Introducing Hierarchical Hybrid Logic

Alexandre Madeira, Renato Neves, Luis Soares Barbosa [1]

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

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 ρ holds in the state named by i, for $i \in \text{Nom}$. Formally, this set, denoted by $\text{Fm}^{\mathcal{HL}}(\text{Prop}, \text{Nom})$, is defined by the grammar $\rho \ni p \mid i \mid @_i\rho \mid \diamondsuit \rho \mid \neg\rho \mid \rho \vee \rho$, for $i \in \text{Nom}$ and $p \in \text{Prop}$.

Models of $\mathcal{HL}$ for a signature $(\text{Nom}, \text{Prop})$, 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 $V : \text{Nom} \cup \text{Prop} \to \mathcal{P}(W)$ 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 $(\text{Nom}, \text{Prop})$ is denoted by $\text{Mod}^{\mathcal{HL}}(\text{Nom}, \text{Prop})$.

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

- if ρ is a $\sigma \in \text{Nom} \cup \text{Prop}$ then, $M, w \vDash^{\mathcal{HL}} \sigma$ iff $w \in V(\sigma)$;
- if ρ is of form $@_i\varphi$ then, $M, w \vDash^{\mathcal{HL}} @_i\varphi$ iff $M, w^i \vDash^{\mathcal{HL}} \varphi$;
- if ρ is of form $\diamondsuit\varphi$ then, $M, w \vDash^{\mathcal{HL}} \diamondsuit\varphi$ iff there is a $v \in W$ such that $(w, v) \in R$ and $M, v \vDash^{\mathcal{HL}} \varphi$;
- if ρ is of form $\neg\varphi$ then, $M, w \vDash^{\mathcal{HL}} \neg\varphi$ iff is false that $M, w \vDash^{\mathcal{HL}} \varphi$;
- if ρ is of form $\varphi \vee \varphi'$ then, $M, w \vDash^{\mathcal{HL}} \varphi \vee \varphi'$ iff $M, w \vDash^{\mathcal{HL}} \varphi$ or $M, w \vDash^{\mathcal{HL}} \varphi'$.

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

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 $\mathcal{HL}$ are pairs (M, s) with $s \in W$. Accordingly, $(M, s) \vDash \rho$ iff $M, s \vDash^{\mathcal{HL}} \rho$.

2.2   Hierarchical hybrid logic

A signature Δ for *hierarchical hybrid logic*, $\mathcal{HHL}$-signature for short, consists of a tuple $(\text{Prop}, \text{Nom}, \text{PROP}, \text{NOM})$ 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 $\Delta = (\mathrm{Prop}, \mathrm{Nom}, \mathrm{PROP}, \mathrm{NOM})$ is consequently organised in a two-level hierarchy: it consists of the smallest set $\mathrm{Fm}(\Delta)$, such that $\mathrm{Fm}^{\mathcal{HL}}(\mathrm{Prop}, \mathrm{Nom}) \subseteq \mathrm{Fm}(\Delta)$, $\mathrm{PROP}, \mathrm{NOM} \subseteq \mathrm{Fm}(\Delta)$, $@_{\mathtt{i}}\rho$, $\diamondsuit\rho$, $\neg\rho$, $\rho \vee\!\!\!\vee \rho' \in \mathrm{Fm}(\Delta)$, for any $\mathtt{i} \in \mathrm{NOM}$ and $\rho, \rho' \in \mathrm{Fm}(\Delta)$.

Finally, Kripke Δ-*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;
- $V : \mathrm{PROP} \cup \mathrm{NOM} \to \mathcal{P}(W)$ is a function where, for any $\mathtt{i} \in \mathrm{NOM}$, $V(\mathtt{i})$ is a singleton. As usual we denote the element $V(\mathtt{i})$ by $w^{\mathtt{i}}$.
- for any $w \in W$, M_w is a $\mathcal{HL}$-pointed model $M_w = (H_w, s_w)$, where $H_w = (W_w, R_w, V_w)$ is a hybrid $(\mathrm{Prop}, \mathrm{Nom})$-model and $s_w \in W_w$.

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

(i) $M, w \vDash \rho$ *iff* $H_w, s_w \vDash^{\mathcal{HL}} \rho$*, for* $\rho \in \mathrm{Fm}^{\mathcal{HL}}(\mathrm{Prop}, \mathrm{Nom})$.

(ii) $M, w \vDash \mathtt{p}$ *iff* $w \in V(\mathtt{p})$*, for* $\mathtt{p} \in \mathrm{PROP}$*;*

(iii) $M, w \vDash \mathtt{i}$ *iff* $V(\mathtt{i}) = \{w\}$*, for* $\mathtt{i} \in \mathrm{NOM}$*;*

(iv) $M, w \vDash @_{\mathtt{i}}\rho$ *iff* $M, w^{\mathtt{i}} \vDash \rho$*;*

(v) $M, w \vDash \diamondsuit\rho$ *iff there is a* $w' \in W$ *such that* $(w, w') \in R$ *and* $M, w' \vDash \rho$*;*

(vi) $M, w \vDash \neg\rho$ *iff is false that* $M, w \vDash \rho$*;*

(vii) $M, w \vDash \rho \vee\!\!\!\vee \rho'$ *iff* $M, w \vDash \rho$ *or* $M, w \vDash \rho'$

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

3 First-order correspondence

The semantics of $\mathcal{HHL}$ induces a first-order correspondence along the lines of the usual standard translation of modal logic. In the sequel consider a $\mathcal{HHL}$-signature $\Delta = (\mathrm{Prop}, \mathrm{Nom}, \mathrm{PROP}, \mathrm{NOM})$. 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 Δ is given by, $S = \{W, U\}$, $F = \{i : W \to U \mid i \in \mathrm{Nom}\} \cup \{\mathtt{i} :\to W \mid \mathtt{i} \in \mathrm{NOM}\} \cup \{Init : W \to U\}$ and $P = \{R : W \times W, r : W \times U \times U\} \cup \{p : W \times U \mid p \in \mathrm{Prop}\} \cup \{\mathtt{p} : W \mid \mathtt{p} \in \mathrm{PROP}\}$.

The translation from Δ to Δ^* is specified by $\_^* : \mathrm{Mod}(\Delta) \to \mathrm{Mod}(\Delta^*)$ as follows: Given a model $M = (W, R, (M_w)_{w \in W}, V)$ in $\mathrm{Mod}(\Delta)$, then $M_W^* = W$ and $M_U^* = \bigcup_{w \in W} W_w$; similarly, $M_i^*(w) = V_w(i)$, for $i \in \mathrm{Nom}$, $M_{\mathtt{i}}^* = V(\mathtt{i})$, for $\mathtt{i} \in \mathrm{NOM}$, and $M_{Init}^*(w) = s_w$; finally, for predicates, $M_R^*(w, w')$ iff $(w, w') \in R$, $M_r^*(w, u, v)$ iff $(u, v) \in R_w$, $M_p^*(w, u)$ iff $u \in V_w(p)$, for $p \in \mathrm{Prop}$, and $M_{\mathtt{p}}^*(w)$ iff $w \in V(\mathtt{p})$, for $\mathtt{p} \in \mathrm{PROP}$.

Hence, for $p \in \mathrm{Prop}$, $i \in \mathrm{Nom}$, $\mathtt{i} \in \mathrm{NOM}$, $\mathtt{p} \in \mathrm{PROP}$ and $\rho \in \mathrm{Fm}^{\mathcal{HL}}(\mathrm{Prop}, \mathrm{Nom})$, we define

$$
\begin{aligned}
\mathrm{ST}_{X,u}(p) &= p(X,u) \\
\mathrm{ST}_{X,u}(i) &= u = i(X) \\
\mathrm{ST}_{X,u}(@_i\rho) &= \mathrm{ST}_{X,i(X)}(\rho) \\
\mathrm{ST}_{X,u}(\Diamond\rho) &= (\exists v : U)(r(X,u,v) \wedge \mathrm{ST}_{X,v}(\rho)) \\
\mathrm{ST}_{X,u}(\mathtt{p}) &= \mathtt{p}(X) \\
\mathrm{ST}_{X,u}(\mathtt{i}) &= X = \mathtt{i} \\
\mathrm{ST}_{X,u}(@_{\mathtt{i}}\rho) &= \mathrm{ST}_{X,u}(\rho)[\mathtt{i}/X, Init(\mathtt{i})/u] \\
\mathrm{ST}_{X,u}(\lozenge\rho) &= (\exists Y : W)R(X,Y) \wedge \mathrm{ST}_{Y,Init(Y)}(\rho)) \\
\mathrm{ST}_{X,u}(\neg\rho) &= \neg\mathrm{ST}_{X,u}(\rho) \\
\mathrm{ST}_{X,u}(\rho \vee \rho') &= \mathrm{ST}_{X,u}(\rho) \vee \mathrm{ST}_{X,u}(\rho')
\end{aligned}
$$

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

Theorem 3.1 ([7]) *Let* $\Delta = (\mathrm{Prop}, \mathrm{Nom}, \mathrm{PROP}, \mathrm{NOM})$ *be a* $\mathcal{HHL}$*-signature,* M *a* Δ*-model and* $\rho \in \mathrm{Fm}(\mathrm{Prop}, \mathrm{Nom}, \mathrm{PROP}, \mathrm{NOM})$.
Then, $M, w \vDash \rho$ *iff* $M^* \vDash^{FOL} \mathrm{ST}_{X,u}(\rho)[w/X, M^*_{Init}(w)/u]$

4   A Hennessy-Milner theorem for $\mathcal{HHL}$

We define in the sequel a notion of bisimulation for $\mathcal{HHL}$. 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 $(\mathrm{Prop}, \mathrm{Nom}, \mathrm{PROP}, \mathrm{NOM})$-models $M = (W, R, (M_w)_{w \in W}, V)$ and $M' = (W', R', (M'_w)_{w \in W'}, V')$ consists of a relation $\mathbb{B} \subseteq W \times W'$ such that, for any $w \in W, w' \in W'$, if $(w, w') \in \mathbb{B}$ then

- **(NOM)** for any $\mathtt{i} \in \mathrm{NOM}$, $(w^{\mathtt{i}}, w'^{\mathtt{i}}) \in \mathbb{B}$
- **(ATOM)** for any $\mathtt{a} \in \mathrm{PROP} \cup \mathrm{NOM}$, $w \in V(\mathtt{a})$ iff $w' \in V'(\mathtt{a})$
- **(LOC)** M_w and $M'_{w'}$ are bisimilar, *i.e.*, there is a relation $\mathrm{B}^{w}_{w'} \subseteq W_w \times W_{w'}$ such that
  - **(ini)** $(s_w, s_{w'}) \in \mathrm{B}^{w}_{w'}$;
  - **(atom)** for any $p \in \mathrm{Prop} \cup \mathrm{Nom}$, $w \in V_w(p)$ iff $w' \in V'_{w'}(p)$
  - **(nom)** for any $i \in \mathrm{Nom}$, $(w^i, w'^i) \in \mathrm{B}^{w}_{w'}$
  - **(zig)** if $(s, t) \in \mathrm{B}^{w}_{w'}$ and $(s, s') \in R_w$ then there is a $t' \in W'_{w'}$ such that $(t, t') \in R'_{w'}$ and $(s', t') \in \mathrm{B}^{w}_{w'}$
  - **(zag)** if $(s, t) \in \mathrm{B}^{w}_{w'}$ and $(t, t') \in R'_{w'}$ there is a $s' \in W_w$ such that $(s', t') \in \mathrm{B}^{w}_{w'}$ and $(s, s') \in R_w$
- **(ZIG)** if $(w, v) \in R$ then there is a $v' \in W'$ such that $v \mathbb{B} v'$ and $(w', v') \in R'$
- **(ZAG)** if $(w', v') \in R'$ then there is a $v \in W$ such that $v \mathbb{B} v'$ and $(w, v) \in R$

Clearly, the union and composition of hierarchical bisimulations still are hierarchical bisimulations. We focus below, however, in two basic results linking this notion to logical equivalence in $\mathcal{HHL}$: an invariance result and a Hennessy-Milner like theorem for this logic.

Theorem 4.1 ([7]) *Let* M *and* M' *be two* $\mathcal{HHL}$*-models over the same signature* Δ *related by a hierarchical bisimulation* $\mathbb{B}$. *Then, for any* $w \mathbb{B} w'$ *and*
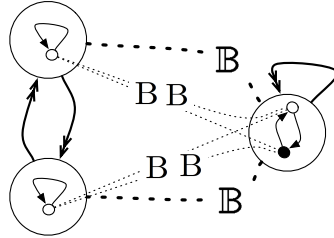
Fig. 1. A$\mathcal{HHL}$-bisimulation

formula ρ, $M, w \vDash \rho$ iff $M', w' \vDash \rho$

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

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

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

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

[1] Richard Banach, Farhad Arbab, George A. Papadopoulos, and John R. W. Glauert. A multiply hierarchical automaton semantics for the iwim coordination model. *J. UCS*, 9(1):2–33, 2003.

[2] Patrick Blackburn. Representation, reasoning, and relational structures: a hybrid logic manifesto. *Logic Journal of IGPL*, 8(3):339–365, 2000.

[3] Torben Braüner. *Hybrid Logic and its Proof-Theory*. Applied Logic Series. Springer, 2010.

[4] Luca Cardelli and Andrew D. Gordon. Mobile ambients. In FoSSaCS'98, volume 1378 of *LNCS*, pages 140–155. Springer, 1998.

[5] David Harel. Statecharts: A visual formalism for complex systems. *Sci. Comput. Program.*, 8(3):231–274, 1987.

[6] Alexandre Madeira, José M. Faria, Manuel A. Martins, and Luís Soares Barbosa. Hybrid specification of reactive systems: An institutional approach. In SEFM 2011, volume 7041 of *LNCS*, pages 269–285. Springer, 2011.

[7] Alexandre Madeira, Renato Neves, Luis Barbosa, and Manuel Martins. Hierarquical hybrid logic. (submitted to a journal).