Introducing Hierarchical Hybrid Logic

Alexandre Madeira, Renato Neves, Luis Soares Barbosa

HASLab INESC TEC and Universidade do Minho, Portugal

Manuel A. Martins

CIDMA, Department of Mathematics, Universidade de Aveiro, Portugal

Abstract

This paper introduces $\mathcal{HHL}$, a hierarchical variant of hybrid logic. First-order correspondence and a Hennessy-Milner like theorem relating (hierarchical) bisimulation and logical equivalence for $\mathcal{HHL}$ are presented. Combining hierarchical transition structures with the ability to refer to specific states at any level of description, this logic seems suitable to express and verify properties of hierarchical transition systems, a pervasive semantic structure in Computer Science.

Keywords: Hierarchical transition systems, hybrid logic.

1 Introduction

From D. Harel’s statecharts [5] to the mobile ambients [4] of A. Gordon and L. Cardelli, models of hierarchical systems are pervasive in Computer Science. In practice, hierarchical, multi-level transitions often coexist within local ones — the ability to represent both and reason uniformly about them is essential to such models and even in more specific applications such as coordination protocols in the project of distributed systems [1]. Some forms of hierarchical models are also used to handle software which operates in different modes of execution and is able to commute between them. The global transition structure defines how such systems evolve from a mode (or configuration) to another [6].

This paper introduces a hierarchical variant of hybrid logic [2,3] which adds to the modal description of hierarchical transition structures the ability to

---

1 This work is funded by ERDF - European Regional Development Fund through the COMPETE Programme (Operational Programme for Competitiveness) and by National Funds through FCT, the Portuguese Foundation for Science and Technology, within projects FCOMP-01-0124-FEDER-028923, project PEst-OE/MAT/UI4106/2014; and by the project Cooperation and Perception for Augmented Autonomy - NORTE-07-0124-FEDER-000060 is co-financed by the North Portugal Regional Operational Programme (ON.2 – O Novo Norte), under the National Strategic Reference Framework (NSRF), through the European Regional Development Fund (ERDF).
refer to specific states at any level of description. As discussed in [6], hybrid logic, providing the ability to refer to specific states in a system, became the specification lingua franca for reconfigurable systems. The hierarchical variant proposed in the sequel sets the ground for a uniform framework to express and verify properties of any kind of hierarchical transition system.

2 Hierarchical hybrid logic \( \mathcal{HHL} \)

2.1 The meaning of hybrid in hybrid logic

The qualifier hybrid [2,3] applies to extensions of modal languages with symbols, called nominals, which explicitly refer to individual states in the underlying Kripke frame. A hybrid signature is a pair \((\text{Prop}, \text{Nom})\), where Prop and Nom are sets of symbols of propositional variables and nominals, respectively. The set of hybrid formulas over \((\text{Prop}, \text{Nom})\) extends the corresponding modal language with formulas \(i\), holding exactly at the state named by \(i\), and \(@i\rho\), asserting that formula \(\rho\) holds in the state named by \(i\), for \(i \in \text{Nom}\). Formally, this set, denoted by \(\text{Fm}^{\mathcal{HHL}}(\text{Prop, Nom})\), is defined by the grammar:

\[
\rho \equiv \rho \land \rho' | \rho \lor \rho' | \neg \rho | \rho' \Rightarrow \rho', \quad \text{for } i \in \text{Nom} \text{ and } p \in \text{Prop}.
\]

Models of \(\mathcal{H}\mathcal{L}\) for a signature \((\text{Nom, Prop})\), are Kripke structures with named states, i.e., structures \(M = (W, R, V)\) where \(W\) is a set of states, \(R \subseteq W \times W\) is the accessibility relation, and \(V: \text{Nom} \cup \text{Prop} \rightarrow \mathcal{P}(W)\) is a function interpreting propositions and nominals, such that for any \(i \in \text{Nom}\), \(V(i)\) is a singleton, its unique element being denoted by \(w^i\). The set of models over a signature \((\text{Nom, Prop})\) is denoted by \(\text{Mod}^{\mathcal{H}\mathcal{L}}(\text{Nom, Prop})\).

The satisfaction relation between a model \(M = (W, R, V)\) in \(\text{Mod}^{\mathcal{H}\mathcal{L}}(\text{Prop, Nom})\) and a formula \(\rho \in \text{Fm}^{\mathcal{H}\mathcal{L}}(\text{Prop, Nom})\) at a state \(w \in W\), is recursively defined as follows:

- if \(\rho\) is a \(\sigma \in \text{Nom} \cup \text{Prop}\) then, \(M, w \models^{\mathcal{H}\mathcal{L}} \sigma\) iff \(w \in V(\sigma)\); 
- if \(\rho\) is of form \(\lnot \varphi\) then, \(M, w \models^{\mathcal{H}\mathcal{L}} \lnot \varphi\) iff \(M, w \not\models^{\mathcal{H}\mathcal{L}} \varphi\); 
- if \(\rho\) is of form \(\varphi \land \varphi'\) then, \(M, w \models^{\mathcal{H}\mathcal{L}} \varphi \land \varphi'\) iff \(M, w \models^{\mathcal{H}\mathcal{L}} \varphi\) and \(M, w \models^{\mathcal{H}\mathcal{L}} \varphi'\); 
- if \(\rho\) is of form \(\lnot \varphi\) then, \(M, w \models^{\mathcal{H}\mathcal{L}} \lnot \varphi\) iff there is a \(v \in W\) such that \((w, v) \in R\) and \(M, v \models^{\mathcal{H}\mathcal{L}} \varphi\); 
- if \(\rho\) is of form \(\varphi \lor \varphi'\) then, \(M, w \models^{\mathcal{H}\mathcal{L}} \varphi \lor \varphi'\) iff \(M, w \models^{\mathcal{H}\mathcal{L}} \varphi\) or \(M, w \models^{\mathcal{H}\mathcal{L}} \varphi'\).

As usual, we write \(M \models^{\mathcal{H}\mathcal{L}} \rho\) when, for any \(w \in W\), \(M, w \models^{\mathcal{H}\mathcal{L}} \rho\), and \(M \models^{\mathcal{H}\mathcal{L}} \rho\) when \(M \models^{\mathcal{H}\mathcal{L}} \rho\) for any \(M \in \text{Mod}^{\mathcal{H}\mathcal{L}}(\text{Prop, Nom})\).

Applications often justify the introduction of a distinguished state in the underlying Kripke structure, regarded as the initial point of evaluation. As discussed in the sequel, such is the case of hierarchical transition systems representing software configurations: each configuration “starts” at a specific entry point, or initial state. Models for such pointed versions of \(\mathcal{H}\mathcal{L}\) are pairs \((M, s)\) with \(s \in W\). Accordingly, \((M, s) \models \rho\) iff \(M, s \models^{\mathcal{H}\mathcal{L}} \rho\).

2.2 Hierarchical hybrid logic

A signature \(\Delta\) for hierarchical hybrid logic, \(\mathcal{HHL}\)-signature for short, consists of a tuple \((\text{Prop, Nom, PROP, NOM})\) where Prop, Nom, PROP and NOM are
four disjoint sets of propositions and nominals corresponding to the two levels of discourse, called the ‘lower’ and the ‘upper’ level, respectively. The set of formulas for a signature $\Delta = \langle \text{Prop}, \text{Nom}, \text{PROP}, \text{NOM} \rangle$ is consequently organised in a two-level hierarchy: it consists of the smallest set $\text{Fn}^{\text{HL}}(\text{Prop}, \text{Nom}) \subseteq \text{Fn}(\Delta)$, $\text{PROP}, \text{NOM} \subseteq \text{Fn}(\Delta)$, $\land, \lor, \neg, \rightarrow$, $\rho \sqsubseteq \rho'$ $\in \text{Fn}(\Delta)$, for any $\rho \in \text{NOM}$ and $\rho, \rho' \in \text{Fn}(\Delta)$.

Finally, Kripke $\Delta$-model are tuples $M = (W, R, (M_w)_{w \in W}, V)$ where

- $W$ is a non empty set of (upper) states;
- $R \subseteq W \times W$ is a binary relation, the upper accessibility relation;
- $V : \text{PROP} \cup \text{NOM} \to \mathcal{P}(W)$ is a function where, for any $\xi \in \text{NOM}$, $V(\xi)$ is a singleton. As usual we denote the element $V(\xi)$ by $w^\xi$;
- for any $w \in W$, $M_w$ is a $\mathcal{H}\mathcal{L}$-pointed model $M_w = (H_w, s_w)$, where $H_w = (W_w, R_w, V_w)$ is a hybrid ($\text{Prop}, \text{Nom}$)-model and $s_w \in W_w$.

**Definition 2.1 ($\mathcal{H}\mathcal{L}$-Satisfaction)** Let $\Delta = \langle \text{Prop}, \text{Nom}, \text{PROP}, \text{NOM} \rangle$ be a $\mathcal{H}\mathcal{L}$-signature and $M = (W, R, V, (M_w)_{w \in W})$ a $\Delta$-model. The satisfaction relation between formulas, models and points is defined recursively as follows:

1. $M, w \models \rho$ iff $H_w, s_w \models^\mathcal{H}\mathcal{L} \rho$, for $\rho \in \text{Fn}^{\mathcal{H}\mathcal{L}}(\text{Prop}, \text{Nom})$.
2. $M, w \models \exists \rho$ iff $w \in V(\exists \rho)$, for $\rho \in \text{PROP}$;
3. $M, w \models \xi$ iff $V(\xi) = \{ w \}$, for $\xi \in \text{NOM}$;
4. $M, w \models \neg \rho$ iff $M, w \not\models \rho$;
5. $M, w \models \rho \land \rho'$ iff there is a $w' \in W$ such that $(w, w') \in R$ and $M, w' \models \rho$;
6. $M, w \models \rho \lor \rho'$ iff $M, w \models \rho$ or $M, w \models \rho'$.

Notice that the semantic interpretation of the Boolean connectives at both levels, e.g., $\land, \lor$ and $\vee, \wedge$, coincide. As in the standard case we write $M \models \rho$ when, for any $w \in W$, $M, w \models \rho$, and $\models \rho$ when $M \models \rho$ for all the models $M \in \text{Mod}(\text{Prop}, \text{Nom})$.

### 3 First-order correspondence

The semantics of $\mathcal{H}\mathcal{L}$ induces a first-order correspondence along the lines of the usual standard translation of modal logic. In the sequel consider a $\mathcal{H}\mathcal{L}$-signature $\Delta = \langle \text{Prop}, \text{Nom}, \text{PROP}, \text{NOM} \rangle$. The following two definitions establish the corresponding first-order signature and translation of models.

The two-sorted first-order signature $\Delta^* = (S, F, P)$ corresponding to $\Delta$ is given by, $S = \{ W, U \}$, $F = \{ i : W \to U \mid i \in \text{Nom} \} \cup \{ \xi : W \mid \xi \in \text{NOM} \} \cup \{ \text{Init} : W \to U \}$ and $P = \{ R : W \times W, r : W \times U \times U \} \cup \{ p : W \times U \mid p \in \text{Prop} \} \cup \{ \exists \rho \}$.

The translation from $\Delta$ to $\Delta^*$ is specified by $\models^* : \text{Mod}(\Delta) \to \text{Mod}(\Delta^*)$ as follows: Given a model $M = (W, R, (M_w)_{w \in W}, V)$ in $\text{Mod}(\Delta)$, then $M^*_W = W$ and $M^*_W = \bigcup_{w \in W} W_w$; similarly, $M^*_i(w) = V_w(i)$, for $i \in \text{Nom}$, $M^*_\xi(w) = V(\xi)$, for $\xi \in \text{NOM}$, and $M^*_\text{Init}(w) = s_w$; finally, for predicates, $M^*_p(w, w') \iff (w, w') \in R$, $M^*_p(w, u, v) \iff (u, v) \in R_w$, $M^*_p(w, u) \iff u \in V_w(p)$, for $p \in \text{Prop}$, and $M^*_p(w)$ iff $w \in V(p)$, for $p \in \text{PROP}$.
Hence, for \( p \in \text{Prop}, i \in \text{Nom}, \# \in \text{NOM}, \mathfrak{p} \in \text{PROP} \) and \( \rho \in \text{Fm}^{\mathcal{H}\mathcal{L}}(\text{Prop}, \text{Nom}) \), we define

\[
\begin{align*}
\text{ST}^X_{X,u}(p) & = p(X,u) \\
\text{ST}^X_{X,u}(i) & = u = i(X) \\
\text{ST}^X_{X,u}(\oplus_i \rho) & = \text{ST}^X_{X,i(X)}(\rho) \\
\text{ST}^X_{X,u}(\ominus \rho) & = (\exists v : U)(r(X,u,v) \land \text{ST}^X_{X,v}(\rho)) \\
\text{ST}^X_{X,u}(\mathfrak{p}) & = \mathfrak{p}(X) \\
\text{ST}^X_{X,u}(\#) & = X = \# \\
\text{ST}^X_{X,u}(\oplus \rho) & = \text{ST}^X_{X,u}(\rho)[\# / X, \text{Init}(\#)/u] \\
\text{ST}^X_{X,u}(\ominus \rho) & = (\exists Y : W)R(X,Y) \land \text{ST}^X_{Y,\text{Init}(Y)}(\rho) \\
\text{ST}^X_{X,u}(\neg \rho) & = \neg \text{ST}^X_{X,u}(\rho) \\
\text{ST}^X_{X,u}(\rho \lor \rho') & = \text{ST}^X_{X,u}(\rho) \lor \text{ST}^X_{X,u}(\rho')
\end{align*}
\]

The characterisation of other translations can be found in [7]. As expected,

**Theorem 3.1 ([7])** Let \( \Delta = (\text{Prop}, \text{Nom}, \text{PROP}, \text{NOM}) \) be a \( \mathcal{H}\mathcal{L} \)-signature, \( M \) a \( \Delta \)-model and \( \rho \in \text{Fm}(\text{Prop}, \text{Nom}, \text{PROP}, \text{NOM}) \).

Then, \( M, w \models \rho \) iff \( M' \models_{\text{FOL}} \text{ST}^X_{X,u}(\rho)[w/X, M'_{\text{Init}}(w)/u] \)

### 4 A Hennessy-Milner theorem for \( \mathcal{H}\mathcal{L} \)

We define in the sequel a notion of bisimulation for \( \mathcal{H}\mathcal{L} \). Basically it entails the zig-zag condition and correspondence of nominals at both models’ lower and upper levels, as illustrated graphically in Fig. 4. Formally, An **hierarchical bisimulation** between two \((\text{Prop}, \text{Nom}, \text{PROP}, \text{NOM})\)-models \( M = (W,R,(M_w)_{w \in W},V) \) and \( M' = (W',R',(M'_w)_{w \in W'},V') \) consists of a relation \( \mathfrak{B} \subseteq W \times W' \) such that, for any \( w \in W, w' \in W' \), if \( (w,w') \in \mathfrak{B} \) then

- **(NOM)** for any \( \# \in \text{NOM}, (w^\#, w'^\#) \in \mathfrak{B} \)
- **(ATOM)** for any \( a \in \text{PROP} \cup \text{NOM}, w \in V(a) \) iff \( w' \in V'(a) \)
- **(LOC)** \( M_w \) and \( M'_w \) are bisimilar, i.e., there is a relation \( B_w \subseteq W_w \times W_{w'} \) such that
  - **(ini)** \((s_w, s_{w'}) \in B_{w'}\),
  - **(atom)** for any \( p \in \text{Prop} \cup \text{Nom} \), \( w \in V(p) \) iff \( w' \in V'(p) \),
  - **(nom)** for any \( i \in \text{Nom} \), \((w^i, w'^i) \in B_w\),
  - **(zag)** if \( (s,t) \in B_w, (s',t') \in R_w, \) then there is a \( t' \in W' \) such that \( (t,t') \in R'_{w'} \) and \((s',t') \in B_{w'}\).

### Theorem 4.1 ([7])

Let \( M \) and \( M' \) be two \( \mathcal{H}\mathcal{L} \)-models over the same signature \( \Delta \) related by a hierarchical bisimulation \( \mathfrak{B} \). Then, for any \( w \mathfrak{B} w' \) and
formula $\rho$, $M, w \models \rho$ iff $M', w' \models \rho$

**Theorem 4.2** ([7]) Let $\Delta$ be a $\mathcal{HHL}$-signature and $M$ and $M'$ two image-finite $\Delta$-models. Then, for every $w \in W$ and $w' \in W'$, the following conditions are equivalent:

(i) $M, w \models \rho$ iff $M', w' \models \rho$, for any formula $\rho \in \text{Fm}(\Delta)$

(ii) There is a hierarchical bisimulation $B \subseteq W \times W'$ such that $(w, w') \in B$.

5 Concluding

In summary, $\mathcal{HHL}$ is a basic logic to specify and reason about hierarchical transition systems, but just an initial step in a broader landscape. More results about translation and the decidability for this logic are reported in [7]. Moreover, several extensions are possible and, in fact currently under investigation. In particular, examples coming from Computer Science may entail the need for more complex features. For example, statecharts, already mentioned in the introduction, comprise different forms of inter-level transitions, including multiple-source and multiple-target ones as well as simultaneous firing of non-conflicting transitions and their prioritisation.

References


