Proof Reconstruction in Classical Propositional Logic

Work in Progress

Jonathan Prieto-Cubides
Joint work with Andrés Sicard-Ramírez

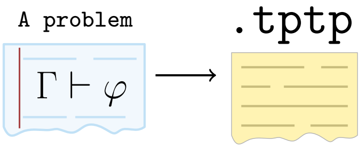
Universidad EAFIT
Medellín, Colombia

Agda Implementors' Meeting XXV
May 9-15th

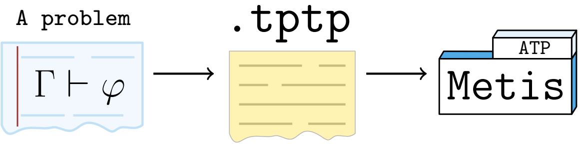
A problem

$$\Gamma \vdash \varphi$$

Proof Reconstruction: Overview

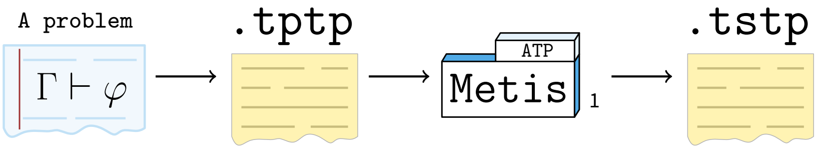


Proof Reconstruction: Overview

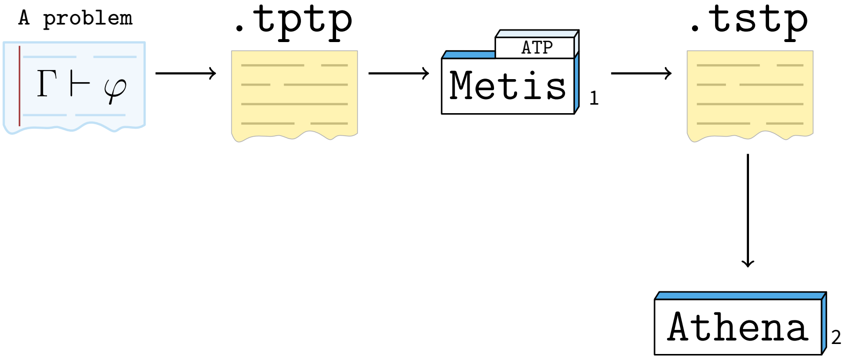


[1]

[1] It is available at `http://www.gilith.com/software/metis`

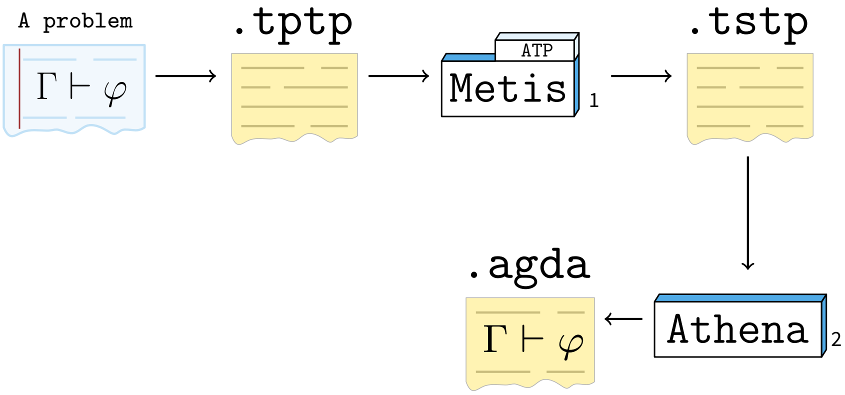


[1] It is available at `http://www.gilith.com/software/metis`



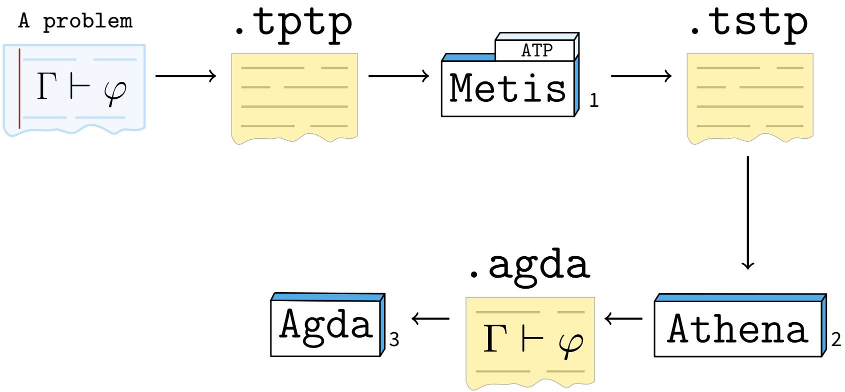
[1] It is available at `http://www.gilith.com/software/metis`

[2] It is available at `http://github.com/jonaprieto/athena`



[1] It is available at `http://www.gilith.com/software/metis`

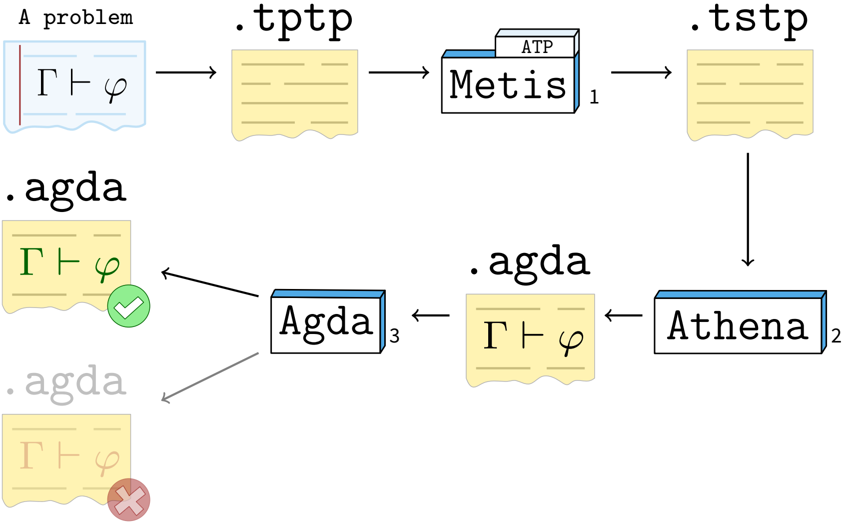
[2] It is available at `http://github.com/jonaprieto/athena`



[1] It is available at `http://www.gilith.com/software/metis`

[2] It is available at `http://github.com/jonaprieto/athena`

[3] It is available at `http://github.com/agda/agda`



[1] It is available at `http://www.gilith.com/software/metis`

[2] It is available at `http://github.com/jonaprieto/athena`

[3] It is available at `http://github.com/agda/agda`

SledgeHammer

- Isabelle/HOL tool
- Metis ported within Isabelle
- Reconstruct proofs of well-known ATPs: EProver, Vampire, among others

Integrating Waldmeister and Agda

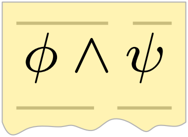
- Source code not available
- Equational Logic
- Reflection Layers

Related Work: Apia

Proving first-order theorems written in Agda using automatic theorem provers for first-order logic

At the moment, the communication between Agda and the ATPs is unidirectional because the ATPs are being used as oracles (Sicard-Ramírez, 2015).

.agda



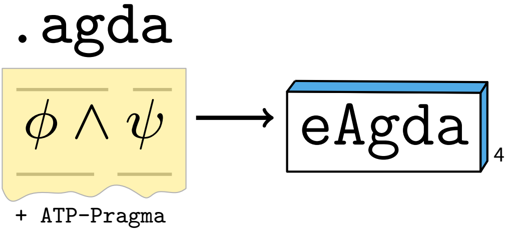
+ ATP-Pragma

```
$ cat Or.agda
module Or where

data _or_ (A B : Set) : Set where
  inj1 : A -> A or B
  inj2 : B -> A or B

postulate
  A B    : Set
  or-comm : A or B -> B or A
{-# ATP prove or-comm #-}
```

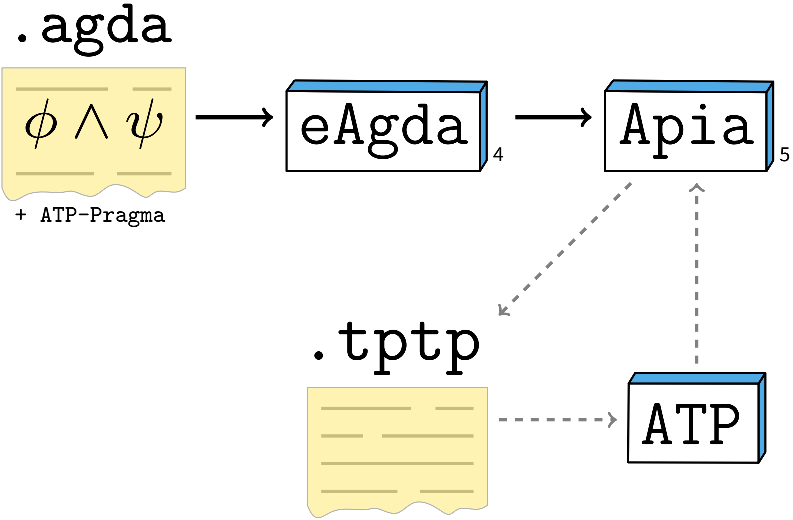
At the moment, the communication between Agda and the ATPs is unidirectional because the ATPs are being used as oracles (Sicard-Ramírez, 2015).



[4] Development version of Agda in order to handle a new built-in ATP-pragma. `https://github.com/asr/eagda`

Related Work: Apia

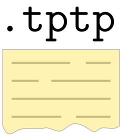
Proving first-order theorems written in Agda using automatic theorem provers for first-order logic



[4] Development version of Agda in order to handle a new built-in ATP-pragma. `https://github.com/asr/eagda`

[5] Haskell program for proving first-order theorems written in Agda using ATPs. `https://github.com/asr/apia`

Bonus Slides



- Is a language[6] to encode problems
- Is the input of the ATPs
- TPTP format contains formulas with the form

```
language(name, role, formula).
```

language FOF or CNF
name to identify the formula within the problem
role axiom, definition, hypothesis, conjecture, among others
formula version in TPTTP format

[6] Is available at `http://www.cs.miami.edu/~tptp/TPTP/SyntaxBNF.html`

Problems in Propositional Logic:

- $p \vdash p$

```
$ cat basic-4.tptp
fof(a, axiom, p).
fof(goal, conjecture, p).
```

- $p \wedge q \vdash q \wedge p$

```
$ cat conj-3.tptp
fof(a, axiom, p & q).
fof(goal, conjecture, q & p).
```

- $\vdash \neg(p \wedge \neg p) \vee (q \wedge \neg q)$

```
$ cat neg-7.tptp
fof(goal, conjecture, ~ ((p & ~ p) | (q & ~ q))).
```

Go Back

TSTP Syntax

.tstp

A TSTP derivation [8]

- Is a Directed Acyclic Graph where
  - `leaf` is a formulae from the TPTP input
  - `node` is a formulae inferred from parent formulae
  - `root` the final derived formulae
- Is a list of annotated formulae:

```
language(name, role, formula, source [,useful info]).
```

where **source** typically is a inference record:

```
inference(rule, useful information, parents)
```

[8] http://www.cs.miami.edu/~tptp/TPTP/QuickGuide/Derivations.html

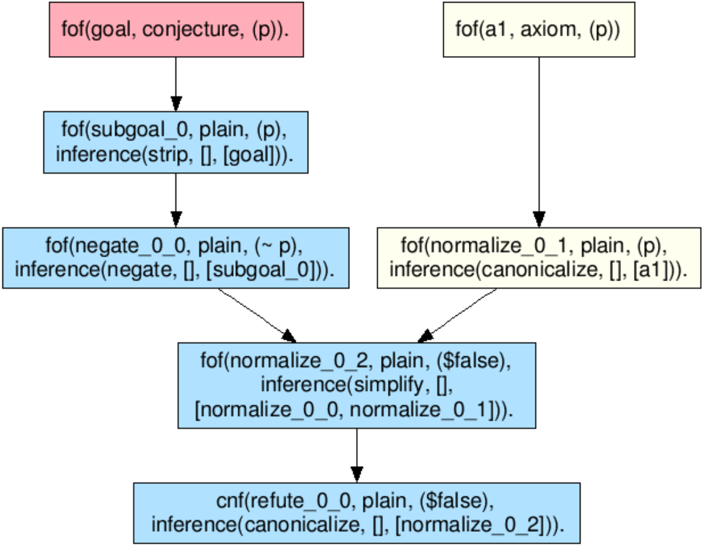
Go Back

- Proof found by **Metis** ATP for the problem $p \vdash p$

ATP
Metis

```
$ metis --show proof basic-4.tptp
fof(a, axiom, (p)).
fof(goal, conjecture, (p)).
fof(subgoal_0, plain, (p),
  inference(strip, [], [goal])).
fof(negate_0_0, plain, (~ p),
  inference(negate, [], [subgoal_0])).
fof(normalize_0_0, plain, (~ p),
  inference(canonicalize, [], [negate_0_0])).
fof(normalize_0_1, plain, (p),
  inference(canonicalize, [], [a])).
fof(normalize_0_2, plain, ($false),
  inference(simplify, [],
    [normalize_0_0, normalize_0_1])).
cnf(refute_0_0, plain, ($false),
    inference(canonicalize, [], [normalize_0_2])).
```

Go Back


fof(goal, conjecture, (p)).
fof(a1, axiom, (p))
fof(subgoal_0, plain, (p), inference(strip, [], [goal])).
fof(negate_0_0, plain, (~ p), inference(negate, [], [subgoal_0])).
fof(normalize_0_1, plain, (p), inference(canonicalize, [], [a1])).
fof(normalize_0_2, plain, ($false), inference(simplify, [], [normalize_0_0, normalize_0_1])).
cnf(refute_0_0, plain, ($false), inference(canonicalize, [], [normalize_0_2])).

Go Back

Athena

Athena

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

It depends on:

- **`agda-prop`** Classical Logic within Agda: Axioms + Theorems
- **`agda-metis`** Theorems of the inference rules of Metis Prover

Go Back

Athena

Haskell

- Parsing
- AST construction
- Creation and analysis of DAG derivations
- Analysis of inference rules used
- Generation of Agda code of the proof

Go Back

Agda

Agda

Is a dependently typed functional programming language and it also a proof assistant.
We used it to type-check the proofs found by Metis Prover

- Agda-Prop Libary: Logic framework for Classical Propositional Logic
- Agda-Metis Library: theorems based on the inference rules of Metis Prover

Go Back

Metis Theorem Prover

http://www.gilith.com/software/metis/

Metis is an automatic theorem prover for first order logic with equality

Why Metis?

- Open source implemented in Standard ML
- Reads problem in **TPTP** format
- Outputs detailed proofs in **TSTP** format
- Each refutation step is one of **6 simple rules**

Go Back

With Classical Propositional Logic, TSTP derivations exhibit these inferences:

- `Canonicalize` transforms formulas to CNF or NNF
- `Clausify` performs clausification
- `Conjunct` extracts a formula from a conjunction
- `Negate` applies negation to the formula
- `Resolve` applies theorems of resolution
- `Simplify` applies over a list of formula to simplify them
- `Strip` splits a formula into subgoals

Go Back

canonicalize

Clausify
Inference Rule

clausify

conjunct

```
$ cat ~/agda-metis/src/ATP/Metis/Rules/Conjunct.agd
...
conjunct : Prop -> Prop -> Prop
conjunct φ( ψ ) ω with  eq φω    |  eq ψω
... | true  | _      = φ
... | false | true   = ψ
... | false | false  = conjunct φω
conjunct φω          = φ

atp-conjunct
  : Γ {} φ{}
  -> ω( : Prop)
  -> Γφ
  -> Γ  conjunct φω
```

negate

resolve

simplify

strip

Example goes here

Go Back

Type-checked Proof

Verified Example goes here

Go Back

Type-checked Proof

Failure Example goes here

Go Back

Future Work

- Add shallow embedding in order to work with Apia
- Support First-Order Logic
- Support another prover like EProver
- Support a Intuitionistic Prover

Sicard-Ramírez, Andrés (2015). *Reasoning about functional programs by combining interactive and automatic proofs.* PEDECIBA Informática, Universidad de la República.