

# Some Remarks on the Annotation %cons

**CoFI Note: T-8**

Version: October 20, 1999

Dieter Hutter\* *E-mail address for comments: [hutter@dfki.de](mailto:hutter@dfki.de)*

CoFI: The Common Framework Initiative  
<http://www.brics.dk/Projects/CoFI>

*This document is available on WWW<sup>†</sup>, and by FTP<sup>‡</sup>*

## Abstract

There has been a discussion about the definition of the annotation %cons in CASL. Within this note I like to point out some pitfalls for CASL-tools which have to support such annotations. This note is mostly a rephrase of well-known facts which have been published for instance by Paulo A.S. Veloso and TSE Maibaum in [Veloso92, VV91, Maibaum97].

## 1 What is the problem?

Conservative extension is frequently used in formal specifications for step-wise refinement and implementation of abstract datatypes. Basically we like to extend a given specification by new function or predicate definitions but without changing the intended meaning of the original parts of the specifications. E.g. we like to extend the definition of natural numbers by a recursive definition of addition but without changing the “meaning” of the specification of natural numbers.

A theory  $T'$  is an *extension* of a theory  $T$  (denoted  $T \subset T'$ ) if  $T'$  can be obtained from  $T$  by adding additional symbols and axioms.

---

<sup>†</sup><http://www.brics.dk/Projects/CoFI/Notes/T-8/>

<sup>‡</sup><ftp://ftp.brics.dk/Projects/CoFI/Notes/T-8/>

\*German Research Center for Artificial Intelligence GmbH, Stuhlsatzenhausweg 3, D-66123 Saarbrücken, Germany, Tel. -49-681-302-5317

There are two ways to define conservative extensions formally, either in terms of the theories (proof theoretical, pt) or in terms of their models (model theoretical, mt):

$T \subset T'$  is a *mt-conservative* extension iff every model of  $T$  can be expanded to a model of  $T'$ .

$T \subset T'$  is a *pt-conservative extension* iff the restriction of  $T'$  to sentences of the language of  $T$  consists only of consequences of  $T$ .<sup>1</sup>

It is well-known that mt-conservativeness implies pt-conservativeness but not vice versa [BP90]. The following example from [Veloso92] illustrates the differences:

Consider a specification of natural numbers with constructors 0 and  $s$  and a binary relation  $<$  in the following (first order) way:

$$\forall y : y = 0 \vee \exists x : y = s(x) \tag{1}$$

$$\forall x, y : x < s(y) \rightarrow (x < y \vee x = y) \tag{2}$$

$$\forall x : \neg x < 0 \tag{3}$$

$$\forall x, y : (x < y \vee x = y \vee y < x) \tag{4}$$

$$\forall x, y : x < y \rightarrow \neg y < x \tag{5}$$

$$\forall x, y, z : (x < y \wedge y < z) \rightarrow x < z \tag{6}$$

This theory is complete and maximally consistent; i.e. for every closed formula  $\Phi$  in the given language either  $\Phi$  or  $\neg\Phi$  holds. This might be surprising knowing Goedels results about arithmetic, but the reason is that the given language (using only  $s$ , 0 and  $<$ ) is so poor that you cannot specify any “interesting” property. Obviously, the axiomatization does **not** characterize natural numbers up to isomorphism. Non-standard models are the natural numbers **plus** additional copies of the integers. Especially the natural numbers plus one copy of the integers is a model of the presented theory.

We now extend this theory  $T$  to  $T'$  by a recursive definition of  $+$ .

$$0 + y = y \tag{7}$$

$$s(x) + y = s(x + y) \tag{8}$$

$$s(x) + y > y \tag{9}$$

The first two axioms coincide with the standard recursive definition of  $+$ . If our specification of natural numbers would contain an induction axiom then

<sup>1</sup>Notice that it is crucial to consider all sentences instead of for instance all axioms. For instance, extending of a theory of natural numbers by two axioms  $c = 0$  and  $c = s(0)$  would identify 0 and  $s(0)$  or render the theory inconsistent.

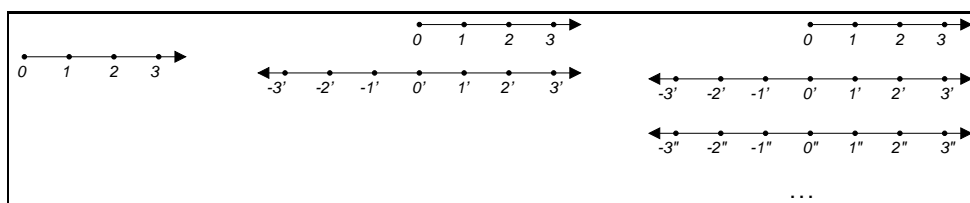


Figure 1: Various models of the given specification

the third axiom would be derivable from all the others. But in this case it is not.

Since  $T$  is maximally consistent,  $T'$  is a pt-conservative extension iff it is consistent, i.e. there is a model of  $T'$ . Obviously, the natural numbers is a model of  $T'$  and thus,  $T'$  is a pt-conservative extension of  $T$ .

From a model-theoretical view  $T'$  is no mt-conservative extension because we cannot extend the model of  $T$  consisting of natural numbers plus one copy of integers to  $T'$  (cf. [Enderton72]). In [Velo92] you can find a refutation proof of this showing that in this model any attempt to interpret  $+$  will result in a contradiction.

The reason for this phenomenon is related to the weakness of logics. The language of  $T$  is too poor to formulate a property which allows us to distinguish, for instance, between the standard model “natural numbers” and the non-standard model mentioned above. All properties which can be formulated in the language of  $T$ , behave in both models in the same way. The situation changes once we add a recursively defined function like  $+$  to the theory, then we have means to distinguish between some of the non-standard models. In practice we fail to rule out all non-standard models:

It is well-known that for many inductively defined structures like for instance natural numbers there is no categorial first-order theory. In case of natural numbers for instance, each first-order axiomatisation has also so-called non-standard models like those mentioned above. Changing to higher-order logics we have to adapt the semantics to obtain a calculus suitable for machines. This ends up in the use of Henkin-semantics which allow for complete calculi. But using Henkin-semantics we also fail to characterize natural numbers up to isomorphism (or more general, to characterize some notion of initiality (cf. [Andrews86] pp. 199)). Roughly speaking, the price for being complete is some kind of blurring the interpretation of given axiomizations.

---

## 2 What are the consequences for CASL?

The question arises which definition of conservative extension should be chosen to allow for optimal tool support. Initially I thought that the proof theoretical definition would allow for more proof support and thus would be more suitable than the model-based definition. While writing this note, my opinion has changed in favour to the model-theoretic definition. But it's like curing one evil with an even worse evil. In the following I have listed some pro's and cons'es of mt-conservative extension:

- + The definition of mt-conservative extensions is independent of the underlying logic. This seems to me an important point as translations of CASL aim at different logics.
- There is no uniform way (to be honest, I don't know of any) to prove the property of being a mt-conservative extension in a logical (proof theoretical) way. In general it is impossible to characterize a single infinite model (like natural numbers) inside any logic usable for automated theorem proving.
- +/- Switching to pt-conservative extensions would not be of any practical help as the definition postulates a property of all (usually infinitely many) sentences of a theory. As illustrated in the footnote, we cannot rephrase this property to a simple property of the given axioms.
- + There are subclasses of extensions for which we know how to prove that they are mt-conservative. Examples for this are constructive specifications. We can, for instance, provide definition principles how to define new functions based on given datatypes (like algorithms in INKA or the definition principle in NQTHM). In these cases the problem of being a mt-extension can be reduced to proving a first-order theorem (with induction).

Summing up, I have no clue how to tackle either notion of conservative extension in a CASL-verification tool. Is there a way to use Ehrenfeucht-Fraisse games for such purposes? From a more general point of view, the notion of mt-conservative extension captures the underlying idea more closer than the proof theoretical version and does not implicitly incorporate the weakness of logics into such a definition. Also, there are some special cases in which we can support the notion of mt-conservative extension, e.g. when using "algorithms" or special definition principles to extend a given theory.

---

## References

- [Andrews86] P.B. Andrews. An Introduction to Mathematical Logic and Type Theory: To Truth Through Proof. Academic Press, 1986
- [BP90] P. Byers, D. Pitt. Conservative Extensions: a Cautionary Note. *EATCS-Bulletin*, No. 41, pp. 196–201, 1997
- [Enderton72] H.B. Enderton. A Mathematical Introduction to Logic. Academic Press, 1972
- [Maibaum97] T.S.E. Maibaum. Conservative Extensions, Interpretations Between Theories and All That! TAPSOFT 97, Springer-Verlag, LNCS, pp. 40–67, 1997
- [Velo92] P.A.S. Veloso. Yet another cautionary note on conservative extensions: A Simple Case With a Computing Flavour. *EATCS Bulletin*, No. 46, pp. 188–192, 1992
- [VV91] P.A.S. Veloso, S.R.M. Veloso. Some Remarks on Conservative Extensions. A Socratic Dialogue. *EATCS Bulletin*, No. 43, pp. 189–198, 1991