On the Role of Automated Proof-Assistants in the Formalization of Upper Ontologies

João R. M. Nicola[1], Giancarlo Guizzardi[2,3]

[1]Ontology and Conceptual Modeling Research Group, PPGI, Federal University of Espírito Santo, Av. Fernando Ferrari, 514, 29075-910, Vitória, ES, Brazil

[3]Faculty of Computer Science, Free University of Bozen-Bolzano, piazza Domenicani, 3, 39100, Bolzano, Italy.

[4]Faculty of Electrical Engineering, Mathematics and Computer Science Zilverling, University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands.

Abstract

The use of formal languages in the specification of upper ontologies helps establishing precise and unambiguous definitions for its concepts and relations. In this context, the use of formal languages with support of proof-assistant software systems has potential of aiding the specification author in various aspects. We describe a study case in which the Isabelle/HOL language and the Isabelle proof-assistant environment are used to formalize a simplified version of the UFO-A ontology of endurants, to verify and correct the original axiomatization, and to optimize the specification theory's axioms and signature.

Keywords

applied ontology, upper ontology, formal methods, proof assistants,

1. Introduction

Upper ontologies are conceptual frameworks that describe systems of general concepts and formal relations that play a foundational role in the construction of other, more specific, ontologies (core ontologies, domain ontologies). An upper ontology should be considered general, in the sense that its elements are present across various (or all) domains, but also complete, in the sense that any concept in the domains of discourse in the scope of an upper ontology should be analyzable using the concepts of the latter. To achieve this objective, an upper ontology describes concepts that represent answers to questions such as "what is an object", "what is a property" or "what is an event". Some examples of upper ontologies include BFO [1], DOLCE [2], GFO [3] and UFO [4].

Since the adoption of an upper ontology represents a commitment regarding the most basic elements of reality, any ambiguity or imprecision in its specification may lead its adopters to a *false agreement*, a situation in which distinct interpretations of the upper ontology concepts may lead agents to believe, erroneously, that they agree on the meaning of a concept specification. To avoid issues related to the inherent ambiguity of informal languages it is common to

FOUST 2021: 5th Workshop on Foundational Ontology, held at JOWO 2021: Episode VII The Bolzano Summer of Knowledge, September 11–18, 2021, Bolzano, Italy

joaoraf@gmail.com (J. R. M. Nicola); g.guizzardi@utwente.nl (G. Guizzardi)

https://people.utwente.nl/g.guizzardi (G. Guizzardi)

rely on formal logical languages for the specification of an upper ontology, in which case a specification takes the form of a logical theory that describe, as precisely as possible, the intended interpretation of its concepts.

The construction of these logical theories can be aided by a variety of automated and semi-automated software tools that can be used in various phases of this process: in the verification of syntactical correctness, in the construction and verification of theorem proofs and in the analysis of the admissible interpretations of the theory. Some of these tools are organized in integrated software environments, called a proof-assistants, including Coq [5], HOL4 [6], NuPRL [7] and Isabelle [8, 9], where the latter one is used in the case study described in the present work. Besides providing software tools to facilitate the construction of logical theories, proof-assistants also provide libraries of theories that provide definitions and axiomatizations that can leveraged in the construction process. Furthermore, the formal languages supported by proof-assistants may provide constructs that aid in the organization and readability of upper ontology theories.

This paper describes a case study in which a simplified version of the Unified Foundational Ontology (UFO) fragment of endurants, UFO-A, is formalized in the Isabelle/HOL language, with the help of the Isabelle proof-assistant system. UFO is an upper ontology designed to provide an ontologically well-founded conceptual basis for conceptual modeling languages. It was first introduced in [4] as an formal ontology of *endurants* and *endurant universals*, describing concepts such as *moments*, *substantials*, *modes*, *qua entities*, *relators*, *quantities*, *collectives, functional complexes, qualities* and *quality spaces*, along with related formal relations such as *existence, inherence*, *parthood, existential dependency* and *generic existential dependency*, and was later extended to include ontologies of events (UFO-B) [10] and of social concepts (UFO-C) [11].

The scope of the simplified upper ontology described in the present case study is limited to a fragment of the UFO ontology of endurants (UFO-A), including the concepts of existence, possible worlds, inherence, moments and substantials. In the present case study we shown how the Isabelle/HOL language and the Isabelle proof-assistant can be useful in the organization, simplification, verification and correction of a formal specification of this simplified upper ontology[1]. The case study, described in section 3, is divided into two parts: subsection 3.1 describes the formalization of the concepts of *possible worlds, existence* and *existential dependency*, and shows the use of Isabelle/HOL *locales* and theorem proofs in a redesign of the theory that reduces the complexity of the theory while maintaining its interpretation; while subsection 3.2 describes the formalization of the concepts of *inherence, substantials* and *moments,* and uses Isabelle/HOL theorems to prove the incompleteness of the original UFO-A axioms regarding the *inherence* relation and the characterization of the missing gap in the original axioms, proposing an alternate axiomatization that is simpler than the original and that addresses the identified issues. The case study descriptions are preceded by a brief background discussion, in section 2, that includes a discussion regarding the design of an upper ontology formal theory (subsection 2.1) and, a description of a strategy for encoding modular theories in Isabelle/HOL. (subsection 2.2).

[1]The Isabelle/HOL source code for the theories presented in this paper can be found at https://github.com/joaoraf/foust-2021-paper-isabelle-sources.

We would like to thank the reviewers for the relevant considerations and useful suggestions and corrections.

2. Background

2.1. Upper Ontology Theory Design

Given an informal description of an upper ontology, the construction of a corresponding formal specification is by process with a determinate outcome. Insofar as the main goal is to produce a formal specification of the intended models of the upper ontology, there isn't necessarily a unique set of axioms and definitions that achieves it. Two logically equivalent set of axioms, though specifying the same set of models, may differ with respect to pragmatic concerns, such as their intelligibility, their relative independence or their usability in a proof-assistant environment. These concerns provide a degree of freedom allows other goals to be considered as well, besides the correct specification of the intended models, among which we may highlight: (1) producing a theory that is easy for (human) stakeholders to understand and (2) producing a formal artifact that is as useful as possible as a formal tool. The first goal is due to the fact that the main consumers of an upper ontology are human beings. The second is due to the fact that a formal specification, aside from being a reference document, may have other uses, e.g. as a basis for specifying extensions of the upper ontology or of other ontologies derived from the same, or in the formal analysis of the properties of the upper ontology or even as a component in a Formal Method's based development process.

Due to these secondary goals, variables that are not related to the verification of the consistency of the theory may also be considered in the design of the theory, such as:

- choice of formal language;
- naming and notation conventions;
- theory organization (modularity and order of presentation);
- (re)use of concepts defined in other theories (existing libraries of formal theories);
- concept introduction by non-conservative extension, i.e. addition of free symbols and restricting axioms, or by conservative extension, i.e. through well-founded definitions;
- choices between distinct but logically equivalent sets of axioms.

All of the above elements have an impact on the intelligibility of the final theory and the last four may impact the utility of the theory, i.e. how ease it is to extend it, to use its axioms in proofs or to produce models of the same. To decide between some of these choices, it might be necessary prove the equivalence of different forms of organizing the theory, of different axiom sets or definition orders, activities that along with proofs of consistency, can be made easier and more controlled by using the tools provided by a proof-assistant, as illustrated in sections subsection 3.1 and subsection 3.2.

2.2. Writing Theories Using Isabelle/HOL *locales*

There are various strategies for encoding theories in Isabelle/HOL. The most straightforward is to encode it directly as axioms in a Isabelle/HOL theory file, introducing the types used in the theory through *typedecl* statements and the free symbols and axioms of the theory through *axiomatization* statements, followed by definitions and theorems [12]. This strategy, though simple, presents some important drawbacks. First, it adds the symbols directly to the global syntactical scope, limiting the choice of notation as to avoid conflict with the existing symbols in the Isabelle/HOL library. Secondly, since Isabelle/HOL does not require a proof of consistency of the axioms that are also introduced in the global scope but simply adds them as valid facts, it risks collapsing the logical system in a manner that is hard to detect. Third, it does not allow the models of the theory to be manipulated at the object level, hindering the investigation of the model-theoretic properties of the theory.

However, Isabelle/HOL provides a mechanism for encoding theories in a modular way using *locale* constructs [13]. A locale is a named context that may include free symbols, axioms and definitions, but which isolates those from the global scope. This produces two different views on the elements of the locale, inside and outside its context. In the context of the locale, the axioms are assumed as facts and can be used in lemmas, while the free symbols are presumed to exist an can be referred to in definitions and lemmas. Outside, in the global scope, the free symbols and axioms are not present. Instead, the free symbols appear as extra parameters in functions and predicates declared in the locale's context, while the axioms are added as extra conditions in all the lemmas and theorems that were declared in the context.

In Isabelle/HOL, the order of the statements is relevant, since a statement may only refer to symbols or theorems that were present before it. This characteristic leads to a important limitation in the use of Isabelle/HOL locales: since any definition made in a locale's context comes *after* the statement of the locale axioms, the latter cannot, in principle, refer to defined elements. However, it is possible to work around this limitation by separating the locale into two locales: one, which only declares the free symbols, but does not state any axiom, and a second one which extends the first by adding the axioms. Using this pattern, it is possible to define the symbols in the context of the first locale, which we call the signature locale of the theory, and refer to those in the axioms of the second locale, which we call the axiomatization locale of the theory. This strategy also has the benefit of freeing the definitions from the conditions represented by the axioms: a definition stated in a free locale (without axioms) is exported from the context of the locale as a simple equality and can be used unconditionally, for example, as simplification rules. It also simplifies the construction and analysis of representations of models of the theory.

3. Revisiting UFO's Original Theory of Endurants

In this section we present a formalization of a part of the UFO's ontology of endurants (UFO-A). The formalization includes only the two most fundamental categories and relations pertaining to the notion of an endurant particular: possible worlds, endurants and existence, on subsection 3.1; and inherence, substantials and moments, on subsection 3.2. Other concepts and relations described in UFO-A were omitted due to the article's size constraints of this article.

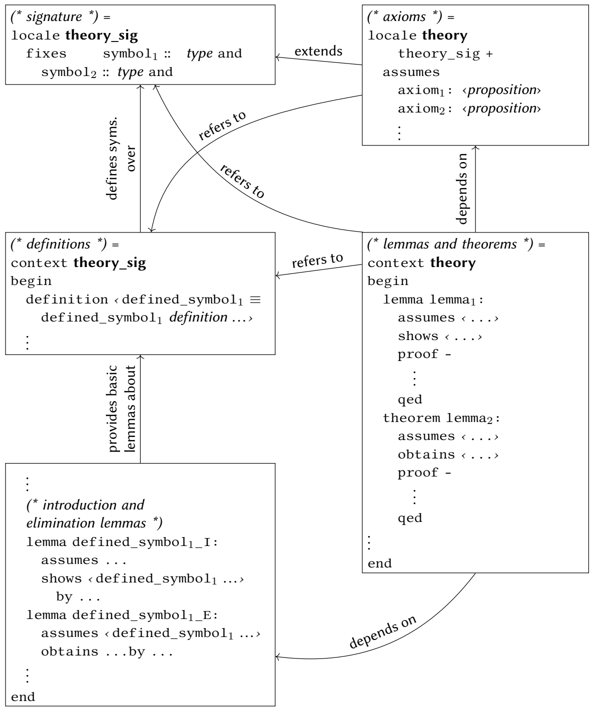


Figure 1: Representing theories in Isabelle/HOL using separate locales for signature and axioms.

3.1. Possible Worlds

We start the Isabelle/HOL axiomatization of the selected fragment of UFO by specifying the concepts of *existence*, *possible worlds* and of *endurants*. For simplicity reasons, we are considering endurants to be the whole class of entities that enjoy or may enjoy existence. As such, the goal is to formalize the notions that existence is a property enjoyed by endurants and that it is relative to a possible world. A *possible world*, on the other hand, is a configuration of endurants that represent a possible configuration of endurants in the universe of discourse.

Our first approach is based on UFO's original presentation [4], with some simplifications: we assume that there is a type of endurant representations (`'e` type parameter) and a type of possible world representations (`'w` type parameter), along with sets that represent the corresponding domains, $\mathcal{W}$ and $\mathcal{E}$, along with a binary predicate ($\texttt{existsIn} :: {}'\texttt{e} \Rightarrow{}' \texttt{w} \Rightarrow \texttt{bool}$) that represents the existence relation. Following the strategy delineated in subsection 2.2, this theory can be encoded using the locales described in Figure 2.

At this point we may consider the possibility of simplifying this theory. To do so, we can consider whether or not: (a) we can reduce the quantity of types; (b) we can reduce the number of free symbols; and (c) we can replace the axioms with a smaller and simpler set. The first hints in this direction are given by the following lemmas, which prove two equalities in the locale context:

1. The set of endurants is equal to the union of the extensions of all possible worlds, i.e. $\mathcal{E} = \bigcup \texttt{extensions}$; where

```
locale possible_worlds_original_sig =
  fixes
    𝒲 :: ‹'w set› and
    ℰ :: ‹'e set› and
    existsIn :: ‹'e ⇒ 'w ⇒ bool›

locale possible_worlds_original =
  possible_worlds_original_sig +
assumes
  existence_scope:
  ‹existsIn x w ⟹
      w ∈ 𝒲 ∧ x ∈ ℰ›
and endurants_exist_somewhere:
   ‹x ∈ ℰ ⟹ ∃w. existsIn x w›
and world_equality:
   ‹⟦ w1 ∈ 𝒲 ; w2 ∈ 𝒲 ;
    ∀x. existsIn x w1 ⟷ existsIn x
w2 ⟧ ⟹
    w1 = w2›
and endurants_are_contingent:
    ‹x ∈ ℰ ⟹
     ∃w ∈ 𝒲. ¬ existsIn x w›
and at_least_one_possible_world:
    ‹𝒲 ≠ ∅›
```

Figure 2: Possible worlds axiomatization based on the original presentation.

```
definition ‹extensions ≡ { extensionOf w | w . w ∈ 𝒲 }›
definition ‹extensionOf w ≡ { x . existsIn x w }›
```

2. The existence relation is equal to the set membership relation on the extension of the world, i.e

```
existsIn x w = (w ∈ 𝒲 ∧ x ∈ extensionOf w)
```

These lemmas suggest that the corresponding free symbols, $\mathcal{E}$ and `inheresIn`, can be replaced with definitions over the other free symbol, i.e. the set of possible worlds $\mathcal{W}$. This change would reduce the number of free symbols from three to one, reducing the complexity of the theory models and potentially eliminating the need for some of the axioms.

Another important consideration is given by a lemma that proves that the set of possible worlds is isomorphic to the set of extensions of possible worlds, i.e. the `extensionOf` function is a bijection from the set $\mathcal{W}$ of possible worlds to the `extensions` set. This property suggests that the set of possible worlds can be replaced with the corresponding set of extensions.

Given these considerations, made with the support of lemmas proved in the context of this locale, we can propose an alternative axiomatization,shown in Figure 3. In comparison with the original locale, this one has less types (just the type `'e` of endurants), less symbols (just the set of possible worlds $\mathcal{W}$), and less axioms. Furthermore, the axioms characterize the set of possible worlds succinctly as a non-empty family of sets whose intersection is the empty set.

We prove the safety of using the alternative locale in place of the original one by proving lemmas that state that there is a pair of functions `pw1_to_pw2`, from the original models to the alternative models, and `pw2_to_pw1`, in the reverse direction, such that a structure is a valid model of the original locale just in case its image with respect to `pw1_to_pw2` is a valid model of the alternative locale and such that a family of sets is a valid model of the alternative locale if and only if its image with respect to `pw2_to_pw1` is also a valid model in the original locale, a situation summarized in Figure 4.

Since both locales are essentially equivalent, we use the simpler one as the base for continuing the axiomatization presented in subsection 3.2.

```
locale possible_worlds_alt_sig =
  fixes  𝒲 :: ‹'e set set›

definition ‹ℰ ≡ { x . ∃w ∈ 𝒲. x ∈ w }›

definition ‹existsIn x w ≡ w ∈ 𝒲 ∧ x ∈ w›

locale possible_worlds_alt =
  possible_worlds_alt_sig +
assumes
    world_set_intersection_empty: ‹⋂ 𝒲 = ∅›
and at_least_one_possible_world: ‹𝒲 ≠ ∅›
```

Figure 3: Alternative possible worlds axiomatization.

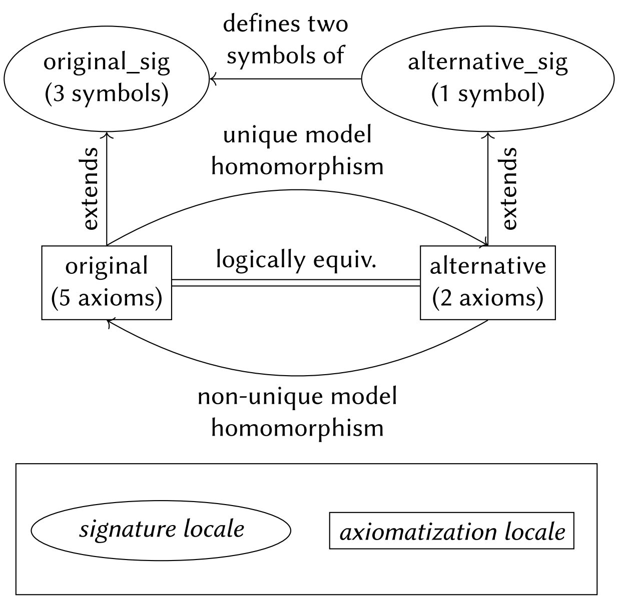


Figure 4: Summary of possible world locales.

3.2. Inherence

The next step in this case study is the formalization of the UFO *inherence* relation. This relation holds between an endurant and a moment that represents a particularized property of this endurant. In this section our focus is strictly on the inherence relation and on the two classes of endurants that are derived from it: substantials and moments. For simplicity sake, other elements that are used to distinguish the types of moments and that characterize the properties they represent are not considered.

UFO endurants are classified into two disjoint classes, depending on whether they *inhere* or not in other endurants. Endurants that do not inhere in any other endurant are called *substantials* and correspond to the commonsensical notion of object. Those that inhere in some

```
locale inheresIn_sig =
    possible_worlds_alt_sig where 𝒲 = 𝒲
  for 𝒲 :: ‹'e set set› +
  fixes
    inheresIn :: ‹'e ⇒ 'e ⇒ bool› (infix ‹◁› 75)

definition ‹ℳ ≡ { x | x y . inheresIn x y }›

definition ‹𝒮 ≡ { x . x ∈ ℰ ∧ (∀y. ¬ inheresIn x y) }›

definition ‹bearerOf s m ≡ (◁)⁻¹⁻¹›

definition ‹ultimate_bearer_of s m ≡ s ∈ 𝒮 ∧ m ∈ ℰ ∧ (◁)** m s›

definition ‹order_of x n ≡ x ∈ ℰ ∧ (∃s ∈ 𝒮. ((◁)^^n) x s)›
```

Figure 5: Inherence signature and basic definitions.

endurant are called *moments* and the endurant they inhere in is called their *bearer*. Inherence may occur in more than one level, i.e. a moment may inhere in another moment instead of inhering directly in a substantial. The number of inherence steps that separate a moment from a substantial is called the moment's *degree*, and the substantial that it inheres in directly, or indirectly, is called the moment's *ultimate bearer*. The signature of the inherence theory, as well as the definition of the symbols that correspond to the concepts mentioned in this paragraph are depicted in Figure 5.

Following the same methodology used in subsection 3.1, we start the formalization by stating a locale containing axioms from the original UFO presentation. However, instead of grouping these axioms in a single locale, we split them into two locales: `inherence_base`, containing axioms that states that the inherence relation implies existential dependency between the moment and its bearer and that moments inhere in a single endurant; and `inherence_original`, that extends the former with other axioms that state that inherence is a relation between endurants and that it is an irreflexive, asymmetric and anti-transitive relation. Both locales are depicted in Figure 6.

Analysis and Redesign

A first analysis that can be done over the original theory, as expressed in these locales, is the interdependence between axioms. Given the axioms of the `inherence_base` locale, we prove the following properties:

1. The `inherence_scope` axiom is derivable from the `inherence_base` axioms.
2. Inherence irreflexivity (`inherence_irrefl` axiom) and anti-transitivity (`inherence_antitransitive` axiom) are derivable from the asymmetry axiom (`inherence_asymm`).

Thus, we can safely simplify the `inherence_original` locale by excluding the `inherence_scope`, `inherence_irrefl` and `inherence_antitransitive` axioms. The resulting locale, called

```
locale inherence_base =
  inherence_sig +
  possible_worlds_alt +
  assumes
    inherence_imp_ed: ‹x ◁ y ⟹ ed x y› and
    moment_non_migration: ‹⟦ x ◁ y ; x ◁ z ⟧ ⟹ y = z›

locale inherence_original =
  inherence_base +
  assumes
    inherence_scope: ‹x ◁ y ⟹ x ∈ ℰ ∧ y ∈ ℰ› and
    inherence_irrefl: ‹¬ x ◁ x› and
    inherence_asymm: ‹x ◁ y ⟹ ¬ y ◁ x› and
    inherence_antitrgansitive: "⟦ x ◁ y ; y ◁ z ⟧ ⟹ ¬ x ◁ z"
```

Figure 6: Inherence locales: base and original theories.

```
locale inherence_simplified =
  inherence_base +
  assumes
    inherence_asymm: ‹x ◁ y ⟹ ¬ y ◁ x›
```

Figure 7: Simplified original inherence locale.

`inherence_simplified` and depicted in Figure 7, adds only the asymmetry axiom to the `inherence_base` locale. The equivalence between both locales is proven using a lemma.

After removing redundant axioms, we might want to check whether some expected properties that were not expressed in axioms in the original work actually hold. Two relevant properties are the *existence and uniqueness of ultimate bearers* of a moment and the *well-definedness of the degree* of a moment. The first means that that every moment should inhere, directly or indirectly, on a single substantial, while the second means that every moment should inhere to a substantial, directly or indirectly, by a well-defined number of inherence steps. In other words, a moment must express, directly or indirectly, a property of a single substantial and it should do so by a well defined and unique degree, i.e. it cannot be, for example, a first degree and a second degree moment at the same time.

Before we evaluate whether or not these properties hold, we prove the following in the context of the original theory:

1. Ultimate bearers are unique, if they exist;
2. The degree of a moment is unique, if it has an degree;
3. The existence of a degree for a moment and the existence of an ultimate bearer are logically equivalent.

In summary, it is sufficient to evaluate whether or not an ultimate bearer exist for every moment. A first effort is to try to prove the proposition “$\forall x \in \mathcal{M}. \exists y.$ `ultimate_bearer_of` $y\, x$. If we

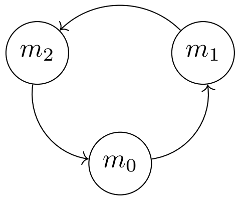


Figure 8: Counterexample identified by Nitpick for the original inherence theory.

```
locale inherence_with_ultimate_bearers =
  inherence_simplified +
assumes
  ultimate_bearers_ex:
  ‹x ∈ ℳ ⟹ ∃y. ultimate_bearer_of y x›
```

Figure 9: Inherence locale with explicit requirement for the existence of ultimate bearers.

```
locale inherence_acyclic =
  inherence_simplified +
 assumes
  acyclic_inherence: ‹¬ ((◁)⁺⁺) x x›
```

Figure 10: Inherence locale with cycle exclusion axiom.

can prove it successfully in Isabelle/HOL, the issue is settled. However, when we present this proposition to Isabelle/HOL and ask it to try to find a counterexample using the Nitpick model finder, it presents the counterexample depicted in Figure 8.

A straightforward solution to this issue is to add an axiom explicitly stating that ultimate bearers must exist, as in the locale depicted in Figure 9. This solution, however, may be considered less than satisfactory due to the fact that it does not elucidate the reason as to why the axiomatization so far is unable to guarantee the existence of ultimate bearers for all moments. Besides not being explanatory, the axiom may also unnecessarily strong in the sense that addition of a weaker axiom to the existing axioms could suffice for guaranteeing the existence of all ultimate bearers.

To look for alternative solutions, we have to analyze the unintended models that are being accepted given the current axioms. The first case is the one found by Nitpick (see Figure 8). In this case, the presence of a *cycle* in the inherence relation was the cause of the nonexistence of an ultimate bearer for all moments. The hypothesis that can be raised is that the exclusion of cycles in the relation could be enough to achieve our goal. To test this hypothesis, we add a locale with that extends the original theory with an axiom that excludes cycles (see Figure 10) and try to find a counterexample.

After failing to find a counterexample in the context of the `inherence_acyclic` locale, using Nitpick, we may consider that a counterexample model, if it exists, might be outside the scope of Nitpick, i.e. it might be too large for Nitpick to find given its scope and time limit

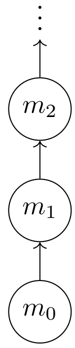


Figure 11: Counterexample of acyclic inherence theory.

```
locale inherence_no_infinite_chains =
  inherence_acyclic +
assumes
  no_infinite_up_chains:
    ‹⟦ x ∈ X ; ∀y ∈ X. (◁)** x y ;
      ∀x ∈ X. ∀y ∈ X. (◁)** x y ∨ (◁)** y x ⟧ ⟹ finite X›
```

Figure 12: Locale with only finite ascending inherence chains.

parameters, or it might be infinite (Nitpick only constructs finite models). In that case, we might try to find a counterexample manually, by defining a candidate counterexample directly in Isabelle/HOL and attempt to prove that it is (1) a valid model for the `inherence_acyclic` locale and (2) that it has a moment without an ultimate bearer.

One such model exists, as depicted in Figure 11. The main characteristic of this model is that it has an infinite ascending chain inherence chain, i.e. a moment that has an infinite number of indirect bearers.

Repeating the same process, we add an axiom to the `inherence_acyclic locale`, excluding infinite ascending inherence chains, producing the locale depicted in Figure 12. In the context of this locale, we can finally prove that all ultimate bearers exist and thus, that the issue is solved.

However, the exclusion of cycles and of infinite ascending chains suggest that we could better explain the inherence relation by requiring it to be noetherian, i.e. for its converse (`bearerOf`) to be wellfounded, i.e. any non-empty set has a maximal element with respect to the inherence relation. In fact, we prove in Isabelle/HOL that this property is equivalent to the existence of all ultimate bearers. Furthermore, we also prove that the addition of an axiom requiring the wellfoundness of the converse of the inherence relation makes redundant all the axioms of that were added by `inherence_simplified` to `inherence_base`. Thus we end with the locale `inherence_noetherian`, depicted in , that replaces the 3 axioms that `inherence_no_infinite_chains` adds to `inherence_base` with a single axiom, since wellfoundness of the converse of the inherence relation implies that it is acyclic, irreflexive, anti-transitive, acyclic and without finite ascending inherence chains. A consequence of the

```
locale inherence_noetherian =
  inherence_base +
    assumes
    inherence_is_noetherian: ‹wfP ((◁)⁻¹⁻¹)›
```

where `wfP` is a predicate defined in the Isabelle/HOL library, such that

$$wfP\ (\triangleleft)^{-1-1} = (\forall Q.\ (\exists x.\ x \in Q) \longrightarrow (\exists z{\in}Q.\ \forall y.\ z \triangleleft y \longrightarrow y \notin Q))$$

Figure 13: Locale with a noetherian inherence relation.

need to use the notion of wellfoundess or of transitive closures to correctly specify UFO's inherence relation is that UFO's inherence relation cannot be axiomatized using a first-order theory, providing a solid argument for using more expressive languages, such as higher order logic, or dependent type theory, in UFO's specification.

Besides the reduction in the number of axioms, the characterization of the inherence relation as a noetherian relation also provides a useful transfinite induction rule that can be used in proofs regarding the inherence relation:

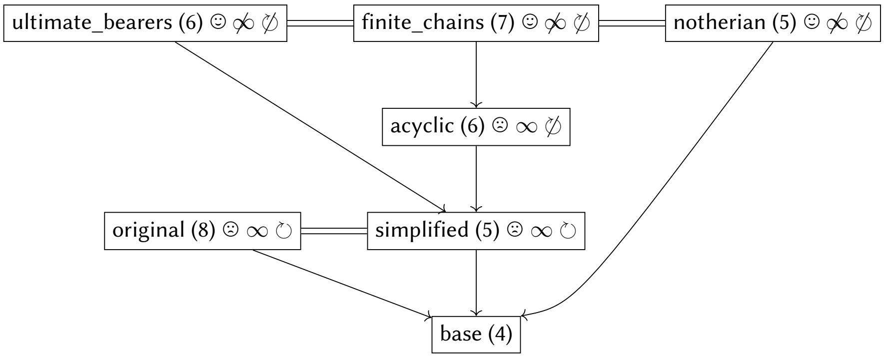
$$(\bigwedge x.\ \forall y.\ x \triangleleft y \longrightarrow P\ y \Longrightarrow P\ x) \Longrightarrow P\ z$$

The diagram in Figure 14 summarizes the alternate axiomatizations considered in this section. By using Isabelle to test different hypothesis regarding the original inherence axioms and to prove equivalences between different axiomatizations, we are able to reduce the number of axioms, fill a gap present in the original axiomatization regarding the existence of ultimate bearers and characterize the inherence relation as a noetherian relation.

4. Conclusion and Related Works

An upper ontology, due to its role as conceptual foundation for building other ontologies and conceptual models, stands to benefit from a rigorous treatment of its formal specification. The availability of mature interactive proof-assistant systems represents an opportunity for using automated and semi-automated formal tools in the improvement of upper ontology formalization processes.

In this paper we presented a study case in which an simplified version of the UFO ontology of endurants was formalized in the Isabelle/HOL formalism, showcasing the use of the Isabelle/HOL and associated software tools in the design of the ontology's specification theory, focusing on two fundamental UFO concepts, existence and inherence, and some other related concepts. We presented a brief discussion regarding the design of upper ontology logical theories and a methodology for presenting ontological theories using Isabelle/HOL *locales*. We described how the Isabelle/HOL formalism can be leveraged to evaluate alternate theory modular organizations, axiomatizations, signatures and to identify and address axiomatization gaps, in order to make the formal specification more precise with respect to its intended interpretation and to make it easier to understand and to use as the basis for further formal specifications and analysis.



locale name (# of axioms) …

Arrows	
$A \longrightarrow B$	A extends B.
$A = B$	A is logically equivalent to B.

Symbols	
☹	Has the missing ultimate bearer problem.
☺	Does not have the missing ultimate bearer problem.
∞	Admits infinite ascending inherence chains.
$\not\infty$	Excludes infinite ascending inherence chains.
⟳	Admits cycles in the inherence relation.
$\not\circlearrowleft$	Excludes cycles in the inherence relation.

Figure 14: Inherence locales summary.

Other formal specifications of the UFO-A ontology are described in [14], using the Alloy language [15], and in [16], however, they do not include analyses similar to those described in this work, e.g. alternative axiomatizations, signature simplification, nor do they point out the possibility of cyclic and infinite inherence chains.

References

[1] R. Arp, B. Smith, A. D. Spear, Building ontologies with basic formal ontology, Mit Press, 2015.

[2] C. Masolo, S. Borgo, A. Gangemi, N. Guarino, A. Oltramari, Ontology library. wonderweb deliverable d18 (ver. 1.0, 31-12-2003), 2003.

[3] H. Herre, B. Heller, P. Burek, R. Hoehndorf, F. Loebe, H. Michalek, General formal ontology (gfo), Part I: Basic Principles. Onto-Med Report 8 (2006).

[4] G. Guizzardi, Ontological foundations for structural conceptual models, CTIT, Centre for Telematics and Information Technology, 2005.

[5] Y. Bertot, G. Huet, P. Castéran, C. Paulin-Mohring, Interactive Theorem Proving and Program Development: Coq'Art: The Calculus of Inductive Constructions, Texts in Theoretical Computer Science. An EATCS Series, Springer Berlin Heidelberg, 2004.

[6] K. Slind, M. Norrish, A brief overview of hol4, in: International Conference on Theorem Proving in Higher Order Logics, Springer, 2008, pp. 28–32.
[7] R. L. Constable, S. F. Allen, H. M. Bromley, W. R. Cleaveland, J. F. Cremer, R. W. Harper, D. J. Howe, T. B. Knoblock, N. P. Mendler, P. Panangaden, J. T. Sasaki, S. F. Smith, Implementing Mathematics with the Nuprl Proof Development System, Prentice-Hall, Inc., USA, 1986.
[8] T. Nipkow, G. Klein, Concrete Semantics: With Isabelle/HOL, Springer International Publishing, 2014.
[9] T. Nipkow, M. Wenzel, L. C. Paulson, Isabelle/HOL: A Proof Assistant for Higher-order Logic, Springer-Verlag, Berlin, Heidelberg, 2002.
[10] A. B. Benevides, J. P. A. Almeida, G. Guizzardi, Towards a unified theory of endurants and perdurants: Ufo-ab., in: JOWO, 2019.
[11] G. Guizzardi, G. Wagner, Some applications of a unified foundational ontology in business modeling, in: Business systems analysis with ontologies, IGI Global, 2005, pp. 345–367.
[12] M. Wenzel, The Isabelle/Isar Reference Manual, 2021. URL: https://isabelle.in.tum.de/doc/isar-ref.pdf.
[13] C. Ballarin, Interpretation of locales in isabelle: Theories and proof contexts, in: International Conference on Mathematical Knowledge Management, Springer, 2006, pp. 31–43.
[14] B. F. Braga, J. P. A. Almeida, G. Guizzardi, A. B. Benevides, Transforming ontouml into alloy: towards conceptual model validation using a lightweight formal method, Innovations in Systems and Software Engineering 6 (2010) 55–63.
[15] D. Jackson, Software Abstractions: Logic, Language, and Analysis, The MIT Press, MIT Press, 2016.
[16] D. Porello, G. Guizzardi, Towards a first-order modal formalisation of the unified foundational ontology., in: JOWO, 2017.