Formalizing a Seligman-Style Tableau System for Hybrid Logic
(Short Paper)

Asta Halkjær From[1(✉)], Patrick Blackburn[2], and Jørgen Villadsen[1]

[1] Technical University of Denmark, Kongens Lyngby, Denmark
ahfrom@dtu.dk
[2] Roskilde University, Roskilde, Denmark

Abstract. Hybrid logic is modal logic enriched with names for worlds. We formalize soundness and completeness proofs for a Seligman-style tableau system for hybrid logic in the proof assistant Isabelle/HOL. The formalization shows how to lift certain rule restrictions, thereby simplifying the original un-formalized proof. Moreover, the completeness proof we formalize is synthetic which suggests we can extend this work to prove a wider range of results about hybrid logic.

Keywords: Isabelle/HOL · Hybrid logic · Soundness · Completeness

1 Introduction

Hybrid logic extends ordinary modal logic with nominals, a special sort of propositional symbol true at exactly one world. Nominals, and the satisfaction operators they give rise to, make hybrid logic well-suited for different applications ranging from temporal logic [4] to epistemic logics for social networks [22]. The description logics underlying the Web Ontology Language and applications in biomedical informatics [16] can also be seen as forms of hybrid logic [2].

ST is a sound and complete tableau system for hybrid logic. It is known to terminate when five restrictions are imposed on the rules, and one key rule is split into three cases [5]. Two completeness proofs exist for ST, a synthetic one that does not cover the rule restrictions [17] and a complex translation-based proof that does [5]. In this paper we modify ST and three of its restrictions slightly, and use the proof assistant Isabelle/HOL to show that we can lift these restrictions by (a) formally proving the admissibility of their unrestricted versions, and (b) formalizing a synthetic completeness proof for the modified calculus.

Isabelle is a generic proof assistant and Isabelle/HOL is its instance based on higher-order logic [20]. Proof assistants like Isabelle provide tools to express mathematical statements and proofs in a formal language that can be mechanically verified; all proofs presented here have been checked in this manner. The full formalization, 4396 lines, is available in the Archive of Formal Proofs which keeps refereed submissions up to date with the current Isabelle version [13]. The formalization was developed for the first author's MSc thesis [15]. We chose Isabelle/HOL because it is the proof assistant we know best.

N. Peltier and V. Sofronie-Stokkermans (Eds.): IJCAR 2020, LNAI 12166, pp. 474–481, 2020.
https://doi.org/10.1007/978-3-030-51074-9_27

2 Syntax and Semantics

The well-formed formulas of basic hybrid logic are defined as follow. We use the letter x for propositional symbols and i, a and b for nominals.

$$\phi, \psi ::= x \mid i \mid \neg\phi \mid \phi \vee \psi \mid \Diamond\phi \mid @_i\phi$$

The language is interpreted on Kripke models $\mathfrak{M}$, consisting of a frame (W, R) and a valuation of propositional symbols V. Here W is a non-empty set of worlds and R is a binary accessibility relation between them. To interpret the nominals we use an assignment g mapping nominals to elements of W; if $g(i) = w$ then we say that nominal i denotes w. Formula satisfiability is defined as follows:

$$\begin{array}{lll}
\mathfrak{M}, g, w \models x & \text{iff} & w \in V(x) \\
\mathfrak{M}, g, w \models i & \text{iff} & g(i) = w \\
\mathfrak{M}, g, w \models \neg\phi & \text{iff} & \mathfrak{M}, g, w \not\models \phi \\
\mathfrak{M}, g, w \models \phi \vee \psi & \text{iff} & \mathfrak{M}, g, w \models \phi \text{ or } \mathfrak{M}, g, w \models \psi \\
\mathfrak{M}, g, w \models \Diamond\phi & \text{iff} & \text{for some } w',\ wRw' \text{ and } \mathfrak{M}, g, w' \models \phi \\
\mathfrak{M}, g, w \models @_i\phi & \text{iff} & \mathfrak{M}, g, g(i) \models \phi
\end{array}$$

An expression of the form $@_i\phi$ is called a satisfaction statement, and such statements are true iff ϕ is true at the world denoted by nominal i. Note two important special cases: $@_i a$ says that the nominals i and a denote the same world, and $@_i\Diamond b$ says that the world denoted by i has access to the world denoted by b.

3 A Seligman-Style Tableau System

Many proof systems for hybrid logic exist; see Blackburn et al. [5] for discussion. These typically work by manipulating only formulas prefixed by satisfaction operators, which gives a global flavour to proofs, however the tableau system we formalize here manipulates *arbitrary* formulas. It is an adaptation of system ST, due to Blackburn et al. [5], which was inspired by Jeremy Seligman's local natural deduction and sequent calculus systems for hybrid logic [23,24].

The tableau rules are based on a subdivision of tableau branches into blocks. Each pair of blocks is separated by a horizontal line and the first formula on each block is a nominal dubbed the opening nominal. The intuition is that the formulas on a block are true in the world denoted by its opening nominal. We assume that the initial block, like the rest, is always named (this is our first modification of the original ST system). This assumption simplifies the formalization, as we can now model all blocks as lists of formulas paired with an opening nominal, and a branch as a list of blocks. If Θ is a branch and ϕ occurs on an i-block in Θ then we say that ϕ occurs at i in Θ. We occasionally refer to the opening nominal of a block as its name or type.

The rules are given in Fig. 1: the first three are propositional, the three below are for working with the blocks, and the four to the right apply to the hybrid logic connectives. The input to the rule is given above the vertical line and the

output below it. Above every input formula, we write the opening nominal of the block it occurs on. Similarly, the opening nominal of the output block is the first thing below the line. If the opening nominals match, then the output block may be the same as an input block. In the formalization we model the rules as an inductively defined set of branches that have closing extensions.

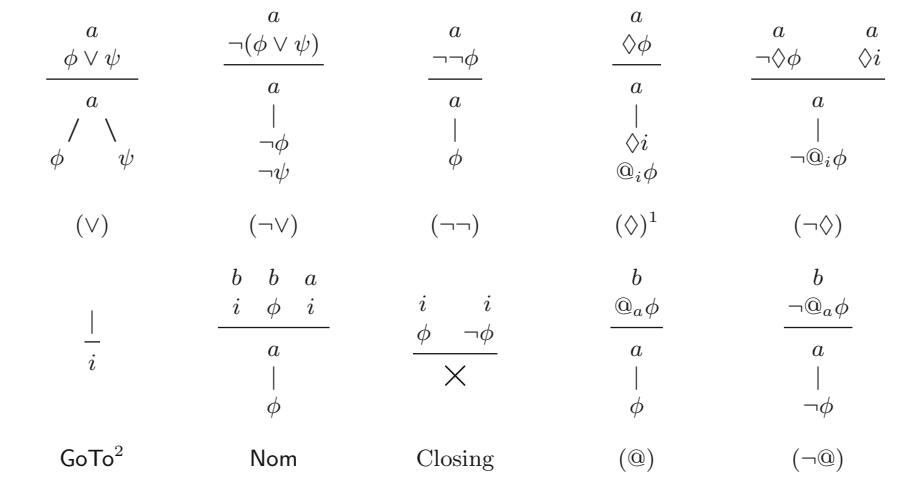

Fig. 1. Tableau rules.

Consider the $(\neg\neg)$ rule: if $\neg\neg\phi$ occurs on an a-block and the current block is an a-block, then ϕ is a legal extension of the branch. For the Nom rule, nominal i occurs at both a and b, so they must denote the same world and copying ϕ from a b-block to the current a-block is legal. Here we also differ from the original ST: we do not require the shared nominal i to occur on the current block as this would be a problem for our Strengthening Lemma in Sect. 4. The GoTo rule allows us to change perspective from one world to another by starting a new block with an opening nominal that already occurs somewhere on the branch.

A branch closes if the same formula occurs on the same type of block both positively and negatively, and a tableau closes if all its branches do. If a closed tableau can be obtained starting from the branch Θ, then we write $\vdash \Theta$. If Θ is a branch and the current block has opening nominal a, then we write the extension of Θ by ϕ as $\phi -_a \Theta$ to resemble the extensions in Fig. 1.

The original ST has five restrictions, called R1-R5 [5]. Restriction R3 is unnecessary in our system since it applies to an omitted rule that names the

initial block. Restriction R4 forbids applying GoTo twice in a row and formalizing it is left for future work. Here are our adaptations of the three remaining restrictions:

R1 The output of a rule must include a formula new to the current block type.
R2 The ($\Diamond$) rule can only be applied to input $\Diamond\phi$ on an a-block if it is not already witnessed on a.
R5 (@) and ($\neg$@) can only be applied to premises i and $@_i\phi$ ($\neg@_i\phi$) when the current block is an i-block.

The formula ϕ is new to a in Θ if ϕ does not occur at a in Θ. A formula $\Diamond\phi$ is witnessed at a in Θ if for some witnessing nominal i, both $\Diamond i$ and $@_i\phi$ occur at a in Θ. The original R2 restriction states that the ($\Diamond$) rule cannot be applied twice to the same formula occurrence, but formalizing this would require keeping track of previous rule applications. We already keep track of the branch so we prefer the R2 presented here. Our version of the @-rules already satisfy the R5 restriction.

4 Main Results

Theorem 1 (Soundness). *If $\vdash \Theta$ where Θ consists of just $\neg\phi$ on an i-block and i does not occur in ϕ, then ϕ is valid.*

Proof. Similar to the original soundness proof by Blackburn et al. [5]. □

The following lemma allows us to derive rules unrestricted by R1:

Lemma 1 (Strengthening). *If an extension is not new then it is redundant. That is, if $\vdash \phi -_a \Theta$ and ϕ occurs at a in Θ then $\vdash \Theta$.*

Proof. The existing ϕ can be used as rule input in place of the extension. □

To lift R2 we use the following substitution lemma where $\phi\sigma$ and $\Theta\sigma$ are obtained from ϕ and Θ, respectively, by replacing every nominal i with $\sigma(i)$.

Lemma 2 (Substitution). *Let σ be a substitution function whose domain and codomain coincide. If $\vdash \Theta$ then $\vdash \Theta\sigma$.*

Proof. By induction on the derivation of $\vdash \Theta$ for arbitrary σ. In the ($\Diamond$) case we assume that $\Diamond\phi$ occurs at a in Θ and need to derive $\vdash \Theta\sigma$ from $\vdash (@_i\phi -_a \Diamond i -_a \Theta)\sigma'$ where i is some nominal fresh to Θ and we get to pick σ'.

By assumption, $\Diamond\phi$ is unwitnessed at a in Θ but since the substitution can collapse formulas, $\Diamond(\phi\sigma)$ may be witnessed in $\Theta\sigma$ by some witnessing nominal j. In this case, where restriction R2 prevents us from applying the ($\Diamond$) rule, we let $\sigma' = \sigma(i := j)$ in the induction hypothesis. Since i occurs only in the extension the rest of the branch is unaffected by this choice, $\Theta(\sigma(i := j)) = \Theta\sigma$, but now the extension occurs elsewhere at a and the Nom rule justifies it. □

Lemma 3 (Unrestricted ($\Diamond$)). *If $\Diamond\phi$ occurs at a in Θ, i is fresh and ϕ is not a nominal then we can derive $\vdash \Theta$ from a witnessing extension $\vdash @_i\phi -_a \Diamond i -_a \Theta$.*

Proof. If $\Diamond\phi$ is already witnessed at a in Θ then use Lemma 2 to make i coincide with the existing witnessing nominal and justify the extension by Nom. □

If Θ consists of blocks $B_1, B_2, \ldots, B_n$, let $\text{Blocks}(\Theta) = \{B_1, B_2, \ldots, B_n\}$. The substitution lemma allows us to prove the following:

Lemma 4 (Branch structure). *Given infinitely many nominals, we can add, contract and rearrange blocks: If $\vdash \Theta$ and $\text{Blocks}(\Theta) \subseteq \text{Blocks}(\Theta')$ then $\vdash \Theta'$.*

Proof. By induction on the derivation of $\vdash \Theta$ for arbitrary Θ'. □

Lemma 5 (Unrestricted (@) (and ($\neg$@))). *If $\vdash \phi -_a \Theta$, $@_i\phi$ occurs at b in Θ and i occurs at a then $\vdash \Theta$.*

Proof. Figure 2 shows the derivation where each new branch to the right is known by Lemma 4 to still have a closing extension. □

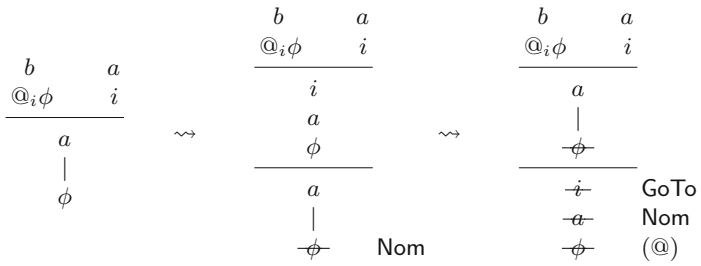

Fig. 2. Deriving the unrestricted (@) rule.

Theorem 2 (Completeness). *If ϕ is valid then $\vdash \Theta$ where Θ consists of a single block with ϕ on it.*

Proof. Essentially a modification of the proof for ST by Jørgensen et al. [17], since our system is similar, and we have proved we can lift our restrictions. □

We remark that the completeness proof is an example of what are known as synthetic approaches to completeness [11,25], which involve reasoning about maximal consistent sets and their properties. However the completeness proof for ST distinguishes itself by using maximal sets of entire blocks rather than plain formulas. One component of the proof is a definition of when such a set of blocks is a Hintikka set and thus satisfiable [17]. In the formalization [13] we precisely formulate this definition in the formal language of Isabelle/HOL and in doing so we discovered a shortcoming in the definition given by Jørgensen et al. Essentially, their requirement on propositional symbols fails to take so-called equivalence of nominals into account, making their model valuation incompatible with their model existence result.

5 Related Work

Linker formalizes in Isabelle/HOL a semantic embedding of a spatio-temporal multi-modal logic designed for reasoning about motorway traffic which includes a hybrid logic-inspired at-operator [18]. Linker and Hilscher give a sound labelled natural deduction proof system for a version of the logic without the hybrid extension [19]. Doczkal and Smolka formalize hybrid logic with nominals but no special operators in constructive type theory using the proof assistant Coq. They do not define a proof system but give algorithmic proofs of small model theorems and computational decidability of satisfiability, validity, and equivalence of formulas [10]. The present work appears to be the first proof system for hybrid logic with a formalized completeness proof.

Formalizations of completeness proofs in Isabelle exist for, among others, a tableau system and a one-sided sequent calculus for first-order logic [14], a natural deduction system for first-order logic [3], a Hilbert system for epistemic logic [12], and the first-order resolution calculus [21]. Blanchette et al. give abstract proofs of soundness and completeness that can be instantiated for a range of Gentzen and tableau systems for various flavors of first-order logic [7]. Moreover, Blanchette gives an overview of the formalized metatheory of various logical calculi and automatic provers in Isabelle [6].

6 Future Work

We are currently working on restricting the GoTo and Nom rules to ensure termination; previous (un-formalized) work has shown via translation to and from a different system that completeness can be preserved and that the resulting system is terminating [5]. We would like to show termination directly via a decreasing length argument in the style of Bolander and Blackburn's work on an internalized labelled tableau system [8]. Given a sound, complete and terminating system we want to verify an algorithm based on it and use it as a decision procedure for basic hybrid logic. Moreover, as the completeness proof that we formalized is based on reasoning about maximal consistent sets and their properties, it should be possible to extend it to other key results for hybrid logic which have been proved by similar forms of reasoning, notably interpolation results [1].

7 Conclusion

We have presented a tableau system for basic hybrid logic whose soundness and completeness has been formalized in Isabelle/HOL. Moreover, we have shown how to lift certain restrictions on the rules so that an existing completeness proof could be formalized and applied. The fact that the completeness proof we formalized is a synthetic proof suggests that it can be extended to a number of other key results for hybrid logic that can be found in the literature.

References

1. Areces, C., Blackburn, P., Marx, M.: Hybrid logics: characterization, interpolation and complexity. J. Symb. Logic **66**(3), 977–1010 (2001)
2. Areces, C.E.: Logic engineering: the case of description and hybrid logics. Ph.D. thesis, Institute for Logic, Language and Computation, Amsterdam, The Netherlands (2000)
3. Berghofer, S.: First-Order Logic According to Fitting. Archive of Formal Proofs, August 2007. http://isa-afp.org/entries/FOL-Fitting.html. Formal proof development
4. Blackburn, P.: Representation, reasoning, and relational structures: a hybrid logic manifesto. Logic J. IGPL **8**(3), 339–365 (2000). https://doi.org/10.1093/jigpal/8.3.339
5. Blackburn, P., Bolander, T., Braüner, T., Jørgensen, K.F.: Completeness and termination for a Seligman-style tableau system. J. Logic Comput. **27**(1), 81–107 (2017). https://doi.org/10.1093/logcom/exv052
6. Blanchette, J.C.: Formalizing the metatheory of logical calculi and automatic provers in Isabelle/HOL (invited talk). In: Mahboubi, A., Myreen, M.O. (eds.) Proceedings of the 8th ACM SIGPLAN International Conference on Certified Programs and Proofs. CPP 2019. pp. 1–13. ACM (2019)
7. Blanchette, J.C., Popescu, A., Traytel, D.: Soundness and completeness proofs by coinductive methods. J. Autom. Reasoning **58**(1), 149–179 (2016). https://doi.org/10.1007/s10817-016-9391-3
8. Bolander, T., Blackburn, P.: Termination for hybrid tableaus. J. Logic Comput. **17**(3), 517–554 (2007). https://doi.org/10.1093/logcom/exm014
9. Braüner, T.: Hybrid Logic and its Proof-Theory. Springer, Dordrecht (2010)
10. Doczkal, C., Smolka, G.: Constructive formalization of hybrid logic with eventualities. In: Jouannaud, J.-P., Shao, Z. (eds.) CPP 2011. LNCS, vol. 7086, pp. 5–20. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25379-9_3
11. Fitting, M.: Proof Methods for Modal and Intuitionistic Logics, vol. 169. Springer, Heidelberg (1983). https://doi.org/10.1007/978-94-017-2794-5
12. From, A.H.: Epistemic Logic. Archive of Formal Proofs, October 2018. http://isa-afp.org/entries/Epistemic_Logic.html. Formal proof development
13. From, A.H.: Formalizing a Seligman-Style Tableau System for Hybrid Logic. Archive of Formal Proofs, December 2019. http://isa-afp.org/entries/Hybrid_Logic.html. Formal proof development
14. From, A.H.: A Sequent Calculus for First-Order Logic. Archive of Formal Proofs, July 2019. http://isa-afp.org/entries/FOL_Seq_Calc1.html. Formal proof development
15. From, A.H.: Hybrid logic. Master's thesis, Technical University of Denmark, January 2020
16. Horrocks, I., Glimm, B., Sattler, U.: Hybrid logics and ontology languages. Electron. Notes Theoret. Comput. Sci. **174**(6), 3–14 (2007). https://doi.org/10.1016/j.entcs.2006.11.022
17. Jørgensen, K.F., Blackburn, P., Bolander, T., Braüner, T.: Synthetic completeness proofs for Seligman-style tableau systems. In: Proceedings of the 11th Conference on Advances in Modal Logic, held in Budapest, Hungary, 30 August–2 September 2016, vol. 11, pp. 302–321 (2016)
18. Linker, S.: Hybrid Multi-Lane Spatial Logic. Archive of Formal Proofs, November 2017. http://isa-afp.org/entries/Hybrid_Multi_Lane_Spatial_Logic.html. Formal proof development

19. Linker, S., Hilscher, M.: Proof theory of a multi-lane spatial logic. Log. Methods Comput. Sci. **11**(3) (2015). https://doi.org/10.2168/LMCS-11(3:4)2015
20. Nipkow, T., Wenzel, M., Paulson, L.C. (eds.): Isabelle/HOL - A Proof Assistant for Higher-Order Logic. LNCS, vol. 2283. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-45949-9
21. Schlichtkrull, A.: The Resolution Calculus for First-Order Logic. Archive of Formal Proofs, June 2016. http://isa-afp.org/entries/Resolution_FOL.html. Formal proof development
22. Seligman, J., Liu, F., Girard, P.: Facebook and the epistemic logic of friendship. In: Schipper, B.C. (ed.) Proceedings of the 14th Conference on Theoretical Aspects of Rationality and Knowledge (TARK 2013), Chennai, India, pp. 229–238 (2013)
23. Seligman, J.: The logic of correct description. In: de Rijke, M. (ed.) Advances in Intensional Logic. Applied Logic Series, vol. 7, pp. 107–135. Springer, Dordrecht (1997). https://doi.org/10.1007/978-94-015-8879-9_5
24. Seligman, J.: Internalization: the case of hybrid logics. J. Logic Comput. **11**(5), 671–689 (2001). https://doi.org/10.1093/logcom/11.5.671
25. Smullyan, R.M.: First-Order Logic. Dover Publications, New York (1995)