

Proof Reconstruction with Athena (Work in Progress)

Jonathan Prieto-Cubides

Advisor: Andrés Sicard-Ramírez

EAFIT University
Medellín, Colombia

Agda Implementors' Meeting XXV

Keywords

Proof Assistant

is a software program that work together with a human in order to give formal proofs to problems in a wide range of topics.

- Agda, Isabelle/HOL, HOL Light, Coq.

Automatic Theorem Prover

Is software program that tries to prove conjecture based on a list of hypothesis.

- Metis, Z3, Vampire, EProver, iProver, SPSS.

Athena

Is a Haskell program that translates proofs given by Metis ATP in TSTP format to Agda code.

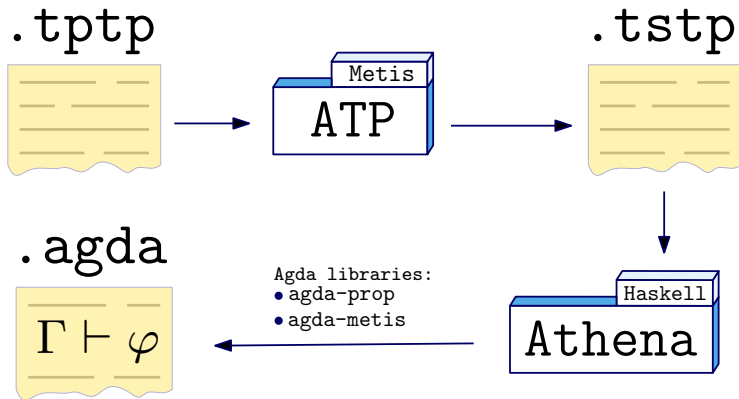


Figure: Proof reconstruction work flow.

TPTP

Is a text format to encode problems in different theories. Its goal is provide a standard for all ATPs in the input file format. The version for derivations is named TSTP but this one is not a standard yet.

A TPTP file looks like:

Listing 1: ../test/prop-pack/problems/basic/basic-4.tptp

```
fof(a1, axiom, p).  
fof(goal, conjecture, p).
```

TSTP

A derivation of the previous problem output by Metis ATP.

Listing 2: ../test/prop-pack/problems/basic/basic-4.tstp

```
% SZS start RequiredInformation
% Congratulations - you have become a registered power user of
% Please consider donating to the TPTP project - see www.tptp.
% When you donate this message will disappear.
% If you do not donate a random delay might be added to your p
% SZS end RequiredInformation
% START OF SYSTEM OUTPUT
-----
SZS status Theorem for /tmp/SystemOnTPTPFormReply82929/SOT_8L_

SZS output start CNFRefutation for /tmp/SystemOnTPTPFormReply8
fof(a1, axiom, (p)).

fof(goal, conjecture, (p)).

fof(subgoal_0, plain, (p), inference(strip, [], [goal])).

fof(negate_0_0, plain, (~ p), inference(negate, [], [subgoal_0
```

Agda

A verified proof of the previous derivation output by Athena.

```
proof0 :  $\Gamma \vdash \text{subgoal}_0$ 
proof0 =
  (RAA
    (atp-canonicalize
      (atp-simplify
        (atp-canonicalize
          (atp-strip
            (assume { $\Gamma = \Gamma$ }
              (atp-negate subgoal0))))))
    (atp-canonicalize
      (weaken (atp-negate subgoal0)
        (assume { $\Gamma = \emptyset$ } a1))))))

proof :  $\Gamma \vdash \text{goal}$ 
proof =
   $\Rightarrow$ -elim
    atp-splitGoal
    proof0
```

Figure: Type-checked Proof.

Natural deduction tree

$\Gamma, p \vdash p$

Proof.

$$\frac{\frac{\frac{\Gamma \vdash a_1}{\Gamma, \neg \text{subgoal}_0 \vdash a_1} \text{(weaken } \neg \text{subgoal}_0)}{\Gamma, \neg \text{subgoal}_0 \vdash p} \text{(canonicalize)}}{\frac{\frac{\frac{\Gamma \vdash p}{\Gamma, \neg \text{subgoal}_0 \vdash \neg p} \text{(assume)}}{\Gamma, \neg \text{subgoal}_0 \vdash \neg p} \text{(canonicalize)}}{\Gamma, \neg \text{subgoal}_0 \vdash \neg p} \text{(simplify)}}{\frac{\perp}{\Gamma \vdash p} \text{(RAA)}}$$

□

Future work

- Extend the libraries Agda-Prop and Agda-Metis to handle predicated logic
- Reconstruct proofs of eprover in Agda-EProver
- Support more versions of GHC in Athena

References