Modal Logic and Bisimulation for Generalized Synchronization Trees

James Ferlez†, Rance Cleaveland§ and Steve Marcus†

§Department of Computer Science & †Department of Electrical and Computer Engineering

University of Maryland — The Institute for Systems Research

CPS Program Information

- CPS Breakthrough: ***Compositional Modeling of Cyber-Physical Systems*** *(NSF Grant: CNS-1446665)*
- PIs: Rance Cleaveland and Steve Marcus

HML and Weak Bisimulation for GSTs

- **Modal logic** has long been used to study transition systems **via bisimulation** [3].
- Modal quantifiers express "possibility" or "necessity" in an "alternate world"
  - For transition systems, "alternate world" = successor state
  - Unlike 1st-order logic in that quantifiers are restricted (to successors).
- **Can we study bisimulation for Cyber-Physical Systems (CPSs) using modal logic?**

Synchronization Trees (STs)

Famously, Milner [5] devised **synchronization trees** for labeled transition systems:

Definition:

A **Synchronization Tree (ST)** over a set of labels $\mathcal{L}$ is an undirected, connected, acyclic graph with a specially identified root node, r.

- Bisimulation is a natural (observational) notion of equivalence between trees.
- Each vertex has a unique incoming edge: vertices may be identified with sub-trees!
- Operations on tree create new trees from old ones. For example:
  - Make a tree's root the **target** of a new edge;
  - **Identify** the root nodes of two trees.
- These operations make STs ideal models for the study of modal logics.

Hennessy-Milner Logic (HML) and STs

- Hennessy and Milner noticed a relationship between bisimulation and a simple modal logic that would become known as Hennessy-Milner Logic (HML). [3]
- Consider the following (inductively defined) modal logic ($\ell \in L$, the set of labels) :

$$\varphi := \top \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \langle \ell \rangle \varphi$$

- **Notation:** let p and q be two STs. Then let
  - $p \leftrightarroweq q$ denote that p and q are bisimilar; and
  - $p \approx_{\text{HML}} q$ denote that p and q satisfy the same HML formulas.

Theorem: [3]

For any two **image-finite STs** p and q, $\quad p \leftrightarroweq q \Leftrightarrow p \approx_{\text{HML}} q.$

(A ST is **image-finite** if each node has at most finitely many ℓ-successors for each label ℓ.)

- Similar theorems are called **Hennessy-Milner Theorems**.

Hennessy-Milner Classes of STs

- Image finite STs are one class of STs for which there is a Hennessy-Milner theorem. There are other such classes, and this is made precise in the following definition:

Definition: [2]

(Visser-Hollenberg Hennessy-Milner Property) Let $\mathfrak{h}$ be a class of STs. $\mathfrak{h}$ **satisfies the VHHM property (or is a VHHM class)** if:

For all $p, q \in \mathfrak{h}$ and **all nodes** p' **and** q' **in** p **and** q, respectively,

$$p' \leftrightarroweq q' \Leftrightarrow p' \approx q'. \quad \bigstar$$

VHHM classes are often called just **Hennessy-Milner Classes**; but sometimes ★ is enforced only on root nodes, and this is a different notion! [2] *(see third column ⟶)*

Maximal VHHM Classes of STs

- **Maximal** (in a set theoretic sense) VHHM classes can be characterized in terms of the **Canonical Model for the smallest normal logic,** K.
- $\mathbf{C}^\Lambda$ - the Canonical Model for a logic Λ - is **the** Kripke structure defined so its
  - *states* are maximally consistent **sets of formulas**; and its
  - *transitions* respect the formulas **within a state** (modally saturated).

Maximal VHHM Classes of STs (continued)

Theorem: [4]

For any state s in $\mathbf{C}^\Lambda$ and any modal formula φ: $\quad s \models \varphi \;\Leftrightarrow\; \varphi \in s$

- $\mathbf{C}^\Lambda$ "maximally" satisfies the above property, but not uniquely!

Definition: [4]

A Kripke structure with the same states as $\mathbf{C}^\Lambda$ is called **Henkin-like** (denoted $\mathbf{HC}^\Lambda$) if

- its transitions are a subset of $\mathbf{C}^\Lambda$'s; and
- $s \models \varphi \Leftrightarrow \varphi \in s$ for all states s and formulas φ.

Theorem: [4]

Let $\mathrm{BS}(\mathbf{HC}^K)$ be the Kripke structures that are bisimilar to a sub-model of $\mathbf{HC}^K$. Then:

- for every $\mathbf{HC}^K$, $\mathrm{BS}(\mathbf{HC}^K)$ is a maximal VHHM class; and
- every maximal VHHM class $\mathfrak{h}$ equals $\mathrm{BS}(\mathbf{HC}^K)$ for some Henkin-like model $\mathbf{HC}^K$.

Generalized Synchronization Trees (GSTs)

Idea: generalize STs to enable modeling of cyber-physical systems (CPSs) [1].

Definition: [1]

A **tree** is a partially ordered set $(P, \preceq)$ with the following two properties:

1. There is a p_0 s.t. $p_0 \preceq p$ for all $p \in P$; p_0 is the root of the tree.
2. For each $p \in P$, the set $[p_0, p] \triangleq \{p' \in P | p' \preceq p\}$ is *linearly ordered* by $\preceq$.

Definition: [1]

A **Generalized Synchronization Tree (GST)** [1] over a let of labels L is a tree $(P, \preceq, p_0)$ along with a labeling function $\mathcal{L} : P \backslash \{p_0\} \to L$.

(Weak) Bisimulation for GSTs

Let $G_P = (P, p_0, \preceq_P, \mathcal{L}_P)$ and $G_Q = (Q, q_0, \preceq_Q, \mathcal{L}_Q)$ be GSTs.

Definition: [1]

G_P **weakly simulates** G_Q [1] if there is a relation $R \subseteq P \times Q$ s.t. $(p_0, q_0) \in R$ and

- For any $(p, q) \in R$ and $q' \succeq q$ there is a $p' \succeq p$ s.t. $(p', q') \in R$, and there is an order-preserving bijection $\lambda : (p, p'] \to (q, q']$ s.t. $\forall r \in (p, p'].(r, \lambda(r)) \in R$.

Notions like this are common in the literature; compare also to **strong bisimulation** [1].

HML for GSTs

- Note the relationship between STs and HML: $\langle \ell \rangle$ **mirrors the idea of an** ℓ**-transition!**
- Generalizing HML is about generalizing $\langle \ell \rangle$ and the notion of an ℓ-transition!

Idea: "label" modalities with functions over an auxiliary totally ordered set (that thus specifies the logic):

Definition(s): [2]

- A **domain of modalities** is a totally ordered set $(\mathscr{I}, \preceq_{\mathscr{I}})$ and a set of labels, L.
- A **modal execution** is a map from a left-open subset of $\mathscr{I}$ to L; denote the set of modal executions by $\mathscr{M}(\mathscr{I}, L)$.

(Left-open subsets are those that: **don't** contain a GLB and **do** contain a LUB.)

Generalized Hennessy-Milner Logic: Syntax

- We define GHML in terms of *equivalence classes* of modal executions:

Definition: [2]

$E_1 : I_1 \to L$ and $E_2 : I_2 \to L$ in $\mathscr{M}(\mathscr{I}, L)$ are **order equivalent** if there is an order preserving bijection $\lambda : I_1 \to I_2$ such that for all $x \in I_1$

$$E_1(x) = E_2(\lambda(x)).$$

$|\mathscr{M}(\mathscr{I}, L)|$ denotes the set of all such equiv. classes; $|E|$ the equiv. class of $E \in \mathscr{M}(\mathscr{I}, L)$.

Definition: [2]

For a domain of modalities $(\mathscr{I}, L)$, the set of GHML formulas $\Phi_{\text{GHML}}(\mathscr{I}, L)$ is defined by:

$$\varphi := \top \quad | \quad \neg\varphi \quad | \quad \varphi_1 \wedge \varphi_2 \quad | \quad \langle\!\langle |E| \rangle\!\rangle \varphi \qquad \text{where } |E| \in |\mathscr{M}(\mathscr{I}, L)|.$$

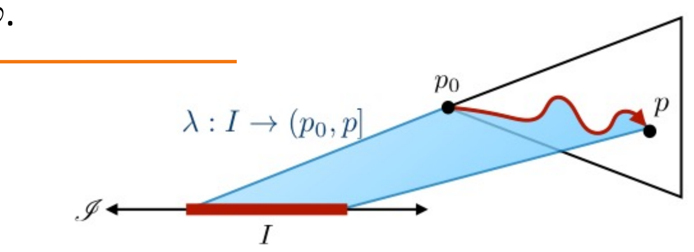
GHML: Semantics

Let $G = (P, \preceq_P, p_0, \mathcal{L})$ be a GST, and $\mathscr{G}_{\text{sub}} := \{G|_p : p \in P\}$ be the set of sub-trees of G.

Definition: [2]

The satisfaction relation $\models \subseteq \mathscr{G}_{\text{sub}} \times \Phi_{\text{GHML}}(\mathscr{I}, L)$ is defined such that

- $G \models \langle\!\langle |E| \rangle\!\rangle \varphi$ iff there exists a left-open $I \subseteq \mathscr{I}$ and an order-preserving bijection $\lambda : I \to (p_0, p]$ such that
  - $\mathcal{L} \circ \lambda \in |E|$ and $G|_p \models \varphi$.



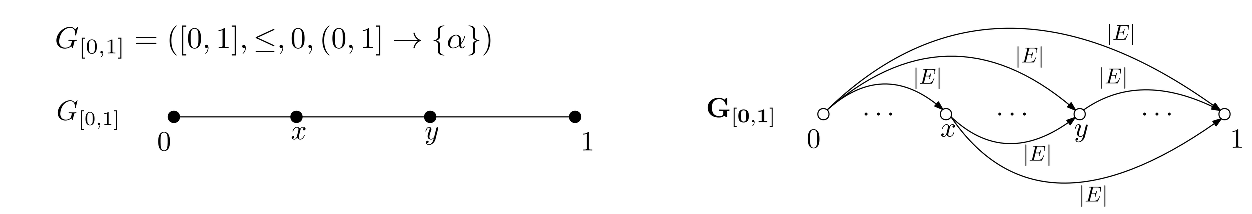
Surrogate Kripke Structures for GSTs

Simple idea: think of $\preceq_P$ as a transition relation and re-label it using $|\mathscr{M}(\mathscr{I}, L)|$.

Definition: [2]

The **surrogate Kripke structure of** G is $\mathbf{G} = (P, \{R^G_{|E|} : |E| \in |\mathscr{M}(\mathscr{I}, L)|\}, V)$ where:

- $p_1 \overset{|E|}{\to} p_2$ iff $p_1 \preceq_P p_2$ and $(p_1, p_2]$ is order equivalent to E; and
- V is the universal valuation.



Theorem: *(weak bisimulation and bisimulation between surrogates) [2]*

$$G_1 \leftrightarroweq_w G_2 \Leftrightarrow p_0 \leftrightarroweq q_0.$$

Theorem: *(GHML formulas in GSTs and HML formulas in STs) [2]*

1. for all $\varphi \in \Phi_{\text{GHML}}(\mathscr{I}, L)$, $\quad G_1 \models \varphi \implies p_0 \models \varphi_{\langle\,\rangle}$
2. for all $\phi \in \Phi_{\text{HML}}(L)$, $\quad p_0 \models \phi \implies G \models \phi_{\langle\!\langle\,\rangle\!\rangle}$

$\varphi_{\langle\,\rangle}$: replace GHML diamond modality with identically labeled HML modality.
$\phi_{\langle\!\langle\,\rangle\!\rangle}$: replace HML diamond modality with identically labeled GHML modality.

Maximal VHHM Classes of GSTs

Use surrogate Kripke structures to define VHHM classes of GSTs:

Definition: [2]

Say $\mathfrak{h}$ is a VHHM class of GSTs if for any two sub-GSTs from $\mathfrak{h}$:

$$G_1|_p \leftrightarroweq_w G_2|_q \quad \Leftrightarrow \quad G_1|_p \approx_{\text{GHML}} G_2|_q.$$

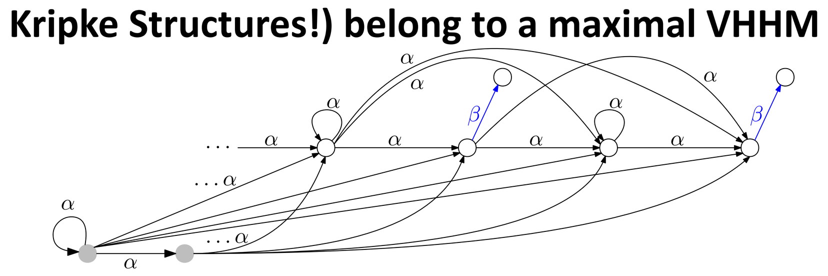
Theorem: *(Surrogate Kripke structures and VHHM classes of GSTs) [2]*

If $\mathfrak{h}$ is a VHHM class of GSTs, then the set of surrogate Kripke structures $\{\mathbf{G} : G \in \mathfrak{h}\}$ is a VHHM class of Kripke structures.

But there are certain additional constraints that can be enforced:

"Weak density": $\langle\!\langle E_1; E_2 \rangle\!\rangle \varphi \to \langle\!\langle E_1 \rangle\!\rangle \langle\!\langle E_2 \rangle\!\rangle \varphi$ "Transitivity": $\langle\!\langle E_1 \rangle\!\rangle \langle\!\langle E_2 \rangle\!\rangle \varphi \to \langle\!\langle E_1; E_2 \rangle\!\rangle \varphi$

Not all GSTs (or Kripke Structures!) belong to a maximal VHHM class! [2]



References

1. **J. Ferlez, R. Cleaveland, and S. I. Marcus. *Generalized synchronization trees*. In FOSSACS 2014, vol. 8412 of LNCS. Grenoble, France, 2014.**
2. **J. Ferlez, R. Cleaveland, and S. Marcus. *Bisimulation and Hennessy-Milner Logic for Generalized Synchronization Trees*. In Proceedings EXPRESS/SOS 2017; published in EPTCS, 255:35–50, 2017 and arXiv:1709.00049.**
3. Hennessy and Milner. Algebraic laws for nondeterminism and concurrency. Journal of the ACM. 1985
4. M. Hollenberg. Hennessy-Milner Classes and Process Algebra. In Modal Logic and Process Algebra: A Bisimulation Perspective, CSLI Lecture Notes, pages 187–216.
5. R. Milner. *A Calculus of Communicating Systems*. Number 92 in LNCS. 1980.