Towards Coinductive Theory Exploration in Horn Clause Logic: Extended Abstract

Ekaterina Komendantskaya[a,1,3] Yue Li[a,2,3]

[a] *School of Mathematical and Computer Sciences Heriot-Watt University UK*

Coinductive proof methods have seen major developments in the last decade, and are reaching the point of maturity when coinductive proofs are used and implemented on par with inductive proofs. This step-change is facilitated by results from several research areas: coalgebra, fixed point theory, type theory, proof theory, automated deduction. In this abstract, we discuss a new coinductive approach to Horn clause logic.

A Horn clause fragment of FOL, named *fohc*, is given by the following syntax:

$$\begin{aligned} D &::= A \mid G \supset D \mid D \wedge D \ \mid \forall Var\ D \\ G &::= \top \mid G \wedge G \mid G \vee G \mid \exists Var\ G \end{aligned}$$

where A stands for the set of atomic first-order formulae of a given signature, and D and G – for sets of definite Horn clauses and definite Horn goals, respectively. A *theory* Γ is a set of D-formulae.

First coinductive interpretation to Horn clause logic was given by Apt and van Emden in the 80s: The *greatest complete Herbrand model* for a theory Γ is the largest set of finite and infinite ground terms *coinductively entailed* by Γ's clauses.

Example 0.1 Consider the three Horn clause theories Γ_1, Γ_2 and Γ_3 in Table 1, None of them has a meaningful inductive interpretation. However, they all have greatest (complete) Herbrand models, as Table 1 shows. These models define their coinductive interpretation. Notice how, depending on the clause structure, the models will differ: they may be given by finite sets of finite atomic formulae (for Γ_1), or infinite sets of finite and infinite formulae (Γ_2), or finite sets of infinite formulae (Γ_3). Note that Γ_3 is a prototypical example of a productive stream definition [2]: just substitute f by a stream constructor $cons(a, \_)$ to obatin a definition of the infinite stream of a's. Only one infinite term satisfies Γ_3.

It has always been problematic to match the greatest complete Herbrand models with equally rich operational semantics. Infinite (SLD)-resolution derivations correspond to

[1] Email: ek19@hw.ac.uk

[2] Email: yl55@hw.ac.uk

[3] This Abstract reports the work in progress. The work is supported by EPSRC grant EP/N014758/1.

This paper is electronically published in
Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

hohc theory:	Γ_1 : 1. $\forall x, p(x) \supset p(x)$	Γ_2 : 2. $\forall x, p(f\ x) \supset p(x)$	Γ_3 : 3. $\forall x, p(x) \supset p(f\ x)$
model:	$\{\mathtt{p(a)}\}$	$\{\mathtt{p(a)}, \mathtt{p(f(a))}, \mathtt{p(f(f(a))}, \ldots, \mathtt{p(f(f\ldots)}\}$	$\{\mathtt{p(f(f\ldots)}\}$

Table 1
Examples of greatest (complete) Herbrand models for fohc theories $\Gamma_1, \Gamma_2, \Gamma_3$. We add an arbitrary constant symbol a to the signature, in order to have ground instances of formulae in the models.

coinductive models. They may be terminated if a loop invariant (also known as *coinductive invariant*) is found. The problem is then to automate the discovery of coinductive invariants. To illustrate how difficult this may prove to be, consider the following example. Given our three theories Γ_1, Γ_2 and Γ_3, suppose we want to prove a property $p(a)$ by coinduction.

Example 0.2 For Γ_1, we will observe the following resolution steps:

$$p(a) \xrightarrow{\mathit{apply}\ 1} p(a) \xrightarrow{\mathit{apply}\ CI_1} \checkmark$$

Clearly, $p(a)$ is the coinductive invariant (denoted as $CI_1 = p(a)$), the derivation is cyclic, and we can terminate soundly by noting this fact. (Note how Γ_1's model in Table 1 agrees with this conclusion).

However, it is entirely possible that an environment Γ entails $p(a)$, yet $p(a)$ does not occur as an invariant in its infinite derivation.

Example 0.3 Consider Γ_2. Trying to replicate the coinductive proof of Example 0.2 with coinductive invariant $p(a)$ would not work, as the coinductive invariant will not apply at any stage (the derivation does not have cycles):

$$p(a) \xrightarrow{\mathit{apply}\ 2} p(f\ a) \xrightarrow{\mathit{apply}\ 2} p(f\ f\ a) \longrightarrow \ldots$$

A valid (as well as useful) coinductive invariant in this proof is $CI_2 = \forall x, p(x)$. So, *given a suitable calculus*, we can first coinductively prove $\Gamma_2 \vdash \forall x, p(x)$, and then obtain $\Gamma_2 \vdash p(a)$ as a corollary. Note, however, that the formula $\forall x, p(x)$ does not satisfy the syntax of a goal formula in *fohc*.

Generally, discovering a suitable coinductive invariant may be a difficult task. Consider the following example, inspired by a similar example in [1].

Example 0.4 Suppose we want to prove $p(a)$ given the theory Γ_4 :
4.1. $\forall x, p(f\ x) \wedge q(x) \supset p(x)$
4.2. $q(a)$
4.3. $\forall x, q(x) \supset q(f\ x)$

It will give the following resolution trace:

$$p(a) \xrightarrow{\mathit{apply}\ 4.1} p(f\ a) \wedge q(a) \xrightarrow{\mathit{apply}\ 4.2} p(f\ a) \xrightarrow{\mathit{apply}\ 4.1} p(f\ f\ a) \wedge q(f\ a) \xrightarrow{\mathit{apply}\ 4.3} \ldots$$

The coinductive invariant $CI_1 = p(a)$ will not apply here, despite $p(a)$ being in the model of Γ_4. Actually, neither $CI_1 = p(a)$ nor $CI_2 = \forall x, p(x)$ would work as a suitable coinductive invariant. However, given a suitable calculus, we would be able to coinductively prove $\Gamma_4 \vdash \forall x, q(x) \supset p(x)$, from which $\Gamma_4 \vdash p(a)$ can be proven as a corollary. Again, note that $CI_3 = \forall x, q(x) \supset p(x)$ cannot be a goal formula in *fohc*, so we will need a different language for reasoning about coinductive invariant of the proof of $\Gamma_4 \vdash p(a)$.

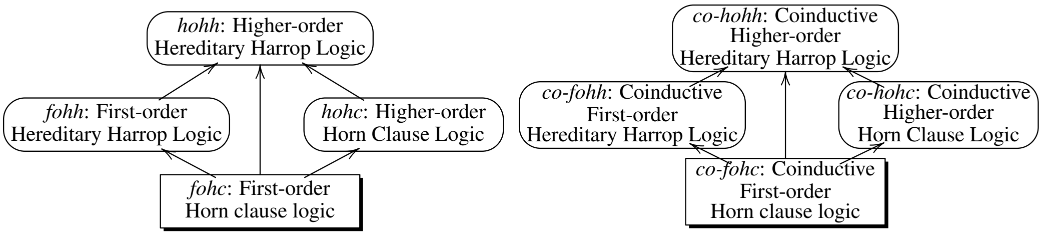
hohh: Higher-order Hereditary Harrop Logic
fohh: First-order Hereditary Harrop Logic
hohc: Higher-order Horn Clause Logic
fohc: First-order Horn clause logic
co-hohh: Coinductive Higher-order Hereditary Harrop Logic
co-fohh: Coinductive First-order Hereditary Harrop Logic
co-hohc: Coinductive Higher-order Horn Clause Logic
co-fohc: Coinductive First-order Horn clause logic

Fig. 1. **Left: uniform proof diamond by Miller et al. Right: coinductive uniform proof diamond proposed in this paper.** The arrows show syntactic extensions from first-order to higher-order, from Horn to hereditary Harrop clauses.

Finding a suitable coinductive invariant in a goal-directed proof search is actually a difficult task, which may require coming up with recursive terms on top of finding a suitable shape for the coinductive invariant, as the next example shows:

Example 0.5 Given a theory Γ_3 from Table 1 the goal-directed search by resolution will result in a derivation:

$$\underline{p(x)} \xrightarrow{apply\ 3,[x\mapsto f(x_1)]} p(x_1) \xrightarrow{apply\ 3,[x_1\mapsto f(x_2)]} p(x_2) \longrightarrow \ldots$$

None of the sub-goals can serve as a suitable coinductive invariant. The correct coinductive invariant in this derivation is $p(\mathit{fix}\ \lambda x.f\ x)$, where the fixpoint term $\mathit{fix}\ \lambda x.f\ x$ should be intuitively understood as a recursive definition for an infinite term $(f(f\ldots))$. Compare also with Γ_3's model in Table 1, and its only inhabitant $\mathtt{p(f(f}\ldots)$.

Thus, we would like to coinductively prove $\Gamma_3 \vdash p(\mathit{fix}\ \lambda x.f\ x)$ in a suitable logic, and then get $\Gamma_3 \vdash \exists x, p(x)$ as a corollary. Yet again, $p(\mathit{fix}\ \lambda x.f\ x)$ is not a formula of *fohc*, because of the syntax of $\mathit{fix}\ \lambda x.f\ x$.

Taking the assumption that a theory Γ and a formula F are expressed in the Horn clause fragment of first-order logic, we can show that there are four different classes of coinductive proofs for $\Gamma \vdash F$, and they are all characterised by the logic in which the coinductive invariant of the goal-directed derivation of F can be expressed and proven. We take the uniform proofs of Miller, Nadathur et. al [3], and in particular the four uniform proof logics *fohc*, *fohh*, *hohc*, *hohh* (see Figure 1), as a basis for our classification of the expressivity of the coinductive invariants. For example, coinductive invariant of Example 0.2 belongs to *fohc*, coinductive invariants of Examples 0.3 and 0.4 – to *fohh*, and the coinductive invariant of Example 0.5 – to *fohc* enriched with fixpoint terms. Horn clauses defining irregular streams will require the syntax of *hohh* with fixpoint terms. This classification provides foundations for automated exploration of coinductive invariants for proofs with coinductive theories expressed in Horn clause logic.

References

[1] P. Fu, E. Komendantskaya, T. Schrijvers, and A. Pond. Proof relevant corecursive resolution. In *FLOPS'16*, pages 126–143. Springer, 2016.

[2] E. Komendantskaya and Y. Li. Productive corecursion in logic programming. *J. TPLP (ICLP'17 post-proc.)*, 17(5-6):906–923, 2017.

[3] Dale Miller and Gopalan Nadathur. *Programming with Higher-order logic*. Cambridge University Press, 2012.