Higher Order Proof Engineering

Robert White

ILLC/INRIA

Cool Logic, ILLC

Outline

- Introduction
- HOL Light and HOL Proof Checking
  - OpenTheory
  - Holide and Dedukti
- ProofCloud
- HOLALA
  - HOL Kernel
  - Attempts
  - HOLALA
- Results and Benchmarks
- Future Work

Higher Order Logic

- Simple type theory (STT) is also known as Higher order logic (HOL).
- HOL = simply typed λ-Calculus + boolean types + axioms + inference rules.
- Most mathematical objects/theories can be expressed in HOL.
- Interactive and automatic theorem provers & proof checkers.
- HOL Light, ProofPower, HOL4, HOL Zero . . . [HOL family].

OpenTheory

- HOL family: HOL Light, ProofPower, HOL4, Isabelle . . .
- Need a platform to reuse proofs from different systems.
- OpenTheory has a standard format of proofs (*.art).
- Export proofs and import proofs (in article files).
- OpenTheory HOL Light:
  a modified version of HOL Light which allows import and export of proofs.

Holide and Dedukti

- OpenTheory has a repository of proof packages (articles).
- Holide translates proofs from OpenTheory articles to Dedukti.
- Dedukti is a proof checker (for proof checking).

Workflow of OpenTheory, Holide and Dedukti

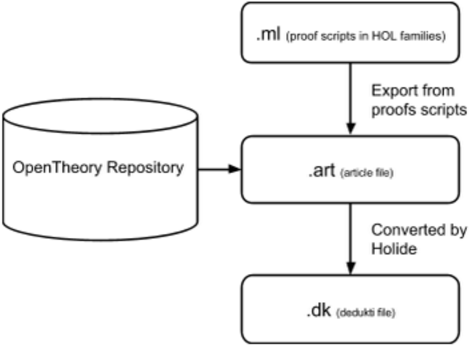
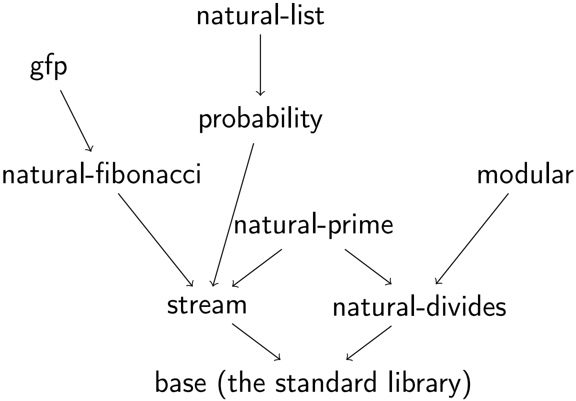


Figure: Work Flow of OpenTheory, Holide and Dedukti

ProofCloud

1. A Proof Retrievel Engine: `http://airobert.github.io/proofcloud/`
2. 1700+ pages of proofs with analysis.
3. A representation of proof checking results by Holide and Dedukti.
4. Which proofs are constructive?

Packages and Dependency



natural-list

gfp

probability

natural-fibonacci

modular

natural-prime

stream

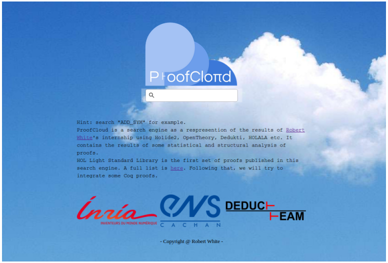
natural-divides

base (the standard library)

Figure: Dependency of Packages of OpenTheory

ProofCloud DEMO

Proof Search Engine which represents the analysis and proof checking results.



Hint: search "ADD_SYM" for example.

ProofCloud is a search engine as a respresention of the results of Robert White's internship using Holide2, OpenTheory, Dedukti, HOLALA etc. It contains the results of some statistical and structural analysis of proofs.

HOL Light Standard Library is the first set of proofs published in this search engine. A full list is here. Following that, we will try to integrate some Coq proofs.

- Copyright @ Robert White -

Figure: Index Page of ProofCloud (version 1)

It's version 2 now!!!

Structural Analysis

the combination of the *subst* and *eqmp* rule takes over 45% of all the inferences rules.

Inference Rules	**Count**
subst	93667
eqmp	92617
appthm	53155
proveHyp	47728
betaConv	21485
absThm	15096
trans	26727
. . .	. . .
assume	16986
Overall	**413207**

Statistical Results

1209 proofs in the standard library.
541 constructive proofs v.s. 668 classical proofs
44.75% of them constructive proofs.

(However) The *natural-divides* package has only 10 constructive proofs out of 136 proofs, making only 7.35% of them constructive.

Next, these 668 proofs to their constructive form?

Proof Translation and Proof Checking

The size of proof articles got reduced by around 7%. The proof checking time reduced by around 5%.
... not fun :(

Kernel

HOL syntax:

type variables	α, β
type operators	p
types	$A, B ::= \alpha \mid p(A_1, \ldots, A_n)$
term variables	x, y
term constants	c
terms	$M, N ::= x \mid \lambda x : A.M \mid MN \mid c$

Polymorphic Typed constant:

$$= : \alpha \to \alpha \to o$$

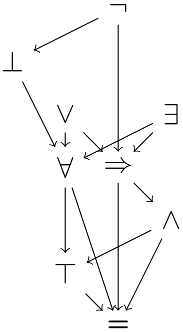
Primitive Inference Rules

Structural	$\dfrac{}{\{A\} \vdash A}$ *ASSUME*
λ Calculus	$\dfrac{\Gamma \vdash A = B}{\Gamma \vdash \lambda x.A = \lambda x.B}$ *ABS* $\dfrac{}{(\lambda x.A)x = A}$ *BETA*
Instantiation	$\dfrac{\Gamma[x_1, \ldots, x_n] \vdash A[x_1, \ldots, x_n]}{\Gamma[t_1, \ldots, t_n] \vdash A[t_1, \ldots, t_n]}$ *INST* $\dfrac{\Gamma[\alpha_1, \ldots, \alpha_n] \vdash A[\alpha_1, \ldots, \alpha_n]}{\Gamma[\gamma_1, \ldots, \gamma_n] \vdash A[\gamma_1, \ldots, \gamma_n]}$ *INST_TYPE*
Bi-implication	$\dfrac{\Gamma \vdash A = B \qquad \Delta \vdash A}{\Gamma \cup \Delta \vdash B}$ *EQ_MP* $\dfrac{\Gamma \vdash A \qquad \Delta \vdash B}{(\Gamma \setminus \{B\}) \cup \Delta \setminus \{A\}) \vdash A = B}$ *DEDUCTANTISYMRULE*
Equality	$\dfrac{}{\vdash A = A}$ *REFL* $\dfrac{\Gamma \vdash A = B \qquad \Delta \vdash C = D}{\Gamma \cup \Delta \vdash A(C) = B(D)}$ *MK_COMB* $\dfrac{\Gamma \vdash A = B \qquad \Delta \vdash B = C}{\Gamma \cup \Delta \vdash A = C}$ *TRANS*

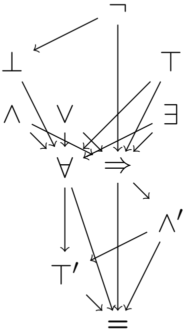
Kernel of OpenTheory HOL Light

OpenTheory HOL Light has a small and reliable kernel.
This kernel is based on $=$
Double negation requires taking $\forall$ and $\Rightarrow$ as primitive symbol.
Thus, kernel hacking!

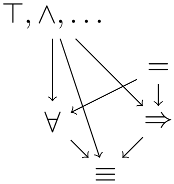
HOLALA



OpenTheory HOL Light

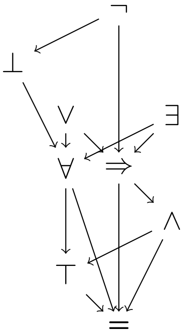


HOL-intermediate

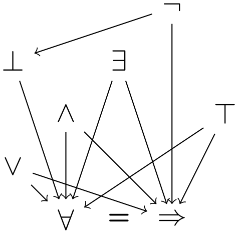


HOLIU

HOLALA



OpenTheory HOL Light



HOLALA

Structural Results

Two primitive deduction rule (subst and eqmp) combined is over 45%

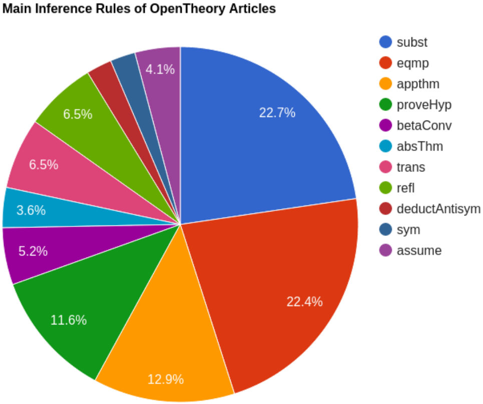


Figure: Frequency of Main Inference Rules of OpenTheory Articles

Structural Results

Introducing ⇒ and ∀ reduce the overall size of proofs by 40.87% (standard library with 1199 proofs).

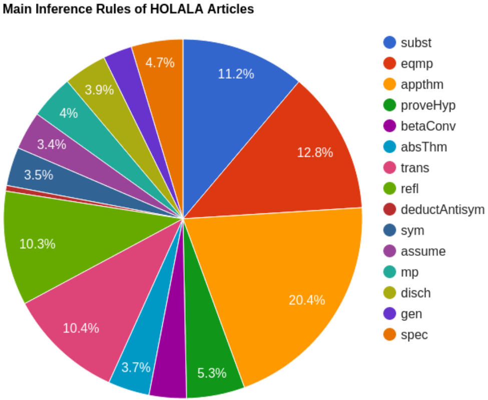


Figure: Frequency of Main Inference Rules of HOLALA Articles

Proof Checking

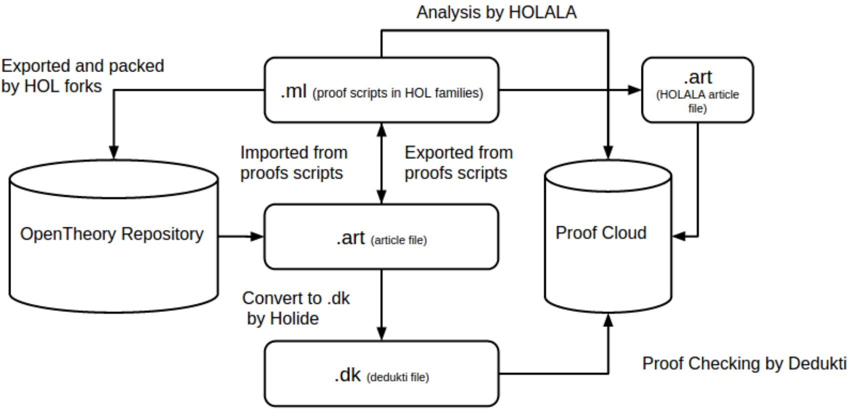

Analysis by HOLALA
Exported and packed by HOL forks
.ml (proof scripts in HOL families)
.art (HOLALA article file)
Imported from proofs scripts
Exported from proofs scripts
OpenTheory Repository
.art (article file)
Proof Cloud
Convert to .dk by Holide
.dk (dedukti file)
Proof Checking by Dedukti

Figure: Work Flow of HOLALA, Holide, OpenTheory and ProofCloud

Poof Checking Results

- Fully verified all the libraries in OpenTheory.
- Little difference between version 5 and version 6.
- The size of article files of HOLALA reduced to 23.63%.
- The translation time improved by 41.81%.
- The size of Dedukti files reduced to 64.33%.
- The proof checking time improved by 38.04%.

Future Work

- HOL-Modulo, a joint project at ILLC & INRIA.
- More proof analysis (for machine learning).
- ProofCloud
  - More packages
  - Better GUI
  - Coq, Agda . . . libraries?

The Actual Future Work

- Epistemic Learning and Planning for MAS.
- Multi-agent Motion Planning.
- O-et-O (a start-up based in Amsterdam Science Park)
- An advertisement for INRIA: a paid student internship opportunity (next summer).