Noname manuscript No.
(will be inserted by the editor)

Exploring Axiom Systems for Category Theory

Utilizing a Novel Approach to Automate Free Logic in HOL

Christoph Benzmüller · Dana Scott

Received: date / Accepted: date

Abstract A shallow semantical embedding of free logic in classical higher-order logic is presented, which enables the off-the-shelf application of higher-order interactive and automated theorem provers (and their integrated sub-provers) for the formalisation and verification of free logic theories. Subsequently, this approach is exemplarily employed in a selected domain of mathematics: starting from a generalization of the standard axioms for a monoid we present a stepwise development of various, mutually equivalent foundational axiom systems for category theory. As a side-effect of this work some (minor) issue in a prominent category theory textbook has been revealed.

Keywords Free Logic · Classical Higher-Order Logic · Category Theory · Interactive and Automated Theorem Proving

1 Introduction

Partiality and undefinedness are prominent challenges in various areas of mathematics and computer science. Unfortunately, however, modern proof assistant systems and automated theorem provers based on traditional classical or intuitionistic logics provide rather inadequate support for these challenge concepts. Free logic offers a theoretically appealing solution, but is has been considered as rather unsuited towards practical utilisation.

In the first part of this article (§2 and §3) we show how free logic can be "implemented" in any theorem proving system for classical higher-order

F. Author
first address
Tel.: +123-45-678910
Fax: +123-45-678910
E-mail: fauthor@example.com

S. Author
second address

logic (HOL) [1]. The proposed solution employs a semantic embedding of free (or inclusive logic) in HOL. We present an exemplary implementation of this idea in the mathematical proof assistant Isabelle/HOL [3]. Various state-of-the-art first-order and higher-order automated theorem provers and model finders are integrated (modulo suitable logic translations) with Isabelle via the Sledgehammer tool [2], so that our solution can be utilized, via Isabelle as foreground system, with a whole range of other background reasoners. As a result we obtain an elegant and powerful implementation of an interactive and automated theorem proving (and model finding) system for free logic.

To demonstrate the practical relevance of our new system, we present, in the second part of this article, a stepwise development of axiom systems for category theory by generalizing the standard axioms for a monoid to a partial composition operation. Our purpose is not to make or claim any contribution to category theory but rather to show how formalizations involving the kind of logic required (free logic) can be validated within modern proof assistants.

A total of eight different axiom systems is studied. The systems I-VI are shown to be equivalent. The axiom system VII slightly modifies axiom system VI to obtain (modulo notational transformation) the set of axioms as proposed by Freyd and Scedrov in their textbook "Categories, Allegories" [**?**], published in 1990; see also Subsection **??** where we present their original system. While the axiom systems I-VI are shown to be consistent, a constricted inconsistency result is obtained for system VII (when encoded in free logic where free variables range over all objects): We can prove $\exists x.\neg(Ex) \rightarrow False$, where E is the existence predicate. Read this as: If there are undefined objects, e.g. the value of an undefined composition $x \cdot y$ then we have falsity. By contraposition, all objects (and thus all compositions) must exist. But when we assume the latter, then the axiom system VII essentially reduces categories to monoids. We note that axiom system V, which avoids this problem, corresponds to a set of axioms proposed by Scott @cite "Scott79" in the 1970s. The problem can also be avoided by restricting the variables in axiom system VII to range only over existing objects and by postulating strictness conditions. This gives us axiom system VIII.

Our exploration has been significantly supported by series of experiments in which automated reasoning tools have been called from within the proof assistant Isabelle/HOL @cite "Isabelle" via the Sledgehammer tool @cite "Sledgehammer". Moreover, we have obtained very useful feedback at various stages from the model finder Nitpick @cite "Nitpick" saving us from making several mistakes.

At the conceptual level this paper exemplifies a new style of explorative mathematics which rests on a significant amount of human-machine interaction with integrated interactive-automated theorem proving technology. The experiments we have conducted are such that the required reasoning is often too tedious and time-consuming for humans to be carried out repeatedly with highest level of precision. It is here where cycles of formalization and experimentation efforts in Isabelle/HOL provided significant support. Moreover, the technical inconsistency issue for axiom system VII was discovered

by automated theorem provers, which further emphasises the added value of automated theorem proving in this area.

The content of article is combines, extends and clarifies the contributions reported in two previous papers [**?**,**?**].

2 Preliminaries

2.1 Free Logic

Free logic [**?**,**?**] refers to a class of logic formalisms that are free of basic existence assumptions regarding the denotation of terms. Remember that terms in e.g. traditional classical and intuitionistic predicate logics always denote an (existing) object in a given (non-empty) domain $\mathbf{D}$, which also serves as the domain of quantification, that is, the set of objects the existential and universal quantifiers of the logic range over. In free logic these basic assumption are abolished. Terms do still denote objects in a (non-empty) domain $\mathbf{D}$, but a (possibly empty) set $\mathbf{E} \subseteq \mathbf{D}$ is chosen to characterize the subdomain of "existing" resp. "defined" objects in $\mathbf{D}$. Quantification, in contrast to traditional logics, is now restricted to this set $\mathbf{E}$ of existing/defined objects only. It is obvious how this can be used to model undefideness and partiality: problematic terms, e.g. division by zero or improper definite descriptions, still denote, but they refer to undefined objects, that is, objects d in $\mathbf{D} \setminus \mathbf{E}$ lying outside of the scope of quantification.

The particular notion of free logic as exploited in the remainder of this article has been introduced by Scott [**?**]. A graphical illustration of this notion of free logic is presented in Fig. 1. It employs a distinguished undefined object $\star$.

Definition 1 (Syntax of *FFOL*) Given a denumerable set V of variable symbols, a denumerable set F of n-ary function symbols ($n \geq 0$), and a denumerable set P of n-ary predicate symbols ($n \geq 0$).

The terms and formulas of *FFOL* are formally defined as the smallest sets such that:

1. each variable $x \in V$ is a term of *FFOL*,
2. given any n-ary ($n \geq 0$) function symbol $f \in F$ and terms $t_1, \ldots, t_n$ of *FFOL*, then $f(t_1, \ldots, t_n)$ is a term of *FFOL*,
3. given terms t_1 and t_2 of *FFOL*, then $t_1 = t_2$ is an (atomic) formula of *FFOL*,
4. given any n-ary ($n \geq 0$) predicate symbol $p \in P$ and terms $t_1, \ldots, t_n$ of *FFOL*, then $p(t_1, \ldots, t_n)$ is an (atomic) formula of *FFOL*,
5. given formulas r and s of *FFOL*, then $\neg r$, $r \rightarrow s$ and $\forall x.r$ are (complex) formulas of *FFOL*
6. given a formulas r of *FFOL*, then $\iota x.r$ is a term of *FFOL* (definite description).

Further formulas of *FFOL* can be defined as usual.

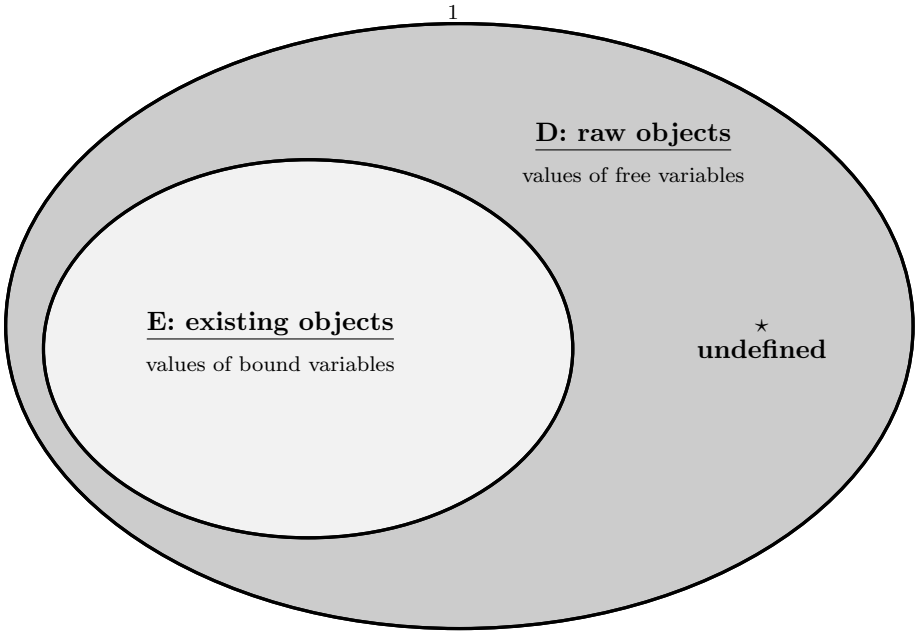

Fig. 1 Illustration of the Semantical Domains of Free Logic

Definition 2 (Dual-domain (positive) semantics of *FFOL*) A model structure for *FFOL* consists of a triple $\langle D, E, I\rangle$, where D is a non-empty raw domain of objects, $E \subseteq D$ a possible empty set of "existing" resp. "defined" objects, and I an Interpretation function mapping 0-ary function symbols (constants) to objects $d \in E$, 0-ary predicate symbols (propositions) to *True* or *False*, n-ary function symbols (for $n \geq 1$) to n-ary functions $D \times \ldots \times D \longrightarrow D$ and n-ary predicate symbols (for $n \geq 1$) to n-ary relations $D \times \ldots \times D$.

Given an variable assignment $g : V \longrightarrow D$, we define the interpretation function $\| \cdot \|^{I,g}$ for terms and formulas of *FFOL* as follows:

1. $\|x\|^{I,g} = g(x)$ for variable symbols x $f \in F$
2. $\|c\|^{I,g} = I(c)$, where $c \in F$ is an 0-ary function symbol
3. $\|f(t_1, \ldots, t_n)\|^{I,g} = I(f)(\|t_1\|^{I,g}, \ldots, \|t_n\|^{I,g})$, where $f \in F$ is an n-ary $(n \geq 1)$ function symbol
4. $\|p\|^{I,g} = I(p)$, where $p \in F$ is an 0-ary predicate symbol
5. $\|t_1 = t_2\|^{I,g} = \mathit{True}$ iff $\|t_1\|^{I,g} = \|t_2\|^{I,g}$ ([1]
6. $\|p(t_1, \ldots, t_n)\|^{I,g} = \mathit{True}$ iff $(\|t_1\|^{I,g}, \ldots, \|t_n\|^{I,g}) \in I(p)$ for n-ary $(n \geq 1)$ predicate symbols $p \in P$
7.

[1] Here we could e.g. require $\|t_1\|^{I,g} \in E$ and $\|t_2\|^{I,g} \in E$ as an additional condition.

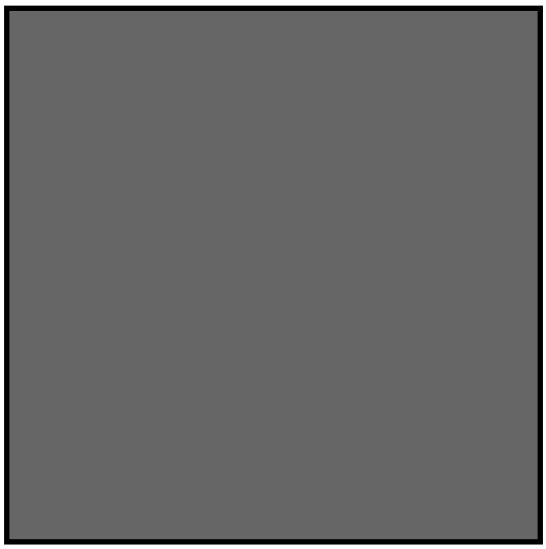

Fig. 2 Please write your figure caption here

Table 1 Please write your table caption here

first	second	third
number	number	number
number	number	number

3 Section title

Text with citations [**?**] and [**?**].

3.1 Subsection title

as required. Don't forget to give each section and subsection a unique label (see Sect. 3).

Paragraph headings Use paragraph headings as needed.

$$a^2 + b^2 = c^2 \tag{1}$$

References

1. Benzmüller, C., Miller, D.: Automation of higher-order logic. In: J. Siekmann, D. Gabbay, J. Woods (eds.) Handbook of the History of Logic, Volume 9 — Logic and Computation. Elsevier (2014)

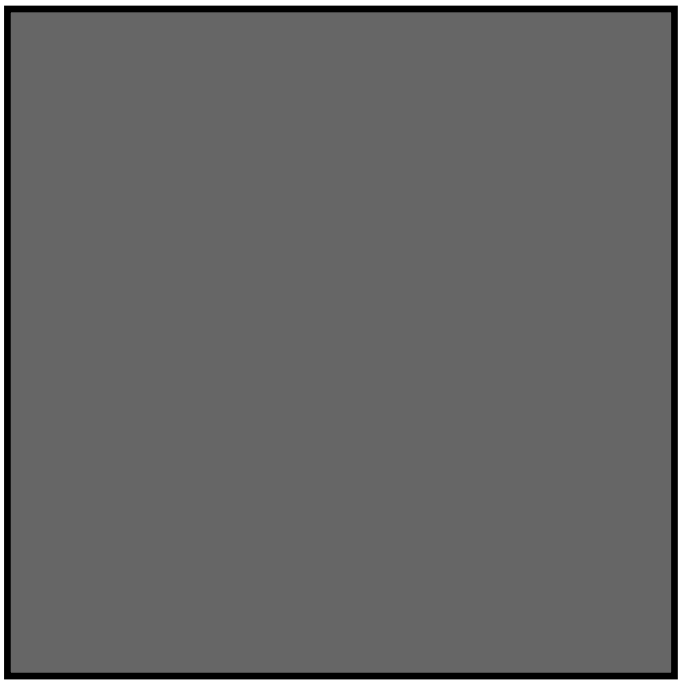

Fig. 3 Please write your figure caption here

2. Blanchette, J.C., Böhme, S., Paulson, L.C.: Extending Sledgehammer with SMT solvers. Journal of Automated Reasoning **51**(1), 109–128 (2013). DOI 10.1007/s10817-013-9278-5. URL http://dx.doi.org/10.1007/s10817-013-9278-5
3. Nipkow, T., Paulson, L.C., Wenzel, M.: Isabelle/HOL: A Proof Assistant for Higher-Order Logic. No. 2283 in LNCS. Springer (2002)