{M} \models \varphi$, if $\mathfrak{M}, \eta \models \varphi$ for every $\eta \in \mathsf{MPath}(\mathfrak{M})$.

Expressing properties in $\mathbf{GFL}^\star$

- As in $\mathbf{CTL}^\star$, safety, liveness, fairness.
- Event-sequence behaviour of hybrid trajectories.
- Aubin's notion of *viability with target* and *invariance with target*.
- Point-controllability and path-controllability (via a rule scheme).
- Determinism (via a formula scheme): $\exists\,\varphi \rightarrow \forall\,\varphi$.

Outline

- Introduction and motivation: logics and systems
- Foundations: time-lines, bounded paths, operations on paths
- General flow systems: definition, properties, examples, maximal extensions
- Relationships between general flow systems
- The logic $\mathbf{GFL}^{\star}$: semantics and examples of expressivity
- Semantic preservation theorem for p-bisimulation relations
- Conclusions and further work

$\mathbf{GFL}^{\star}$ preservation by p-bisimulations

Definition: Fix a set of atomic propositions Prp, and for $i = 1, 2$, let $\mathfrak{M}_i = (X_i, L_i, \Phi_i, \mathcal{P}_i)$ be a logic model for proposition set Prp, with $\Phi_i \colon X_i \rightsquigarrow \mathsf{Path}(L_i, X_i)$ a (deadlock-free) general flow system.
A relation $R : X_1 \rightsquigarrow X_2$ is a *p-simulation* of model $\mathfrak{M}_1$ by model $\mathfrak{M}_2$ if:
$\mathrm{(i)}$ relation R is a p-simulation of Φ_1 by Φ_2; and
$\mathrm{(ii)}$ 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 $\mathfrak{M}_1$.

$\mathbf{GFL}^\star$ preservation by p-bisimulations

Theorem: Fix a set of atomic propositions Prp, and for $i = 1, 2$, let $\mathfrak{M}_i = (X_i, L_i, \Phi_i, \mathcal{P}_i)$ be two logic models over propositions Prp, 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 $x_2 \in X_2$,

if $x_1 \, B \, x_2$, *then* for all $\varphi \in \mathcal{F}(\mathrm{Prp})$, $\left[x_1 \in [\![\varphi]\!]^{\mathfrak{M}_1}_{\mathsf{st}} \Leftrightarrow x_2 \in [\![\varphi]\!]^{\mathfrak{M}_2}_{\mathsf{st}} \right]$.

Corollary: 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 $\varphi \in \mathcal{F}(\mathrm{Prp})$, $\mathfrak{M}_1 \models \varphi$ iff $\mathfrak{M}_2 \models \varphi$.

Example: atomic props $\mathrm{Prp} = \{q_1, q_2, q_3, q_4\}$. Model $\mathfrak{M}_2$ over X_2 with one system Φ_2, with continuous time $L_2 = \mathbb{R}^+_0$, and model $\mathfrak{M}_3$ over X_3 with one system Φ_3, with hybrid time $L_3 = \mathbb{H}$, are p-bisimilar. Consider formula $\varphi = \forall \, (q_1 \mathbf{U} q_2 \wedge q_2 \mathbf{U} q_3 \wedge q_3 \mathbf{U} q_4 \wedge q_4 \mathbf{U} q_1)$.

Outline

- Introduction and motivation: logics and systems
- Foundations: time-lines, bounded paths, operations on paths
- General flow systems: definition, properties, examples, maximal extensions
- Relationships between general flow systems
- The logic $\mathbf{GFL}^\star$: semantics and examples of expressivity
- Semantic preservation theorem for p-bisimulation relations
- Conclusions and further work

Conclusions and further work

- Have developed new bisimulation concept that is adequate to preserve semantics of a temporal logic that (a) concides with well-known logic $\mathbf{CTL}^\star$ for discrete time, and (b) is rich enough to capture hybrid dynamics (and more) in their full complexity.
- Existing results on decidability of model-checking via finite bisimulations for certain classes of systems only apply to fragment of logic $\mathbf{GFL}^\star$ because they are only r-bisimulations, and not p-bisiumlations. More work to see what extensions possible.
- To express properties with topological or metric content (e.g. stability, robustness), need to both enrich logic with topological/metric operators, and then to enrich concept of (bi-)simulation accordingly (to preserve whatever structure there is).
- Notions of δ-approximate p-(bi-)simulations also to be examined.

blank